

# Алгебраические числа как векторы

Жюри проекта: И. Воробьёв, С. Дориченко, А. Жилина, А. Канель–Белов, А. Канунников, Б. Френкин

## Введение

В геометрии мы привыкли складывать *векторы* и умножать их на *скаляры* (числа). Этот геометрический язык часто оказывается полезным в совершенно не геометрических ситуациях. В этом проекте мы рассмотрим в качестве векторов *алгебраические числа* — так называются корни многочленов с рациональными коэффициентами. Сами же рациональные числа будут выступать в роли скаляров.

Говорят, что комплексные числа  $x_1, \dots, x_n$  *линейно независимы* над  $\mathbb{Q}$ , если равенство  $a_1x_1 + \dots + a_nx_n = 0$ , где  $a_1, \dots, a_n \in \mathbb{Q}$ , возможно только при  $a_1 = \dots = a_n = 0$  (ср. с некомпланарными векторами на рисунке 1). Вообще, взгляд на алгебраические числа как на векторы оказывается очень естественным и продуктивным — он позволяет применять геометрические идеи к алгебраическим задачам.

Как устроен проект? Мы начнём с олимпиадных задач о радикалах для затравки. Некоторые из них можно решить школьными методами, для других нужны новые идеи и методы — начальные сведения об алгебраических числах и полях, изложенные во втором разделе. Вы научитесь удобному языку и аппарату для решения широкого круга задач. Это — предварительная часть проекта.

В третьей части мы сформулируем основную теорему проекта и предложим её доказать по приведённому плану, используя полученные знания. В заключение мы дадим исследовательскую задачу, развивающую и обобщающую теорему.

Что нужно знать заранее? Базовые факты о комплексных числах и многочленах. Главное — уметь извлекать корни из комплексных чисел и делить многочлены с остатком. Если вы мало знакомы с комплексными числами, то заведомо вам будут посильны задачи о квадратных радикалах.

Основы теории алгебраических чисел начали формироваться в трактате Карла Гаусса „Арифметические исследования“ (1801), сыгравшим огромную роль в теории чисел и подготовившим почву (наряду с работами Лагранжа) для открытий Эвариста Галуа, который установил критерий разрешимости уравнений в радикалах (1830) и заложил основы таких современных разделов алгебры, как теория групп и полей. Теория Галуа и теория полей алгебраических чисел были систематизированы и разработаны во второй половине XIX и начале XX века усилиями Куммера, Кронекера, Гильберта и др.

## 1. Задачи для затравки

Если какие-то задачи вызовут затруднения — вернитесь к ним после раздела 2.

**1.1.** Докажите иррациональность следующих чисел: а)  $\sqrt[3]{1001}$ ; б)  $\sqrt{2} + \sqrt{3} + \sqrt{6}$ ; в)  $\sqrt{2} + \sqrt[3]{3}$ ; г)\*  $\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7} + \sqrt{11}$ ; д)\*  $\sqrt[5]{3} - \sqrt[5]{2}$ ; е)\*\*  $\sqrt{\frac{3}{5}} + \frac{\sqrt[17]{2020!}}{2020} + \sqrt[5]{7^{77}}$ .

Если вы даже не представляете как подступиться к последнему, нарочно дикому, числу, то вот первое соображение: лучше доказывать более сильное утверждение о линейной независимости. Например, в пункте б) вот такое:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0, \text{ где } a, b, c, d \in \mathbb{Q} \implies a = b = c = d = 0.$$

**1.2.** Найдите многочлен наименьшей степени с рациональными коэффициентами и следующим корнем: а)  $\sqrt[3]{4}$ ; б)  $\sqrt{2} + \sqrt{3}$ ; в)  $\sqrt[3]{2} + \sqrt[3]{4}$ ; г)\*  $\sqrt[8]{8} + \sqrt[9]{9}$ ; д)\*  $\sqrt{6} + \sqrt{10} + \sqrt{15}$ ;

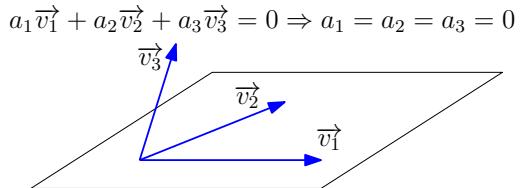


Рис. 1

- е)  $\sqrt[3]{1+\sqrt{2}} + \sqrt[3]{1-\sqrt{2}}$ ;    ё)  $\sqrt[3]{7+5\sqrt{2}} + \sqrt[3]{7-5\sqrt{2}}$  (внешнее сходство обманчиво!);  
ж)  $\cos \frac{2\pi}{5}$ ;    з)  $\cos \frac{2\pi}{9}$ ;    и)\*  $\cos \frac{2\pi}{97}$ ;    к)\*\*  $\cos \frac{2\pi}{n}$  при любом  $n \in \mathbb{N}$ .

Если нашли многочлен, но нет уверенности, что его степень минимальна, то всё равно укажите этот многочлен. Во всех пунктах, кроме в), г), и), к), напишите многочлен в стандартном виде. Как ни странно, для решения пунктов и), к) лучше перейти в комплексную плоскость.

- 1.3.** Какие числа вида  $\frac{a+bi}{a-bi}$ , где  $a, b \in \mathbb{Z}$ , являются корнями из единицы?

Вот несколько задач на квадратичные иррациональности. В них заложена важная идея ... (обойдёмся без спойлеров).

- 1.4.** Существуют ли такие рациональные числа  $a, b, c, d$ , что  $(a+b\sqrt{2})^2 + (c+d\sqrt{2})^2 = 7+5\sqrt{2}$ ?

- 1.5.** Найдите первые 1000 знаков после запятой в десятичной записи числа  $(6+\sqrt{37})^{1001}$ .

- 1.6.** Перемножаются все  $2^{100}$  выражений вида

$$\pm\sqrt{1} \pm \sqrt{2} \pm \dots \pm \sqrt{99} \pm \sqrt{100}$$

(при всех комбинациях знаков). Докажите, что результат: а) целое число; б) квадрат целого числа.

## 2. Немного теории: поля и алгебраические числа

Линейная независимость 1 и  $\sqrt{2}$  (над  $\mathbb{Q}$ ) означает просто иррациональность  $\sqrt{2}$ , известную ещё древним грекам. Увеличим число радикалов.

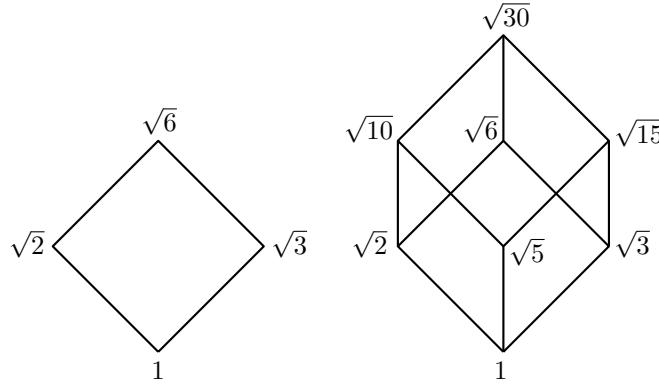


Рис. 2а

Рис. 2б

- 2.1.** Заполните пропуски в следующем рассуждении.

Докажем, что числа  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  линейно независимы над  $\mathbb{Q}$ . Пусть

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0, \text{ где } a, b, c, d \in \mathbb{Q}.$$

Отделим радикал  $\sqrt{3}$ :

$$a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0.$$

Если  $c + d\sqrt{2} = 0$ , то \_\_\_\_\_

Если же  $c + d\sqrt{2} \neq 0$ , то \_\_\_\_\_

$$\sqrt{3} = -\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = A + B\sqrt{2}, \text{ где } A = \text{_____} \in \mathbb{Q}, B = \text{_____} \in \mathbb{Q}.$$

Завершить доказательство можно разными способами.

На разобранном примере видны некоторые идеи. Мы свели линейную независимость чисел на рисунке 2а к тому, что число  $\sqrt{3}$  «инородно» по отношению к множеству

$$\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

(формально —  $\sqrt{3}$  не лежит в нём), подобно тому, как  $\sqrt{2}$  инородно по отношению к  $\mathbb{Q}$ . При этом оказалось важно, что в множестве  $\mathbb{Q} + \mathbb{Q}\sqrt{2}$  можно не только складывать, вычитать, умножать, но и делить (не на 0), как и в  $\mathbb{Q}$ , с помощью избавления от иррациональности в знаменателе.

Числовое множество, содержащее 0 и 1 и замкнутое относительно четырёх арифметических действий, называется *числовым полем*. Слово „числовое“ мы будем опускать<sup>1</sup>. Итак,  $K$  — поле, если  $0, 1 \in K$  и для любых  $a, b \in K$  верно  $a \pm b, ab \in K$  и  $a/b \in K$  при  $b \neq 0$ . Легко понять,  $\mathbb{Q}$  — поле, причём „самое маленькое“ — любое (числовое) поле его содержит. Если  $K \subseteq L$  — поля, то говорят, что  $K$  — *подполе* в  $L$ .

Говорят, что система чисел<sup>2</sup>  $x_1, \dots, x_n \in \mathbb{C}$  линейно независима над полем  $K$ , если равенство  $a_1x_1 + \dots + a_nx_n = 0$ , где  $a_1, \dots, a_n \in K$ , выполняется только при  $a_1 = \dots = a_n = 0$ . Например, числа 1 и  $\sqrt{2}$  линейно независимы над  $\mathbb{Q}$ , но линейно зависимы над  $\mathbb{R}$ .

**2.2. Простейшие свойства линейной зависимости.** Пусть  $K$  — поле. Докажите, что:

- а) система, содержащая 0 или два пропорциональных над  $K$  числа, линейно зависима над  $K$ ;
- б) подсистема линейно независимой системы линейно независима (над тем же полем);
- в) система  $1, x$  линейно независима над  $K$ , если и только если  $x \notin K$ ;
- г) коэффициенты  $a_1, \dots, a_n \in K$  в записи числа  $a_1x_1 + \dots + a_nx_n$  определены однозначно, если и только если система  $x_1, \dots, x_n$  линейно независима над  $K$ .

Присоединить к полю  $K$  числа  $\alpha_1, \dots, \alpha_n$  — значит взять наименьшее (по включению) поле, содержащее  $K$  и эти числа. Оно обозначается  $K(\alpha_1, \dots, \alpha_n)$ .

**2.3. Присоединение квадратного радикала.** Пусть  $K$  — подполе в  $\mathbb{R}$ ,  $0 < d \in K$  и  $\sqrt{d} \notin K$  (например,  $K = \mathbb{Q}$  и  $d = 2$ ). Докажите, что

$$K(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\},$$

причём числа  $a, b \in K$  в записи  $a + b\sqrt{d}$  определены однозначно.

**2.4.** Докажите, что  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

**2.5.** Избавьтесь от иррациональности в знаменателе:  $\frac{1}{1 + \sqrt{2} - \sqrt{3} + \sqrt{6}}$ .

**2.6. а)** Докажите, что числа в вершинах куба на рис. 2б линейно независимы над  $\mathbb{Q}$ .

**б)\*** Добавьте ещё  $\sqrt{7}$ , попробуйте нарисовать гиперкуб и докажите утверждение, аналогичное пункту а). А может, пора сформулировать общую теорему о квадратных радикалах из простых чисел и доказать её по индукции? В частности, из неё будет следовать решение задачи 1.1г).

Во что превратится определение линейной зависимости над полем  $K$  для степеней  $1, \alpha, \alpha^2, \dots, \alpha^n$  некоторого числа  $\alpha$ ? Существуют такие числа  $c_0, c_1, \dots, c_n \in K$ , не все равные нулю, что

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_n\alpha^n = 0.$$

Другими словами,  $\alpha$  является корнем ненулевого многочлена с коэффициентами из  $K$  — такое  $\alpha$  называется *алгебраическим над  $K$* . Среди всех таких многочленов только один имеет наименьшую степень и старший коэффициент 1 (почему?). Он называется *минимальным многочленом* числа  $\alpha$  над  $K$  и часто обозначается  $\mu_\alpha^K(x)$ . Например,  $\mu_i^{\mathbb{R}}(x) = x^2 + 1$ ,  $\mu_i^{\mathbb{C}}(x) = x - i$ . Степень  $\deg \mu_\alpha^K(x)$  этого многочлена называется также *степенью* числа  $\alpha$  над  $K$  и обозначается  $\deg_K(\alpha)$ . Корни многочлена  $\mu_\alpha^K(x)$  называются *сопряжёнными* с  $\alpha$  над  $K$ .

В случае  $K = \mathbb{Q}$  говорят просто об алгебраических числах.

**2.7.** Пусть число  $\alpha \in \mathbb{C}$  алгебраично над полем  $K \subseteq \mathbb{C}$ . Докажите:

- а)  $\deg_K(\alpha)$  есть наименьшее такое  $n \in \mathbb{N}$ , что степени  $1, \alpha, \dots, \alpha^n$  линейно зависимы над  $K$ ;
- б) многочлен  $\mu_\alpha^K(x)$  неприводим над  $K$  (т. е. не раскладывается в произведение многочленов строго меньшей степени);
- в) любой многочлен из  $K[x]$  с корнем  $\alpha$  делится на  $\mu_\alpha^K(x)$ ;
- г) неприводимый над  $K$  многочлен с корнем  $\alpha$  и старшим коэффициентом 1 равен  $\mu_\alpha^K(x)$ .

<sup>1</sup>Бывают и другие поля, например, поля вычетов, поля рациональных функций, ...

<sup>2</sup>Неупорядоченный набор чисел, в котором могут быть повторы.

Следующим признаком неприводимости многочлена над  $\mathbb{Q}$  можно пользоваться без доказательства.

**Теорема 1** (признак Эйзенштейна). *Если коэффициенты многочлена  $a_nx^n + \dots + a_1x + a_0 \in \mathbb{Z}[x]$  для некоторого простого  $p$  удовлетворяют условиям:*

- $p \nmid a_n$ ,
- $p \mid a_{n-1}, \dots, p \mid a_0$ ,
- $p^2 \nmid a_0$ ,

*то этот многочлен неприводим над  $\mathbb{Q}$ .*

**2.8. а)** Завершите решение задачи 1.1д). Пусть  $\sqrt[5]{3} - \sqrt[5]{2} = a \in \mathbb{Q}$ , тогда  $\sqrt[5]{3} = \sqrt[5]{2} + a$ . Найдём минимальные многочлены для чисел в левой и правой частях.

**б)** Решите уравнение в натуральных числах:  $\sqrt[5]{m} + \sqrt[5]{n} = 2020$ .

Обобщим теперь задачу 2.3.

**Теорема 2** (об избавлении от иррациональности в знаменателе). *Пусть число  $\alpha$  алгебраично над полем  $K$  и имеет степень  $n$ . Тогда каждое число в поле  $K(\alpha)$  однозначно записывается в виде*

$$c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}, \text{ где } c_0, c_1, \dots, c_{n-1} \in K.$$

**2.9. а)** Избавьтесь от иррациональности в знаменателе дроби  $\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3}$ . Указание. Здесь уже не работает пресловутое домножение на сопряжённое. Найдите такие многочлены  $u(x), v(x) \in \mathbb{Q}[x]$ , что  $u(x)(x^2 + x + 3) + v(x)(x^3 - 2) = 1$ . Для этого можно использовать либо обратный ход алгоритма Евклида, либо метод неопределённых коэффициентов.

**б)** Докажите теорему 2.

Согласно основной теореме алгебры, любой многочлен над  $\mathbb{C}$  степени  $n > 0$  имеет  $n$  корней с учётом кратности. Согласно следующей теореме, многочлен  $\mu_\alpha^K(x)$  не имеет кратных корней и, тем самым, *каждое алгебраическое число степени  $n$  имеет ровно  $n$  сопряжённых* (включая себя).

**Теорема 3.** *Многочлен, неприводимый над некоторым подполем в  $\mathbb{C}$ , не имеет кратных комплексных корней.*

**2.10.** Разложите двучлен  $x^4 - 2$  на неприводимые и разбейте его корни на классы сопряжённых над каждым из полей  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ .

Особого внимания заслуживают корни из единицы. Как известно, комплексные корни уравнения  $x^n = 1$  имеют вид

$$1, \varepsilon_n, \varepsilon_n^2, \dots, \varepsilon_n^{n-1}, \text{ где } \varepsilon_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

(это частный случай формулы Муавра). Разобъём их на классы сопряжённых над полем  $\mathbb{Q}$ . Для этого нужно разложить двучлен  $x^n - 1$  на неприводимые множители над  $\mathbb{Q}$ : корни каждого множителя образуют класс сопряжённых алгебраических чисел. Разберём примеры при малых  $n$ . На рисунке 3 неприводимые множители и их корни выделены одним цветом.

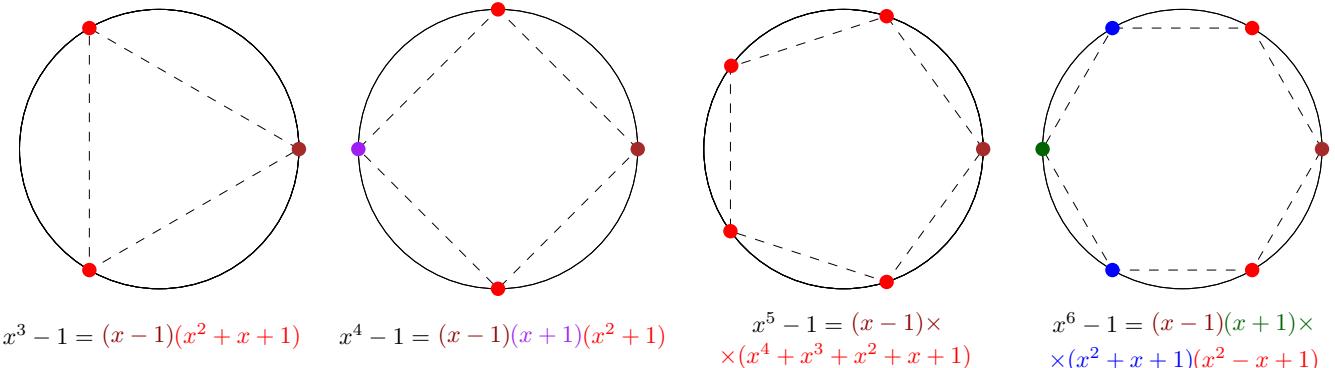


Рис. 3

Нужно пояснить лишь неприводимость многочлена  $x^4 + x^3 + x^2 + x + 1$ . Вот более общий факт.

**2.11.** Докажите, что для любого простого  $p$  многочлен

$$\Phi_p(x) = x^{p-1} + \dots + x + 1$$

неприводим над полем  $\mathbb{Q}$ . *Указание.* Используйте признак Эйзенштейна (теорема 1). Подумайте, как его применить, ведь все коэффициенты у  $\Phi_p(x)$  равны 1.

**2.12.** Разложите двучлен  $x^{12} - 1$  на неприводимые над  $\mathbb{Q}$  и нарисуйте картинку, аналогичную рисунку 3.

Пусть  $\varepsilon$  — корень из единицы. Его *порядком* называется наименьшее такое  $n \in \mathbb{N}$ , что  $\varepsilon^n = 1$ . Корни порядка  $n$  называются *первообразными* корнями степени  $n$ . Легко показать, что все такие корни имеют вид  $\varepsilon_n^k$ , где  $k$  взаимно просто с  $n$ . Количество чисел среди  $1, \dots, n$ , взаимно простых с  $n$ , обозначается  $\varphi(n)$ , функция  $\varphi$  называется *функцией Эйлера*.

**Теорема 4.** Корни степени  $n$  из единицы сопряжены над  $\mathbb{Q}$ , если и только если они имеют одинаковый порядок. В частности,  $\deg_{\mathbb{Q}}(\varepsilon_n) = \varphi(n)$  для всех  $n \in \mathbb{N}$ .

Эта теорема равносильна неприводимости над  $\mathbb{Q}$  так называемых *круговых многочленов*

$$\Phi_n(x) = \prod_{1 \leq k \leq n, (k,n)=1} (x - \varepsilon_n^k).$$

Задача 2.11 — простой частный случай. В общем случае не сразу очевидно даже, что коэффициенты у многочлена  $\Phi_n(x)$  — рациональные. Доказательство теоремы 4 в общем случае желающие смогут доказать на конференции. В любом случае ей можно пользоваться. С помощью теоремы 4 можно решить задачу 1.3 очень быстро.

Заполните пропуски в решении задачи **1.2в**). Найдём многочлен  $\mu_{\sqrt[3]{4} + \sqrt[3]{2}}(x)$  (по умолчанию — над полем  $\mathbb{Q}$ ). Ключевая идея в том, что  $\sqrt[3]{2}$  — корень многочлена  $\mu_{\sqrt[3]{4} + \sqrt[3]{2}}(x^2 + x)$ , который, стало быть, делится на  $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$ , а значит, имеет также корни  $\sqrt[3]{2}\varepsilon$  и  $\sqrt[3]{2}\varepsilon^2$ , где  $\varepsilon = \varepsilon_3$ . Следовательно, числа  $\sqrt[3]{4} + \sqrt[3]{2}$ ,  $\sqrt[3]{4}\varepsilon^2 + \sqrt[3]{2}\varepsilon$ ,  $\sqrt[3]{4}\varepsilon + \sqrt[3]{2}\varepsilon^2$  сопряжены. Далее, они все различны (почему?). Осталось показать, что многочлен

$$(x - \sqrt[3]{4} - \sqrt[3]{2})(x - \sqrt[3]{4}\varepsilon^2 - \sqrt[3]{2}\varepsilon)(x - \sqrt[3]{4}\varepsilon - \sqrt[3]{2}\varepsilon^2)$$

имеет рациональные коэффициенты — тогда он и будет  $\mu_{\sqrt[3]{4} + \sqrt[3]{2}}(x)$ . Покажите это.

Обобщением этого рассуждения является следующая теорема — одна из главных в проекте.

**Теорема 5.** Если  $\alpha = \alpha_1, \dots, \alpha_n$  — все сопряжённые с числом  $\alpha$  над полем  $K$ , то для любого многочлена  $f(x) \in K[x]$  число  $f(\alpha)$  алгебраично над  $K$  и его сопряжённые суть  $f(\alpha_1), \dots, f(\alpha_n)$ , причём в этом списке могут быть повторы и тогда каждый элемент встречается одно и то же число раз.

**2.13.** Докажите теорему 5: **а)** в случае, когда  $\alpha$  — корень неприводимого двучлена; **б)** в общем случае. (Для исследования линейной независимости радикалов достаточно пункта **а**), который проще. В пункте **б**) можно использовать основную теорему о симметрических многочленах.)

Вот план доказательства.

1) Чтобы доказать, что  $f(\alpha)$  алгебраично и его сопряжённые находятся среди чисел  $f(\alpha_1), \dots, f(\alpha_n)$ , рассмотрите многочлен

$$F(x) = (x - f(\alpha_1)) \dots (x - f(\alpha_n))$$

и докажите, что  $F(x) \in K[x]$ .

2) Чтобы доказать, что все числа  $f(\alpha_1), \dots, f(\alpha_n)$  сопряжены над  $K$ , рассмотрите многочлен  $\mu_{f(\alpha)}f(x)$ .

3) Докажите, что все корни многочлена  $F(x)$  имеют одинаковую кратность, рассмотрев многочлен  $F(x)/\mu_{f(\alpha)}(x)$ .

**2.14.** Найдите все  $n \in \mathbb{N}$ , при которых число  $\cos \frac{2\pi}{n}$ : **а)** рационально; **б)** представляется в виде  $a + \sqrt{b}$ , где  $a, b \in \mathbb{Q}$ , т. е.  $\deg_{\mathbb{Q}}(\cos \frac{2\pi}{n}) \leq 2$ .

### 3. Построение правильных многоугольников

Подумайте, как решить задачу **1.2з**) с помощью теорем 4 и 5. Эта задача — ключевая в доказательстве части «только если» теоремы Гаусса–Ванцеля: *правильный  $n$ -угольник строится циркулем и линейкой, если и только если  $\varphi(n)$  — степень двойки, т. е. если  $n$  — произведение степени двойки и простых чисел Ферма.* Числа Ферма — это числа вида  $2^{2^k} + 1$ . Первые 5 из этих чисел простые: 3, 5, 17, 257, 65537.

**3.1.** Постройте с помощью циркуля и линейки правильные: **а)** 5-угольник; **б)** 17-угольник.

**3.2.** Разработайте алгоритм и напишите программу на компьютере для построения правильного  $p$ -угольника при: **а)**  $p = 17$ ; **б)**  $p = 257$ ; **в)**  $p = 65537$ .

Гаусс построил правильный 17-угольник и доказал, что для любого простого числа Ферма  $p$  правильный  $p$ -угольник можно построить. Этот случай (пункт а)) не оценивается отдельно, но представляет собой важную ступеньку, и мы рекомендуем разобрать его как вручную, так и с помощью компьютерной программы.

Правильный 257-угольник был построен Ришело в XIX веке; в XXI веке вычисления лучше поручить компьютеру. Программа для  $p = 257$  будет оценена отдельным дипломом. Программа для  $p = 65537$  будет новым результатом и может быть подана в научный журнал.

**3.3.** Постройте с помощью циркуля, линейки и трисектора (прибора, делящего угол на три равных угла) корни многочленов: **а)**  $8x^3 - 6x + 1$ ; **б)**  $512x^9 - 1152x^7 + 864x^5 - 240x^3 + 18x + 1$ . (Это связано с 9- и 27-угольниками.)

**3.4.** Найдите все простые  $p$ , для которых существует единственное  $a \in \{1, \dots, p-1\}$  с условием  $p \mid a^3 - 3a + 1$ .

**3.5.** Постройте с помощью циркуля, линейки и трисектора правильные: **а)** 7-угольник; **б)** 13-угольник.

“Один слишком навязчивый аспирант довёл своего руководителя до того, что тот сказал ему: “Идите и разработайте построение правильного многоугольника с 65537 сторонами”. Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением” (Дж. Литвуд, “Математическая смесь”) А рукопись И. Г. Гермеса, написанная в 1894 г. в результате более чем десятилетних исследований и содержащая построение правильного 65537-угольника, хранится в библиотеке Гётtingенского университета и содержит больше 200 страниц. Но сейчас с помощью компьютера можно добиться этого результата за значительно меньшее время.

### 4. Линейная независимость радикалов

**Теорема 6.** Пусть  $N, k_1, \dots, k_N \in \mathbb{N}$ ,  $N > 1$ ,  $Q_1, \dots, Q_N \in \mathbb{Q}_+$ , причём  $\sqrt[k_i]{Q_i}/\sqrt[k_j]{Q_j} \notin \mathbb{Q}$  при всех  $i \neq j$ . Тогда равенство

$$a_1 \sqrt[k_1]{Q_1} + \dots + a_N \sqrt[k_N]{Q_N} = 0, \text{ где } a_1, \dots, a_N \in \mathbb{Q},$$

выполняется только при  $a_1 = \dots = a_N = 0$ .

В частности, при  $Q_1 = 1$  получим, что сумма  $\sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N}$  иррациональна, так как равенство  $a_1 \sqrt[3]{1} + \sqrt[3]{Q_2} + \dots + \sqrt[N]{Q_N} = 0$  не может выполняться ни при каком  $a_1 \in \mathbb{Q}$ .

Иrrациональность одного радикала — простой, чисто арифметический, вопрос, сводящийся к однозначности разложения на простые множители.

**Лемма 1.** Для всех  $k \in \mathbb{N}$  и  $Q \in \mathbb{Q}_+$  имеем:  $\sqrt[k]{Q} \in \mathbb{Q}$ , если и только если показатели всех простых делителей числителя и знаменателя в несократимом представлении  $Q$  кратны  $k$ .

**4.1.** Докажите лемму 1.

**4.2.** Выведите из теоремы 6 и леммы 1 иррациональность чисел из задачи 1.1.

Не умаляя общности, в теореме 6 можно считать все числа  $Q_i$  натуральными, а все показатели  $k_i$  равными, и доказывать тем самым следующую равносильную теорему.

**Теорема 7.** Пусть  $k, n \in \mathbb{N}$ ,  $p_1, \dots, p_n$  — различные простые числа,  $r_i = \sqrt[k]{p_i}$  при  $i = 1, \dots, n$ . Тогда система  $\{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leq l_1, \dots, l_n < k\}$  из  $k^n$  чисел линейно независима над  $\mathbb{Q}$ .

Эту систему удобно представлять в виде  $n$ -мерной решётки, см. примеры на рисунках 2 и 4.

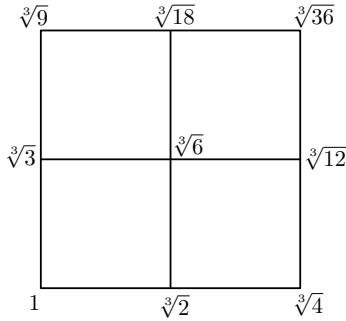


Рис. 4

**4.3.** Выполните теоремы 6 и 7 друг из друга.

**4.4.** Как в задаче 2.6, сведите теорему 7 при  $k = 2$  к следующему утверждению и докажите его:

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}).$$

(Рекомендуем использовать переход к сопряжённым числам — так проще понять случай  $k > 2$ .)

**4.5.** Докажите, что теорема 7 равносильна **теореме 7'**: в обозначениях теоремы 7 степени  $1, r_n, \dots, r_n^{k-1}$  линейно независимы над полем  $\mathbb{Q}(r_1, \dots, r_{n-1})$ .

**4.6.** Пусть  $K$  — подполе в  $\mathbb{R}$ ,  $r \in \mathbb{R}$ ,  $r^k \in K$  и  $r, \dots, r^{k-1} \notin K$ . Докажите, что двучлен  $x^k - r^k$  неприводим над  $K$  и степени  $1, r, \dots, r^{k-1}$  линейно независимы над  $K$ .

Таким образом, теорема 7' сведена к следующей **теореме 7''**: в тех же обозначениях

$$r_n^l \notin \mathbb{Q}(r_1, \dots, r_{n-1}) \text{ ни для какого } l \in \{1, \dots, k-1\}.$$

Предположим противное. По предположению индукции каждое число из поля  $\mathbb{Q}(r_1, \dots, r_{n-1})$  однозначно представляется в виде суммы произведений вида  $ar_1^{l_1} \dots r_{n-1}^{l_{n-1}}$ , где  $a \in \mathbb{Q}$  и все  $l_i \in \{0, \dots, k-1\}$ .

**4.7.** Получите противоречие, если в этой сумме ровно одно слагаемое.

Если в этой сумме хотя бы два слагаемых, то с точностью до перестановки радикалов  $r_1, \dots, r_{n-1}$  можно считать, что

$$r_n^l = A_0 + A_1 r_{n-1} + \dots + A_{k-1} r_{n-1}^{k-1}, \text{ где } A_0, \dots, A_{k-1} \in \mathbb{Q}(r_1, \dots, r_{n-2}), \quad (1)$$

где среди  $A_0, \dots, A_{k-1}$  хотя бы два ненулевых.

**4.8. а)** Докажите, что  $A_0 = 0$ .

**б)** Пусть  $A_j$  — первый ненулевой коэффициент в (1). Придите к противоречию, доказав, что  $A_j = 0$  (подумайте, как свести задачу к предыдущему пункту). Это завершает доказательство теоремы 7.

**4.9.** Остаётся ли теорема 7 в силе, если под каждым  $r_j$  ( $j = 1, \dots, n$ ) понимать некоторое комплексное значение корня  $\sqrt[k]{p_j}$ ?

## 5. Размерности расширений полей

Для более глубокого понимания алгебраических чисел и решения более трудных задач мы познакомимся с понятием векторного пространства, его размерности и освоим технику расширений полей (всё — для числовых множеств).

Подмножество  $V \subseteq \mathbb{C}$ , содержащее поле  $K$ , называется *векторным пространством над  $K$* , а его элементы — *векторами*, если  $V$  замкнуто относительно умножения на числа из  $K$  и сложения,

т. е.  $a + b, ka \in V$  для любых  $a, b \in V$  и  $k \in K$ . Например, всякое поле является векторным пространством над любым своим подполем.

Предположим, что пространство  $V \subseteq \mathbb{C}$  над полем  $K$  содержит такие числа  $e_1, \dots, e_n$ , что всякое  $\alpha \in V$  представляется в виде

$$\alpha = k_1 e_1 + \dots + k_n e_n \quad (2)$$

с однозначно определёнными коэффициентами  $k_1, \dots, k_n \in K$ . Тогда система  $e_1, \dots, e_n$  называется *базисом* пространства  $V$  над  $K$ , а равенство (2) — *разложением* числа  $\alpha$  по этому базису.

**5.1.** Докажите, что базис пространства можно определить равносильным образом как максимальную по включению линейно независимую систему векторов. Иными словами, система  $e_1, \dots, e_n$  — базис в  $V$  над  $K$ , если и только если она линейно независима над  $K$ , а система  $e_1, \dots, e_n, \alpha$  линейно зависима над  $K$  для любого  $\alpha \in V$ .

Пространство, обладающее конечным базисом, называется конечномерным, а расширение поля, обладающее конечным базисом, называют *конечным*. Число элементов в базисе пространства  $V$  над  $K$  называется его *размерностью* и обозначается  $\dim_K V$ . Корректность этого определения, т. е. независимость от выбора базиса, вытекает из следующей леммы.

**Лемма 2** (основная лемма о линейной зависимости). *Если числа  $f_1, \dots, f_m$  линейно выражаются над полем  $K$  через числа  $e_1, \dots, e_n$  и  $m > n$ , то числа  $f_1, \dots, f_m$  линейно зависимы над  $K$ .*

Пусть  $U \subseteq W$  — конечномерные пространства над полем  $K$ . Несложно проверить, что всякий базис в  $U$  можно дополнить до базиса в  $V$ . Тем самым,  $\dim_K U \leq \dim_K V$  и  $\dim_K U = \dim_K V \Leftrightarrow U = V$ .

Если  $L$  — подполе поля  $K$ , то говорят о расширении полей  $L/K$ . Очевидно, в этом случае  $L$  — векторное пространство над  $K$ . Размерность конечного расширения  $L/K$  называется также его *степенью* и обозначается  $[L : K]$ .

**5.2.** Пусть  $L/K$  — конечное расширение. Докажите, что  $[L : K] = 2 \Leftrightarrow L = K(\alpha)$  для некоторого такого  $\alpha \in L \setminus K$ , что  $\alpha^2 \in K$ .

**5.3.** Докажите, что числа  $1, \alpha, \dots, \alpha^{n-1}$  образуют базис расширения  $K(\alpha)/K$ , если и только если число  $\alpha$  алгебраично над  $K$  и имеет степень  $n$ . Итак, если  $\alpha$  алгебраично над  $K$ , то  $\deg_K(\alpha) = [K(\alpha) : K]$ .

Полезный инструмент в теории конечных расширений — следующая теорема (докажите её).

**Теорема 8** (о размерности башни). *Если  $K \subseteq P \subseteq L$  — конечные расширения полей, то*

$$\dim_K L = \dim_K P \cdot \dim_P L.$$

Ср. со свойством логарифмов  $\log_a c = \log_a b \cdot \log_b c$ .

Вернитесь к задаче для затравки **1.1в**).

**5.4.** Найдите все подполя в полях: а)  $\mathbb{Q}(\sqrt[11]{1024})$ ; б)  $\mathbb{Q}(\sqrt[4]{3})$ ; в)  $\mathbb{Q}(\varepsilon_5)$ ; г)  $\mathbb{Q}(\varepsilon_8)$ .

**5.5\*.** Обозначим  $\varepsilon = \varepsilon_{17}$ . Из теоремы 2 и задачи 2.11 следует, что  $\deg(\varepsilon) = 16$ .

а) Найдите все  $\alpha \in \mathbb{Q}(\varepsilon)$ , для которых  $\deg(\alpha) = 2, 4, 8$ . Указание: воспользуйтесь теоремой 5, рассмотрев базис  $\varepsilon, \varepsilon^3, \varepsilon^{3^2}, \dots, \varepsilon^{3^{15}}$  в  $\mathbb{Q}(\varepsilon)$  над  $\mathbb{Q}$  (докажите, что это базис). Это упорядочение принадлежит Гауссу.

**5.6.** Найдите все сопряжённые над  $\mathbb{Q}$  к числам: а)  $\sqrt{6} + \sqrt{10} + \sqrt{15}$ ; б)  $\sqrt[3]{2} + \sqrt[3]{3}$ .

б) Пусть  $U_k = \{\alpha \in \mathbb{Q}(\varepsilon) \mid \deg(\alpha) \text{ делит } k\}$ ,  $k = 1, 2, 4, 8, 16$ . В частности,  $U_1 = \mathbb{Q}$  и  $U_{16} = \mathbb{Q}(\varepsilon)$ . Докажите, что  $U_1 \subset U_2 \subset U_4 \subset U_8 \subset U_{16}$  — цепочка квадратичных расширений полей. Таким способом можно построить правильный 17-угольник с помощью циркуля и линейки (открытие Гаусса).

**Исследовательская задача.** Какие правильные  $n$ -угольники можно построить с помощью циркуля, линейки и трисектора? Частные случаи:  $n = 7, 13, 19, 37$ .

**Исследовательская задача.** Разработайте алгоритм нахождения степени любого алгебраического числа из расширения  $\mathbb{Q}(\sqrt[p_1]{\dots}, \sqrt[p_n]{\dots})$ , где  $p_1, \dots, p_n$  — различные простые числа. Частные случаи:  $k = 2$ ;  $k$  — простое.

# Линейная независимость радикалов

А. Канунников, И. Воробьёв

## §1. Введение

Как доказать иррациональность чисел

$$\sqrt[3]{\frac{121}{111}}, \sqrt{2} + \sqrt{3}, \sqrt{2} + \sqrt[3]{3}, \sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7}, \sqrt[5]{3} - \sqrt[5]{2}, \sqrt{\frac{3}{5}} + \frac{\sqrt[17]{2021!}}{2021} + \sqrt[5]{\frac{7^7}{3^{33}}}?$$

Иррациональность одного радикала — простой, чисто арифметический, вопрос, сводящийся к разложению на простые множители.

**Лемма 1.** Пусть  $A, B, k \in \mathbb{N}$  и  $\text{НОД}(A, B) = 1$ . Тогда  $\sqrt[k]{A/B} \in \mathbb{Q}$ , если и только если показатели степеней всех простых делителей в разложениях чисел  $A$  и  $B$  кратны  $k$ .

**Доказательство.** Пусть  $\sqrt[k]{A/B} = a/b$ , где  $a, b \in \mathbb{N}$ , тогда  $Ab^k = Ba^k$ . Каждый простой делитель  $p$  числа  $A$  не делит  $B$  и входит в разложения чисел  $a^k$  и  $b^k$  в степенях, кратных  $k$ , поэтому  $p$  входит в разложение  $A$  в степени, тоже кратной  $k$ . Рассуждение с простыми делителями числа  $B$  аналогично. В обратную сторону утверждение очевидно.  $\square$

Число  $\sqrt[3]{\frac{121}{111}} = \sqrt[3]{\frac{11^2}{3 \cdot 37}}$  иррационально по лемме 1. Если  $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$ , то  $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \in \mathbb{Q}$ , откуда  $\sqrt{6} \in \mathbb{Q}$ , что неверно по той же лемме. Предположив, что  $\sqrt{2} + \sqrt[3]{3} = a \in \mathbb{Q}$ , возведём равенство  $\sqrt[3]{3} = a - \sqrt{2}$  в куб:  $3 = a^3 + 6a - (3a^2 + 2)\sqrt{2}$  и придём к противоречию:  $\sqrt{2} = \frac{a^3 + 6a - 3}{3a^2 + 2} \in \mathbb{Q}$ . Однако остальные числа «голыми руками не возьмёшь»: незатейливое возведение в степень только приумножит количество радикалов.

„Неужели, прочитав статью, я пойму, почему даже последнее, нарочито дикое, число иррационально?“ — наверное, думает читатель в эту минуту. „Да, — ответим мы, — если только вы умеете делить многочлены с остатком и извлекать корни из комплексных чисел. Если пока не умеете, то во всяком случае вы разберётесь со сколь угодно длинными суммами квадратных радикалов.“

На самом деле, мы докажем даже большее: между корнями из рациональных чисел не существует линейных соотношений с рациональными коэффициентами, кроме очевидных отношений пропорциональности, например,  $\sqrt{8} = 2\sqrt{2}$ . Вот точная формулировка.

**Теорема 1.** Пусть  $N, k_1, \dots, k_N \in \mathbb{N}$ ,  $N > 1$ ,  $0 < Q_1, \dots, Q_N \in \mathbb{Q}$  и  $\sqrt[k_i]{Q_i}/\sqrt[k_j]{Q_j} \notin \mathbb{Q}$  при  $i \neq j$ . Тогда равенство

$$a_1 \sqrt[k_1]{Q_1} + \dots + a_N \sqrt[k_N]{Q_N} = 0, \text{ где } a_1, \dots, a_N \in \mathbb{Q},$$

выполняется только при  $a_1 = \dots = a_N = 0$ .

В частности, при  $Q_1 = 1$  получим, что сумма  $\sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N}$  иррациональна, так как равенство  $a_1 \sqrt[k_1]{1} + \sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N} = 0$  не может выполняться ни при каком  $a_1 \in \mathbb{Q}$ .

Чтобы применять теорему 1, нужно проверять иррациональность отдельных радикалов  $\sqrt[k_i k_j]{Q_i^{k_j}/Q_j^{k_i}}$  по лемме 1.

**ЗАДАЧА 1.** Выведите из теоремы 1 и леммы 1 иррациональность трёх последних чисел в начале статьи.

На языке векторов утверждение теоремы 1 формулируется так: числа  $\sqrt[k_1]{Q_1}, \dots, \sqrt[k_N]{Q_N}$  линейно независимы над  $\mathbb{Q}$  (сравните с некомпланарными векторами на рисунке 1). Условие  $\sqrt[k_i]{Q_i}/\sqrt[k_j]{Q_j} \notin \mathbb{Q}$  в этих терминах означает линейную независимость чисел  $\sqrt[k_i]{Q_i}$  и  $\sqrt[k_j]{Q_j}$  над  $\mathbb{Q}$  (линейная независимость двух векторов — это просто их неколлинеарность).

Вообще, взгляд на алгебраические числа (в частности, на радикалы) как на векторы оказывается естественным и продуктивным — он позволяет применять геометрические идеи к алгебраическим задачам [4].

Сформулируем более удобную для доказательства, но, как окажется, равносильную теорему.

**Теорема 2.** Пусть  $k, n \in \mathbb{N}$ ,  $p_1, \dots, p_n$  — различные простые числа,  $r_1 = \sqrt[k]{p_1}, \dots, r_n = \sqrt[k]{p_n}$ . Тогда система  $\{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leq l_1, \dots, l_n < k\}$  из  $k^n$  чисел линейно независима над  $\mathbb{Q}$ .

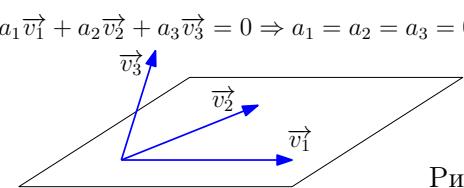


Рис. 1

Эту систему удобно представлять в виде  $n$ -мерной решётки, см. примеры на рисунке 2.

**ЗАДАЧА 2.** а) Как связаны наборы чисел на параллельных сторонах квадрата на рисунке 2а и на параллельных рёбрах и гранях куба на рисунке 2б? б) Попробуйте нарисовать гиперкуб (4-мерный куб) и расставить в его вершинах радикалы по тому же принципу.

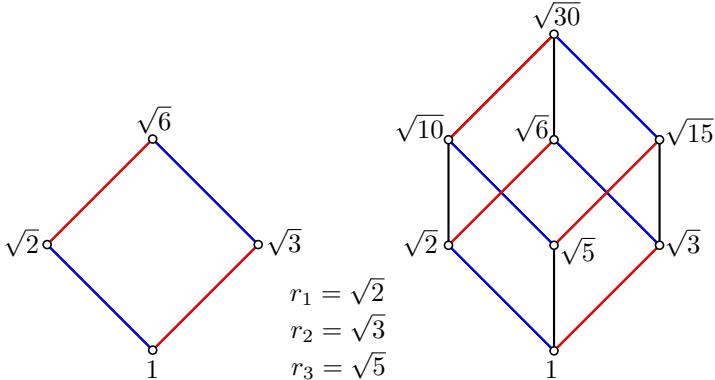


Рис. 2а

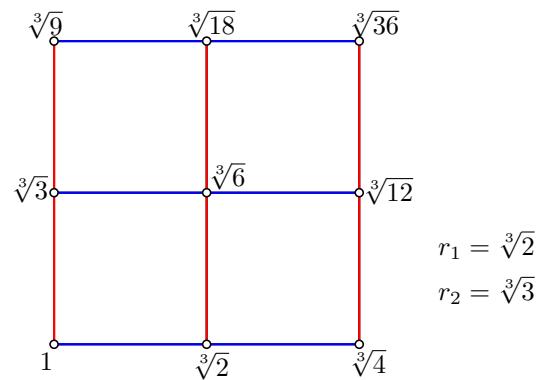


Рис. 2в

**ЗАДАЧА 3.** Выведите теоремы 1 и 2 друг из друга. *Указание.* 1  $\Rightarrow$  2: числа из системы в теореме 2 попарно непропорциональны над  $\mathbb{Q}$ ; 2  $\Rightarrow$  1: обобщите рассуждение из следующего примера.

**Пример 1.** Сведём линейную независимость (по умолчанию — над  $\mathbb{Q}$ ) чисел  $1, \sqrt{1/2}, \sqrt[3]{4/3}$  к теореме 2. Выравняем показатели корней:  $1, \sqrt[6]{1/2^3}, \sqrt[6]{2^4/3^2}$ , домножим второе число на 2, а третье — на 3:  $1, \sqrt[6]{2^3}, \sqrt[6]{2^4 \cdot 3^4}$  (это не влияет на линейную независимость). Получили подсистему системы  $\{\sqrt[6]{2^{l_1}}, \sqrt[6]{3^{l_2}} \mid 0 \leq l_1, l_2 \leq 5\}$ , а она линейно независима по теореме 2.

В литературе для школьников неоднократно обсуждался случай квадратных радикалов [2, 4, 6]. В §2 мы разберём его на примерах, подводя ко многим, пусть и не всем, идеям в общей ситуации. Теорема 2 при  $n = 1$  доказана в [5]. Общий случай разобран, например в научной статье [7] с помощью теории Галуа. В §3 мы докажем теорему 2 достаточно элементарно, попутно сообщая необходимые сведения об алгебраических числах, интересные и сами по себе. В конце мы приведём совсем короткое доказательство теоремы 1, доступное первокурснику. Всё необходимое для понимания собрано в §4.

## §2. Случай квадратных радикалов

Теорему 2 при  $k = 2$  можно доказать индукцией по  $n$ . База  $n = 1$ : линейная независимость 1 и  $\sqrt{p_1}$  означает просто иррациональность  $\sqrt{p_1}$  и имеет место по лемме 1. Разберём случаи  $n = 2, 3$  на конкретных примерах — так проще объяснить и понять идеи доказательства. Полное рассуждение с любым  $k$  индукцией по  $n$  проведём в §3.

**Пример 2.** Докажем, что числа  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  (рис. 2а) линейно независимы. Пусть  $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ , где  $a, b, c, d \in \mathbb{Q}$ . Выделим  $\sqrt{3}$ :  $a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0$ . Если  $c + d\sqrt{2} = 0$ , то и  $a + b\sqrt{2} = 0$ , а тогда, ввиду иррациональности  $\sqrt{2}$ ,  $c = d = 0$  и  $a = b = 0$ . Если же  $c + d\sqrt{2} \neq 0$ , то

$$\sqrt{3} = -\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = -\frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = A + B\sqrt{2}, \text{ где } A = \frac{2bd - ac}{c^2 - 2d^2}, B = \frac{ad - bc}{c^2 - 2d^2} \in \mathbb{Q}.$$

Возведём равенство  $\sqrt{3} = A + B\sqrt{2}$  в квадрат:

$$3 = A^2 + 2B^2 + 2AB\sqrt{2} \implies AB = 0, \text{ иначе } \sqrt{2} \in \mathbb{Q}.$$

При  $A = 0$  получаем  $\sqrt{3}/2 = B \in \mathbb{Q}$ , при  $B = 0$  получаем  $\sqrt{3} = A \in \mathbb{Q}$  — противоречие с леммой 1.

Мы свели линейную независимость чисел на рисунке 2а к «инородности»  $\sqrt{3}$  по отношению к множеству  $\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  (формально —  $\sqrt{3}$  не лежит в нём), подобно тому, как  $\sqrt{2}$  инородно по отношению к  $\mathbb{Q}$ . При этом оказалось важно, что в множестве  $\mathbb{Q} + \mathbb{Q}\sqrt{2}$  можно не только складывать, вычитать, умножать, но и делить (не на 0), как и в  $\mathbb{Q}$ . Прежде чем сделать следующий шаг, введём несколько понятий.

**Немного теории.** Множество чисел, содержащее 0 и 1 и замкнутое относительно четырёх арифметических действий, называется *числовым полем*. Слово „числовое“ мы будем опускать. Итак,  $K$  — поле, если  $0, 1 \in K$  и для любых  $a, b \in K$  верно  $a \pm b, ab \in K$  и  $a/b \in K$  при  $b \neq 0$ . Легко понять,  $\mathbb{Q}$  — поле,

причём „самое маленькое“ — любое поле его содержит<sup>1</sup>. Если поле  $K$  содержится в поле  $L$ , то говорят, что  $K$  — подполе в  $L$ . В этом параграфе все поля лежат в поле  $\mathbb{R}$  действительных чисел.

Числа  $x_1, \dots, x_n$  называются *линейно независимыми над полем  $K$* , если равенство  $a_1x_1 + \dots + a_nx_n = 0$ , где  $a_1, \dots, a_n \in K$ , выполняется только при  $a_1 = \dots = a_n = 0$ . Например, числа  $1$  и  $\sqrt{2}$  линейно независимы над  $\mathbb{Q}$ , но линейно зависимы над  $\mathbb{R}$  (равенство  $a_1 \cdot 1 + a_2\sqrt{2} = 0$  верно при  $a_1 = \sqrt{2}$  и  $a_2 = -1$ ).

**ЗАДАЧА 4.** Проверьте свойства линейной зависимости/независимости над произвольным полем  $K$ :

- а) система, содержащая  $0$  или два числа, отношение которых лежит в  $K$ , линейно зависима над  $K$ ;
- б) подсистема линейно независимой системы линейно независима;
- в) система  $1, x$  линейно независима над  $K$ , если и только если  $x \notin K$ ;
- г) коэффициенты  $a_1, \dots, a_n \in K$  в записи числа  $a_1x_1 + \dots + a_nx_n$  определены однозначно, если и только если система  $x_1, \dots, x_n$  линейно независима над  $K$ .

Наименьшее (по включению) поле, содержащее поле  $K$  и числа  $\alpha_1, \dots, \alpha_n$ , обозначается  $K(\alpha_1, \dots, \alpha_n)$  и называется полем, порожденным над  $K$  этими числами. Опишем поле, порожденное над  $K$  одним квадратным радикалом  $\sqrt{d} \notin K$ , где  $d \in K$ . Поле  $K(\sqrt{d})$ , очевидно, состоит из отношений чисел вида  $a+b\sqrt{d}$ , где  $a, b \in K$ . Но от иррациональности в знаменателе можно избавиться, умножив на *сопряжённое*  $a-b\sqrt{d}$ :  $\frac{1}{a+b\sqrt{d}} = \frac{a-b\sqrt{d}}{a^2-db^2}$  (как в примере 2). Значит,

$$K(\sqrt{d}) = \{a+b\sqrt{d} \mid a, b \in K\}.$$

**Пример 3.** Пусть  $p, q$  — различные простые числа. Аналогично примеру  $2 \sqrt{q} \notin \mathbb{Q}(\sqrt{p})$  и числа  $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$  линейно независимы над  $\mathbb{Q}$ . Поэтому

$$\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p})(\sqrt{q}) = \{a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq} \mid a, b, c, d \in \mathbb{Q}\},$$

причём запись чисел в таком виде однозначна.

**Пример 4.** Докажем, что числа на рисунке 2б линейно независимы над  $\mathbb{Q}$ . Пусть

$$a_1 + a_2\sqrt{2} + \dots + a_8\sqrt{30} = 0, \text{ где } a_1, a_2, \dots, a_8 \in \mathbb{Q}.$$

**Шаг 1.** Вынося  $\sqrt{5}$  за скобки, получим равенство вида  $A + B\sqrt{5} = 0$ , где  $A, B \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ :

$$\underbrace{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_5\sqrt{6}}_A + \underbrace{(a_4 + a_6\sqrt{2} + a_7\sqrt{3} + a_8\sqrt{6})\sqrt{5}}_B = 0. \quad (1)$$

Достаточно доказать, что  $A = B = 0$ . Тогда, согласно примеру 2,  $a_1 = a_2 = a_3 = a_5 = 0$  и  $a_4 = a_6 = a_7 = a_8 = 0$ .

**Шаг 2.** Надо доказать, что числа  $1$  и  $\sqrt{5}$  линейно независимы над полем  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . Это равносильно условию  $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$  (задача 4в).

**Шаг 3.** Предположим, что  $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , т. е., с учётом описания этого поля в примере 3,

$$\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \text{ где } a, b, c, d \in \mathbb{Q}. \quad (2)$$

Большое число радикалов может отбить желание возводить в квадрат. Однако это можно сделать по-умному, предварительно сгруппировав слагаемые одним из двух способов:

$$\underbrace{a+b\sqrt{2}}_C + \underbrace{(c+d\sqrt{2})\sqrt{3}}_D = \sqrt{5} = \underbrace{a+c\sqrt{3}}_{C'} + \underbrace{(b+d\sqrt{3})\sqrt{2}}_{D'}, \quad (3)$$

и «не тревожить»  $C, D, C', D'$ . Возведём в квадрат первое равенство:

$$C^2 + 3D^2 + 2CD\sqrt{3} = 5.$$

Так как числа  $1$  и  $\sqrt{3}$  линейно независимы над полем  $\mathbb{Q}(\sqrt{2})$ , то  $CD = 0$ . Аналогично  $C'D' = 0$ . Всего 4 варианта:  $C = C' = 0$ ,  $C = D' = 0$ ,  $C' = D = 0$  или  $D = D' = 0$ . Если  $C = C' = 0$ , то  $a = b = c = 0$ , поэтому  $\sqrt{5} = d\sqrt{6}$ , а это противоречит лемме 1. В других случаях получается аналогичное противоречие, так как в правой части равенства (2) остаётся лишь одно ненулевое слагаемое.

<sup>1</sup>Бывают и другие поля: поле вычетов  $\mathbb{Z}_p$ , поле рациональных функций и др. Любое поле содержит либо  $\mathbb{Q}$ , либо  $\mathbb{Z}_p$ .

**ЗАДАЧА 5.** Докажите теорему 2 при  $k = 2$ : сделайте шаг индукции от  $n - 1$  к  $n$ , следя примеру 4.

Прежде чем переходить к радикалам более высокой степени, обсудим, как можно было сделать последний шаг с прицелом на общий случай — без возведения в квадрат. Согласитесь, даже столь безобидное равенство как  $\sqrt[5]{3} = a + b\sqrt[5]{2}$  ( $a, b \in \mathbb{Q}$ ) едва ли удастся привести к противоречию любым возведением в пятую степень... Что если в равенствах (3) перейти к сопряжённым числам?

Назовём числа вида  $a \pm b\sqrt{d}$  над полем  $K$ , где  $a, b, d \in K$ ,  $\sqrt{d} \notin K$ , сопряжёнными. В равенствах (3) сопряжённым к числу  $C + D\sqrt{3}$  над полем  $\mathbb{Q}(\sqrt{2})$  будет  $C - D\sqrt{3}$ , а сопряжённым к числу  $C' + D'\sqrt{2}$  над полем  $\mathbb{Q}(\sqrt{3})$  будет  $C' - D'\sqrt{2}$ . В то же время сопряжённым к числу  $\sqrt{5}$  над обоими полями будет  $-\sqrt{5}$ . Раз числа равны, то равны и их сопряжённые:

$$C - D\sqrt{3} = -\sqrt{5} = C' - D'\sqrt{2}. \quad (4)$$

Отсюда и из (3) получаем  $C = C' = 0$ , что невозможно, как показано выше.

Увы, несмотря на кажущуюся строгость, это рассуждение содержит «дыру», однако его можно спасти. Логическая ошибка довольно тонкая, и читатель, который её обнаружит и исправит, вправе собой гордиться.

**ЗАДАЧА 6.** Почему переход от (3) к (4) не обоснован, и как его доказать?

Переход к сопряжённым часто бывает эффективен. Вот несколько олимпиадных задач на эту тему.

**ЗАДАЧА 7.** Существуют ли такие рациональные числа  $a, b, c, d$ , что  $(a + b\sqrt{2})^2 + (c + d\sqrt{2})^2 = 7 + 5\sqrt{2}$ ?

**ЗАДАЧА 8.** Найдите первые 1000 знаков после запятой в десятичной записи числа  $(6 + \sqrt{35})^{1000}$ .

**ЗАДАЧА 9.** Докажите, что произведение  $2^{100}$  чисел  $\pm\sqrt{1} \pm \sqrt{2} \pm \dots \pm \sqrt{99} \pm \sqrt{100}$  — полный квадрат.

### §3. Общий случай

Начнём доказывать теорему 2 при произвольном  $k$ , следя плану в примере 4. При этом на каждом шаге будут возникать новые трудности. Чем дальше в лес — тем больше дров.

**Шаг 1: отщепление последнего радикала.** Линейное соотношение над  $\mathbb{Q}$  (т. е. с коэффициентами из  $\mathbb{Q}$ ) девяти чисел на рисунке 2в можно записать в виде

$$f_0(\sqrt[3]{2}) + f_1(\sqrt[3]{2})\sqrt[3]{3} + f_2(\sqrt[3]{2})\sqrt[3]{9} = 0,$$

где  $f_0, f_1, f_2$  — многочлены степени меньше 3 над  $\mathbb{Q}$  (сгруппировали слагаемые как в (1)). Поэтому линейная независимость этих чисел будет следовать из двух фактов:

числа  $1, \sqrt[3]{3}, \sqrt[3]{9}$  линейно независимы над полем  $\mathbb{Q}(\sqrt[3]{2})$ ; (5)

числа  $1, \sqrt[3]{2}, \sqrt[3]{4}$  линейно независимы над полем  $\mathbb{Q}$ . (6)

В самом деле, из (5) получаем  $f_0(\sqrt[3]{2}) = f_1(\sqrt[3]{2}) = f_2(\sqrt[3]{2}) = 0$ , а тогда из (6) коэффициенты многочленов  $f_0, f_1, f_2$  — нулевые. Обобщим это рассуждение и покажем, что достаточно доказать **теорему 2'**: в обозначениях теоремы 2 числа  $1, r_n, \dots, r_n^{k-1}$  линейно независимы над полем  $\mathbb{Q}(r_1, \dots, r_{n-1})$ .

Пусть теорема 2' доказана. Докажем теорему 2 индукцией по  $n$ . При  $n = 1$  теоремы совпадают буквально:  $\mathbb{Q}(r_1, \dots, r_{n-1}) = \mathbb{Q}$ . Пусть  $n > 1$ . Переформулируем теорему 2: если  $F(x_1, \dots, x_n)$  — многочлен над  $\mathbb{Q}$ , имеющий по каждой переменной степень меньше  $k$ , и  $F(r_1, \dots, r_n) = 0$ , то  $F = 0$  (т. е. все коэффициенты многочлена  $F$  нулевые). Запишем  $F$  в виде

$$F(x_1, \dots, x_n) = f_0(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1})x_n + \dots + f_{k-1}(x_1, \dots, x_{n-1})x_n^{k-1}.$$

По условию  $F(r_1, \dots, r_n) = 0$ . По теореме 2' имеем  $f_j(r_1, \dots, r_{n-1}) = 0$  для всех  $j = 0, \dots, k-1$ . По предположению индукции  $f_0 = \dots = f_{n-1} = 0$ , т. е.  $F = 0$ .

**Шаг 2: «инородность» последнего радикала.** Пусть  $K$  — любое поле,  $r$  — такое число, что  $r^k \in K$ . Выясним, когда

$$\text{числа } 1, r, \dots, r^{k-1} \text{ линейно независимы над } K. \quad (7)$$

Иными словами,  $r$  не должно быть корнем многочлена степени меньше  $k$  с коэффициентами из  $K$ . При  $k = 2$  это просто означает, что  $r \notin K$  (задача 4в). При  $k > 2$  всё гораздо сложнее и интереснее.

**Немного теории.** Множество многочленов над полем  $K$  обозначается  $K[x]$ . Многочлен над  $K$  положительной степени, который не раскладывается в произведение многочленов меньших степеней, называется **неприводимым** над  $K$ . Многочлены над полем можно делить с остатком («уголком»).

Пусть число  $\alpha$  является корнем ненулевого многочлена над полем  $K$ , тогда оно называется *алгебраическим над  $K$* . Среди всех таких многочленов только один имеет наименьшую степень и старший коэффициент 1 (если бы их было два, то их разность была бы многочленом меньшей степени с корнем  $\alpha$ ). Он называется *минимальным многочленом* числа  $\alpha$  над  $K$ , и мы будем его обозначать  $\mu_\alpha^K(x)$  или  $\mu_\alpha(x)$ , если ясно, о каком поле  $K$  идёт речь. Степень этого многочлена есть наименьшее такое  $m \in \mathbb{N}$ , что числа  $1, \alpha, \dots, \alpha^m$  линейно зависимы над  $K$ . Вот основные свойства многочлена  $\mu_\alpha^K(x) = \mu_\alpha(x)$ :

- 1) многочлен  $\mu_\alpha(x)$  неприводим над  $K$ ;
- 2) любой многочлен из  $K[x]$  с корнем  $\alpha$  делится на  $\mu_\alpha(x)$ ;
- 3) неприводимый над  $K$  многочлен  $p(x)$  с корнем  $\alpha$  и старшим коэффициентом 1 равен  $\mu_\alpha(x)$ .

*Доказательство.* 1) Если многочлен  $\mu_\alpha$  раскладывается в произведение многочленов над  $K$  меньшей степени, то  $\alpha$  — корень одного из сомножителей, что противоречит минимальности степени  $\deg \mu_\alpha$ .

2) Пусть  $f \in K[x]$  и  $f(\alpha) = 0$ . Разделим  $f$  на  $\mu_\alpha$  с остатком:  $f = \mu_\alpha q + s$ , где  $q, s \in K[x]$  и либо  $s = 0$ , либо  $\deg s < \deg \mu_\alpha$ . Второй вариант нево возможен, так как  $s(\alpha) = f(\alpha) - \mu_\alpha(\alpha)q(\alpha) = 0$ .

3) По пункту 2)  $p(x)$  делится на  $\mu_\alpha(x)$ , а так как  $p(x)$  неприводим над  $K$ , то  $p(x)/\mu_\alpha(x) = c \in K$ . Поскольку старшие коэффициенты у  $p(x)$  и  $\mu_\alpha(x)$  равны 1, то  $c = 1$ .  $\square$

Таким образом, (7)  $\Leftrightarrow \mu_r^K(x) = x^k - r^k \Leftrightarrow$  двучлен  $x^k - r^k$  неприводим над  $K$ . Например, утверждения (5) и (6) равносильны соответственно неприводимости двучлена  $x^3 - 3$  над  $\mathbb{Q}(\sqrt[3]{2})$  и двучлена  $x^3 - 2$  над  $\mathbb{Q}$ , а это значит, что  $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$  и  $\sqrt[3]{2} \notin \mathbb{Q}$  (кубический многочлен неприводим над полем, если не имеет в нем корней). В общем случае условие «инородности»  $r \notin K$  необходимо, но не достаточно. Хотя в нашем случае действующие лица  $K$  и  $r$  лежат в поле  $\mathbb{R}$ , мы выйдем в комплексную плоскость — поле  $\mathbb{C}$ , где двучлен  $x^k - r^k$  раскладывается на линейные множители. По формуле Муавра [3]

$$x^k - r^k = (x - r)(x - r\varepsilon) \dots (x - r\varepsilon^{k-1}), \text{ где } \varepsilon = \varepsilon_k = \cos \frac{2\pi}{k} + i \sin \frac{2\pi}{k}. \quad (8)$$

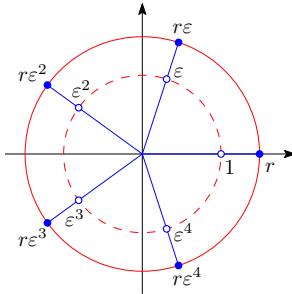


Рис. 3

**Лемма 2.** Пусть  $K$  — подполе в  $\mathbb{R}$ ,  $r \in \mathbb{R}$ ,  $r^k \in K$  и  $r, \dots, r^{k-1} \notin K$ . Тогда двучлен  $x^k - r^k$  неприводим над  $K$ .

*Доказательство.* Предположим, что двучлен  $x^k - r^k$  имеет делитель из  $K[x]$  степени  $l \in \{1, \dots, k-1\}$  и  $c$  — свободный член этого делителя. Из разложения (8) имеем  $c = (-r)^l \varepsilon^s$  для некоторого целого  $s$ . Поскольку  $c \in K \subseteq \mathbb{R}$ ,  $r \in \mathbb{R}$  и  $|\varepsilon^s| = 1$ , то  $r^l = \pm |c| \in K$ , что противоречит условию.  $\square$

*Замечание.* Для  $r \notin \mathbb{R}$  лемма неверна, например, при  $k=3$  и  $r=\varepsilon$  имеем  $\varepsilon, \varepsilon^2 \notin \mathbb{R}$ , но двучлен  $x^3 - 1$  приводим.

**Пример 5.** Для любого простого  $p$  и натурального  $k > 1$  имеем  $\sqrt[k]{p}, \dots, \sqrt[k]{p^{k-1}} \notin \mathbb{Q}$  (лемма 1), поэтому двучлен  $x^k - p$  неприводим над  $\mathbb{Q}$  (лемма 2)<sup>2</sup>, значит,  $\mu_{\sqrt[k]{p}}^\mathbb{Q}(x) = x^k - p$ .

Вообще, теорема 2' посредством леммы 2 сведена к **теореме 2''**: в тех же обозначениях

$$r_n, \dots, r_n^{k-1} \notin \mathbb{Q}(r_1, \dots, r_{n-1}). \quad (9)$$

При  $n=1$  это верно по лемме 1. Чтобы прийти к противоречию при  $n > 1$ , научимся записывать числа из  $\mathbb{Q}(r_1, \dots, r_{n-1})$  в виде многочленов от  $r_1, \dots, r_{n-1}$ . Например, условие  $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$  запишется в виде  $\sqrt[3]{3} \neq a + b\sqrt[3]{2} + c\sqrt[3]{4}$  при  $a, b, c \in \mathbb{Q}$ .

**Шаг 3: избавление от иррациональности в знаменателе.** Пресловутое «домножение на сопряжённое» работает лишь с квадратными радикалами. Как действовать при  $k > 2$ , сначала покажем на примере.

<sup>2</sup>В [5] линейная независимость чисел  $1, \sqrt[k]{p}, \dots, \sqrt[k]{p^{k-1}}$  также сведена к неприводимости двучлена  $x^k - p$ , установленной по признаку Эйзенштейна.

**Пример 6.** Избавимся от иррациональности в знаменателе дроби  $\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3}$ . Обозначим  $r = \sqrt[3]{2}$  и  $f(x) = x^2 + x + 3$ . Надо найти такой многочлен  $u \in \mathbb{Q}[x]$ , что  $\frac{1}{f(r)} = u(r)$ . Это значит, что многочлен  $f(x)u(x) - 1$  имеет корень  $r$ , а тогда делится на  $\mu_r^{\mathbb{Q}}(x) = x^3 - 2$  (пример 5). Таким образом,

$$u(x)f(x) + v(x)(x^3 - 2) = 1.$$

для некоторого многочлена  $v \in \mathbb{Q}[x]$ . Многочлены  $u$  и  $v$  найдём с помощью алгоритма Евклида:

Алгоритм Евклида	Обратный ход алгоритма Евклида
$x^3 - 2 = (x^2 + x + 3)(x - 1) - 2x + 1$	$\frac{15}{4} = f(x) - (f(x)(x - 1) - (x^3 - 2)) \left(\frac{1}{2}x + \frac{3}{4}\right) =$
$x^2 + x + 3 = (2x - 1) \left(\frac{1}{2}x + \frac{3}{4}\right) + \frac{15}{4}$	$= (x^3 - 2) \left(\frac{1}{2}x + \frac{3}{4}\right) + f(x) \left(-\frac{1}{2}x^2 - \frac{1}{4}x + \frac{7}{4}\right)$

Итак,  $(2x^2 + x - 7)(x^2 + x + 3) - (2x + 3)(x^3 - 2) = -15$ , откуда при  $x = r$  получаем

$$\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3} = \frac{7 - \sqrt[3]{2} - 2\sqrt[3]{4}}{15}.$$

Докажем теперь общее утверждение, следуя разобранному примеру.

**Лемма 3** (об избавлении от иррациональности в знаменателе). *Если число  $\alpha$  алгебраично над полем  $K$  и  $\deg \mu_{\alpha}(x) = k$ , то каждое число в поле  $K(\alpha)$  однозначно записывается в виде*

$$c_0 + c_1\alpha + \dots + c_{k-1}\alpha^{k-1}, \text{ где } c_0, c_1, \dots, c_{k-1} \in K. \quad (10)$$

*Доказательство.* Числа такого вида лежат в  $K(\alpha)$ , поэтому надо проверить, что они сами образуют поле. Замкнутость относительно сложения, вычитания и умножения очевидна. Пусть  $f \in K[x]$  и  $f(\alpha) \neq 0$ . Тогда  $f(x)$  не делится на  $\mu_{\alpha}(x)$ , а потому эти многочлены взаимно просты. По алгоритму Евклида найдутся такие многочлены  $u, v \in K[x]$ , что  $u(x)f(x) + v(x)\mu_{\alpha}(x) = 1$ . При  $x = \alpha$  получим  $1/f(\alpha) = u(\alpha)$ , что преобразуется к виду (10) заменой  $u$  его остатком от деления на  $\mu_{\alpha}$ . Коэффициенты  $c_i$  определены однозначно, иначе  $\alpha$  был бы корнем многочлена степени меньше  $k$ .  $\square$

**ЗАДАЧА 10.** Избавьтесь от иррациональности в знаменателях: а)  $\frac{1}{1 + \sqrt{2} - \sqrt{3} + \sqrt{6}}$ ; б)  $\frac{1}{\sqrt[4]{27} + 2\sqrt[4]{3} - 1}$ .

Вернёмся к доказательству теоремы 2''. По предположению индукции двучлен  $x^k - r_1^k$  неприводим над  $\mathbb{Q}$ , двучлен  $x^k - r_2^k$  — над  $\mathbb{Q}(r_1), \dots$ , двучлен  $x^k - r_{n-1}^k$  — над  $\mathbb{Q}(r_1, \dots, r_{n-2})$ . Последовательно избавляясь от иррациональности в знаменателе, представим каждое число из  $\mathbb{Q}(r_1, \dots, r_{n-1})$  однозначно в виде суммы чисел вида

$$ar_1^{l_1} \dots r_{n-1}^{l_{n-1}}, \text{ где } a \in \mathbb{Q}, 0 \leq l_1, \dots, l_{n-1} < k. \quad (11)$$

Пусть (9) неверно, т. е.  $r_n^l$  при некотором  $l \in \{1, \dots, k-1\}$  равно сумме чисел вида (11). В этой сумме должно быть больше одного слагаемого, иначе  $r_n^l / (r_1^{l_1} \dots r_{n-1}^{l_{n-1}}) = a \in \mathbb{Q}$ , что противоречит лемме 1. Значит, какой-то из радикалов  $r_1, \dots, r_{n-1}$  встречается в двух слагаемых в разных степенях, пусть это  $r_{n-1}$ . Итак,

$$r_n^l = A_0 + A_1 r_{n-1} + \dots + A_{k-1} r_{n-1}^{k-1}, \quad (12)$$

где среди  $A_0, \dots, A_{k-1} \in \mathbb{Q}(r_1, \dots, r_{n-2})$  хотя бы два ненулевых. Самое интересное наступает в этот момент — трудность по сравнению со случаем  $k=2$  возрастает ещё больше. И вправду, при  $k=2$  равенство (12) совсем не страшно:  $\sqrt{p_n} = A_0 + A_1 \sqrt{p_{n-1}}$  и без труда возводится в квадрат. Но при  $k>2$  о возведении (12) в  $k$ -ю степень даже думать не хочется... На помощь вновь приходят минимальные многочлены. Но если для левой части минимальный многочлен найти легко, то для правой не очевидна даже алгебраичность.

**Пример 7.** Приведём к противоречию упомянутое выше равенство  $\sqrt[5]{3} = a + b\sqrt[5]{2}$ , где  $a, b \in \mathbb{Q}$ , — частный случай (12). По лемме 1  $a \neq 0$  и  $b \neq 0$ . Согласно примеру 5,  $\mu_{\sqrt[5]{3}}(x) = x^5 - 3$  и  $\mu_{\sqrt[5]{2}}(x) = x^5 - 2$ , а тогда  $\mu_{a+b\sqrt[5]{2}}(x) = (x-a)^5 - 2b^5$  (сделали линейную замену  $x \mapsto \frac{x-a}{b}$  и умножили на  $b^5$ ). Получаем противоречие:

$$x^5 - 3 = (x-a)^5 - 2b^5 = x^5 - 5ax^4 + \dots \implies a = 0.$$

**Задача 11.** Решите уравнение в натуральных числах:  $\sqrt[5]{m} + \sqrt[5]{n} = 2021$ .

**Задача 12.** Опровергните равенство  $\sqrt[6]{3} = a\sqrt[3]{2} + b\sqrt{2}$ , где  $a, b \in \mathbb{Q}$ .

В общем случае путь к минимальному многочлену правой части равенства (12) лежит через *сопряжённые числа*. Вот только что такое, мы определили пока лишь для квадратичных иррациональностей, и в конце §2 наметили рассуждение с переходом к сопряжённым.

**Ещё немного теории.** Пусть число  $\alpha \in \mathbb{C}$  алгебраично над полем  $K$  и

$$\mu_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_k)$$

(согласно основной теореме алгебры любой многочлен над  $\mathbb{C}$  раскладывается на линейные множители<sup>3</sup>). Числа  $\alpha_1, \dots, \alpha_k$  называются *сопряжёнными с  $\alpha$  над  $K$* . Обозначим их сумму  $\sigma(\alpha)$ . По теореме Виета

$$\sigma(\alpha) = \alpha_1 + \dots + \alpha_k \iff \mu_\alpha(x) = x^k - \sigma(\alpha)x^{k-1} + \dots \quad (13)$$

Пример (7) показывает, что именно коэффициент  $-\sigma(\alpha)$  будет играть ключевую роль.

*Замечание.* Числа  $\alpha_1, \dots, \alpha_k$  различны (для доказательства это не нужно): если  $\mu_\alpha(x) = (x - \alpha_j)^2 g(x)$ , то производная  $\mu'_\alpha(x) = 2(x - \alpha_j)g(x) + (x - \alpha_j)^2 g'(x) \in K[x]$  имеет корень  $\alpha_j$ , хотя  $\deg \mu'_\alpha < \deg \mu_\alpha$ .

Ввиду свойства 3) минимального многочлена все алгебраические над  $K$  числа разбиваются на классы сопряжённых, каждый из которых состоит из корней какого-то неприводимого над  $K$  многочлена.

**Пример 8.** Разложим двучлен  $x^4 - 2$  на неприводимые и разобъём его корни на классы сопряжённых над каждым из полей  $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ :

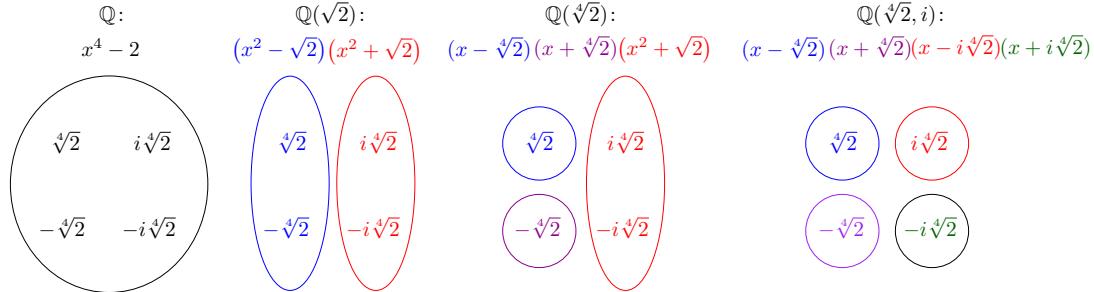


Рис. 4

**Пример 9.** Для квадратичных иррациональностей  $a \pm b\sqrt{d}$  ( $a, b \in K, b \neq 0, \sqrt{d} \notin K$ ) данное определение согласовано с привычным понятием сопряжённости:

$$\mu_{a \pm b\sqrt{d}}^K(x) = x^2 - 2ax + a^2 - db^2, \quad \sigma(a \pm b\sqrt{d}) = 2a.$$

(Кстати, при  $K = \mathbb{R}$  и  $d = -1$  получаем комплексно-сопряжённые числа  $a \pm bi$ .) Это спасает приведённое выше обоснование перехода от (3) к (4).

**Пример 10.** Пусть  $a, b \in \mathbb{Q}$ ,  $b \neq 0$ . Числа  $a \pm b\sqrt[5]{2}$ , конечно, не будут сопряжёнными при  $k > 2$  (по аналогии с квадратичными иррациональностями). Сопряжённые с числом  $a + b\sqrt[5]{2}$  суть корни многочлена  $\mu_{a+b\sqrt[5]{2}}(x) = (x - a)^5 - 2b^5$  (аналогично примеру 7), т. е. числа  $a + b\sqrt[5]{2}\varepsilon^j$ ,  $j = 0, \dots, k - 1$  (пример на рис. 5). Знак  $\pm$  при  $k = 2$  объясняется тем, что  $\varepsilon_2 = -1$ .

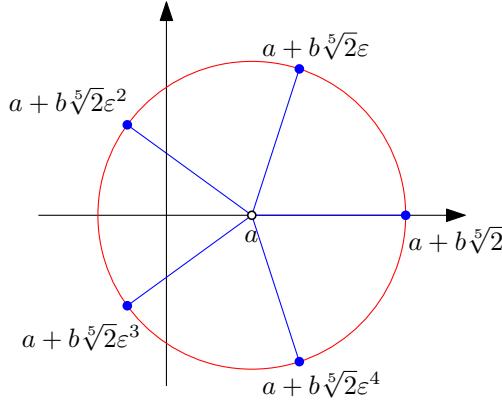


Рис. 5

<sup>3</sup>Мы этим пользоваться не будем: в доказательстве все многочлены раскладываются явно.

**Лемма 4.** Пусть  $K$  — подполе в  $\mathbb{R}$ ,  $r \in \mathbb{R}$ ,  $r \notin K$ ,  $r^k \in K$  для некоторого  $k \in \mathbb{N}$ . Тогда  $\sigma(r) = 0$ .

**Доказательство.** Существует наименьшее  $m \in \mathbb{N}$ , такое что  $r^m \in K$ . По лемме 2 двучлен  $x^m - r^m$  неприводим над  $K$ , а значит, равен  $\mu_r^K(x)$ . Так как  $r \notin K$ , то  $m > 1$  и  $\sigma(r) = 0$ .  $\square$

**Шаг 4: переход к сопряжённым числам.** Пример 10 подсказывает вид сопряжённых к числу вида (10).

**Пример 11.** Опровергнем равенство  $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ , где  $a, b, c \in \mathbb{Q}$ . Сопряжённые с левой частью суть  $\sqrt[3]{3}$ ,  $\sqrt[3]{3}\varepsilon$ ,  $\sqrt[3]{3}\varepsilon^2$ , где  $\varepsilon = \varepsilon_3$ . С другой стороны, рассмотрим многочлен

$$F(x) = (x - (a + b\sqrt[3]{2} + c\sqrt[3]{4})) (x - (a + b\sqrt[3]{2}\varepsilon + c\sqrt[3]{4}\varepsilon^2)) (x - (a + b\sqrt[3]{2}\varepsilon^2 + c\sqrt[3]{4}\varepsilon)).$$

Как показать, что  $F(x) \in \mathbb{Q}[x]$ , не портя настроение раскрытием скобок? Чистая алгебра: заменим  $\sqrt[3]{2}$  на  $y$  и  $\sqrt[3]{4}$  на  $y^2$ . Получим многочлен, не меняющийся при подстановке  $y\varepsilon$  вместо  $y$ , а значит,  $y$  в него входит только в степенях, кратных 3. Заменяя  $y^3$  на 2, получим многочлен  $F(x) \in \mathbb{Q}[x]$ . Следовательно,  $F(x)$  делится на  $\mu_{\sqrt[3]{3}}(x) = x^3 - 3$ , отсюда  $F(x) = x^3 - 3$ . Но сумма корней многочлена  $F$  равна  $3a$  (так как  $1 + \varepsilon + \varepsilon^2 = 0$ ). Значит,  $a = 0$  и  $\sqrt[3]{3} = b\sqrt[3]{2} + c\sqrt[3]{4}$ . Поделим на  $\sqrt[3]{2}$ :  $\sqrt[3]{3}/\sqrt[3]{2} = b + c\sqrt[3]{2}$ . Аналогично или как в примере 7 получим  $b = 0$ . Значит,  $\sqrt[3]{3} = c\sqrt[3]{4}$ , что невозможно по лемме 1.

**Лемма 5.** Пусть  $\alpha_1 = \alpha, \dots, \alpha_k$  — все сопряжённые с числом  $\alpha$ , алгебраичны над полем  $K$ , и  $f \in K[x]$ . Тогда число  $f(\alpha)$  алгебраично над  $K$  и для некоторого  $d \in \mathbb{N}$

$$\mu_{f(\alpha)}(x)^d = (x - f(\alpha_1)) \dots (x - f(\alpha_k)). \quad (14)$$

**Доказательство.** для наших целей достаточно провести в случае  $\mu_\alpha(x) = x^k - r^k$ , где  $r = \alpha$ . Равенство (14) примет вид

$$\mu_{f(r)}(x)^d = (x - f(r))(x - f(r\varepsilon)) \dots (x - f(r\varepsilon^{k-1})). \quad (15)$$

1. Рассмотрим вспомогательный многочлен

$$G(x, y) = (x - f(y))(x - f(y\varepsilon)) \dots (x - f(y\varepsilon^{k-1})).$$

Он не меняется при замене  $y$  на  $y\varepsilon$  (скобки сдвигаются по циклу), а потому все входящие в него степени  $y$  кратны  $k$ . Поэтому  $G(x, r)$  — многочлен с коэффициентами из  $K$  и корнем  $f(r)$ . Значит, число  $f(r)$  алгебраично над  $K$  и  $\mu_{f(r)}(x)$  делит  $G(x, r)$ .

2. Многочлен  $\mu_{f(r)}(f(x)) \in K[x]$  имеет корень  $r$ , а потому делится на многочлен  $\mu_r(x) = x^k - r^k$ . Значит, все корни  $r, r\varepsilon, \dots, r\varepsilon^{k-1}$  этого двучлена являются корнями многочлена  $\mu_{f(r)}(f(x))$ , т. е. числа  $f(r), f(r\varepsilon), \dots, f(r\varepsilon^{k-1})$  сопряжены.

3. Пусть  $d \in \mathbb{N}$  — наименьшее такое число, что  $\mu_{f(r)}(x)^d$  делит  $G(x, r)$ . Докажем, что  $G(x, r) = \mu_{f(r)}(x)^d$ . Действительно, в противном случае многочлен  $G(x, r)/\mu_{f(r)}(x)^d \in K[x]$  имеет некоторый корень  $f(r\varepsilon^j)$ , а значит, делится на  $\mu_{f(r\varepsilon^j)}(x) = \mu_{f(r)}(x)$ , что противоречит минимальности  $d$ .

Для доказательства в общем случае рассмотрим многочлен

$$G(x, y_1, \dots, y_k) = (x - f(y_1)) \dots (x - f(y_k)).$$

Он не меняется при перестановках  $y_1, \dots, y_k$  и по основной теореме о симметрических многочленах [1, стр. 134] выражается через  $x$  и элементарные симметрические многочлены  $\sigma_1, \dots, \sigma_k$ , определяемые равенством  $(x - y_1) \dots (x - y_k) = x^k - \sigma_1 x^{k-1} + \sigma_2 x^{k-2} - \dots + (-1)^k \sigma_k$ . Поскольку  $(x - \alpha_1) \dots (x - \alpha_k) = \mu_\alpha(x) \in K[x]$ , то  $G(x, \alpha_1, \dots, \alpha_k) \in K[x]$ . Последующие рассуждения аналогичны.  $\square$

Приравняем суммы корней (с кратностями) многочленов в равенстве (15):

$$d\sigma(f(r)) = f(r) + f(r\varepsilon) + \dots + f(r\varepsilon^{k-1}).$$

Сосчитаем правую часть для  $f(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}$ :

$$\begin{aligned} f(r) &= c_0 + c_1r + \dots + c_{k-1}r^{k-1}, \\ f(r\varepsilon) &= c_0 + c_1r\varepsilon + \dots + c_{k-1}r^{k-1}\varepsilon^{k-1}, \\ &\dots \\ f(r\varepsilon^{k-1}) &= c_0 + c_1r\varepsilon^{k-1} + \dots + c_{k-1}r^{k-1}\varepsilon^{(k-1)^2}. \end{aligned}$$

Сложим числа в каждом столбике. Так как  $\varepsilon^k = 1$ , то

$$1 + \varepsilon^j + \varepsilon^{2j} + \dots + \varepsilon^{(k-1)j} = \frac{1 - \varepsilon^{kj}}{1 - \varepsilon^j} = 0, \quad j = 1, \dots, k-1.$$

Значит,  $f(r) + f(r\varepsilon) + \dots + f(r\varepsilon^{k-1}) = kc_0$ , откуда

$$\sigma(c_0 + c_1r + \dots + c_{k-1}r^{k-1}) = \frac{k}{d} \cdot c_0. \quad (16)$$

Наконец мы готовы привести равенство (12) к противоречию. Пусть  $A_j$  — первый ненулевой коэффициент в ряду  $A_0, \dots, A_{k-1}$ . Разделим равенство (12) на  $r_{n-1}^j$ :

$$\frac{r_n^l}{r_{n-1}^j} = A_j + A_{j+1}r_{n-1} + \dots + A_{k-1}r_{n-1}^{k-j-1}. \quad (17)$$

Пусть  $K = \mathbb{Q}(r_1, \dots, r_{n-2})$ ,  $R = r_n^l/r_{n-1}^j$ . Тогда  $R \notin K$ , иначе  $R = A_j$  и  $A_{j+1} = \dots = A_{k-1} = 0$  ввиду линейной независимости  $1, r_{n-1}, \dots, r_{n-1}^{k-1}$  над  $K$  (напомним, среди чисел  $A_j, \dots, A_{k-1}$  хотя бы два ненулевых). При этом  $R^k = p_n^l/p_{n-1}^j \in \mathbb{Q}$ , поэтому  $\sigma(R) = 0$  по лемме 4. В то же время значение  $\sigma$  от правой части (17), согласно (16), пропорционально  $A_j$  (играющего роль  $c_0$ ), а потому не равно 0. Полученное противоречие доказывает теорему 2.

Фактически мы доказали большее: каждое число в поле  $\mathbb{Q}(r_1, \dots, r_n)$  представляется в виде линейной комбинации  $k^n$  чисел

$$r_1^{l_1} \dots r_n^{l_n}, \text{ где } 0 \leq l_1, \dots, l_n < k,$$

с однозначно определёнными рациональными коэффициентами. На языке векторов, эти числа образуют базис поля  $\mathbb{Q}(r_1, \dots, r_n)$  над  $\mathbb{Q}$ . Такое представление достигается избавлением от иррациональности в знаменателе, а однозначность коэффициентов равносильна линейной независимости данной системы.

### Короткое доказательство с помощью следа

Используя чуть больше сведений об алгебраических числах, либо владея начальными линейной алгебры, можно совсем коротко доказать теорему 1 (не сводя её к теореме 2). В основе рассуждения также лежит некоторая величина, пропорциональная сумме сопряжённых. Но при этом она обладает замечательным свойством линейности, благодаря чему техника сводится к минимуму.

Функция  $f: L \rightarrow \mathbb{C}$ , где  $L$  — подполе в  $\mathbb{C}$ , называется *линейной* (точнее,  $\mathbb{Q}$ -линейной), если  $f(ax+by) = af(x)+bf(y)$  для всех  $x, y \in L$  и  $a, b \in \mathbb{Q}$ . Пусть  $L = \mathbb{Q}(\sqrt[k]{Q_1}, \dots, \sqrt[k]{Q_N})$ . В §4 мы покажем, что существует линейная функция  $\text{tr}: L \rightarrow \mathbb{C}$ , называемая следом (от англ. trace — след), такая что

$$\text{для каждого } \alpha \in L \text{ найдётся такое } d \in \mathbb{N}, \text{ что } \text{tr}(\alpha) = d\sigma(\alpha) \quad (18)$$

( $\sigma(\alpha)$  определено в (13)). Предположим, что  $a_1\sqrt[k]{Q_1} + \dots + a_N\sqrt[k]{Q_N} = 0$ , где  $a_1, \dots, a_N \in \mathbb{Q}$  не все равны 0. Будем считать, что  $a_N \neq 0$ . Неожиданным образом уединим не радикал, а коэффициент. Разделим обе части на  $\sqrt[k]{Q_N}$  и обозначим  $R_i = \sqrt[k]{Q_i}/\sqrt[k]{Q_N}$ ,  $i = 1, \dots, N-1$ :

$$-a_N = a_1R_1 + \dots + a_{N-1}R_{N-1}. \quad (19)$$

Так как  $R_i^{k_N} \in \mathbb{Q}$  и по условию  $R_i \notin \mathbb{Q}$ , то  $\sigma(R_i) = 0$  по лемме 4, а тогда  $\text{tr}(R_i) = 0$  в силу (18). Отсюда в силу линейности след от правой части равенства (19) равен 0. В то же время  $\sigma(-a_N) = -a_N \neq 0$  и по (18)  $\text{tr}(-a_N) \neq 0$ . Это противоречие завершает доказательство теоремы 1.

### §4. Дополнение про след

Мы построим функцию след  $\text{tr}: L \rightarrow L$  для любого расширения  $L \supseteq \mathbb{Q}$ , порожденного конечным числом алгебраических чисел, в частности, для  $L = \mathbb{Q}(\sqrt[k]{Q_1}, \dots, \sqrt[k]{Q_N})$ . Сделаем это двумя способами. Начиём с того, который более соответствует рассуждению в §3 и обогащает его, переводя на язык теории Галуа. Затем мы дадим основное определение следа, объясняющее, кстати, его название. На этом пути нам понадобятся начальные сведения из линейной алгебры:

- базис и размерность расширения, теорема о башне [4, §5];
- операции над матрицами, обратная матрица [1, с. 41–44, 73];
- матрица линейного оператора в базисе, её преобразование при смене базиса [1, с. 234–236].

#### I подход (в духе теории Галуа)

Нам нужен хорошо известный факт [4, теорема 2]: *множество  $\mathbb{A}$  алгебраических (над  $\mathbb{Q}$ ) чисел является полем*. Отсюда  $L \subseteq \mathbb{A}$ , так как  $L$  порождено над  $\mathbb{Q}$  алгебраическими числами.

Назовём отображение  $\varphi: L \rightarrow \mathbb{C}$  *вложением*, если  $\varphi(a + b) = \varphi(a) + \varphi(b)$ ,  $\varphi(ab) = \varphi(a)\varphi(b)$  для всех  $a, b \in L$  и  $\varphi(c) = c$  при  $c \in \mathbb{Q}$ . В частности,  $\varphi$  линейно:  $\varphi(ca) = \varphi(c)\varphi(a) = c\varphi(a)$  при  $c \in \mathbb{Q}$  и  $a \in L$ . Ниже мы покажем, что существует лишь конечное число вложений  $\varphi_1, \dots, \varphi_n$  поля  $L$ . Определим

$$\text{tr}(\alpha) = \sum_{j=1}^n \varphi_j(\alpha). \quad (20)$$

**ЗАДАЧА 13.** Не читая далее, а) докажите, что все вложения  $\mathbb{Q}(i) \rightarrow \mathbb{C}$  суть  $a + bi \mapsto a \pm bi$  ( $a, b \in \mathbb{Q}$ ); б) опишите все вложения  $\mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right) \rightarrow \mathbb{C}$ . Найдите  $\text{tr}(1 + i)$  в каждом из пунктов.

Вложения открывают новый взгляд на сопряжённые числа, которые прежде мы характеризовали в терминах корней неприводимых многочленов. Пусть  $\alpha \in L$  и

$$\mu_\alpha(x) = x^m - c_{m-1}x^{m-1} - \dots - c_1x - c_0. \quad (21)$$

Применив любое вложение  $\varphi: L \rightarrow \mathbb{C}$  к обеим частям равенства  $\mu_\alpha(\alpha) = 0$ :

$$\varphi(\mu_\alpha(\alpha)) = \varphi(\alpha)^m - c_{m-1}\varphi(\alpha)^{m-1} - \dots - c_1\varphi(\alpha) - c_0 = \mu_\alpha(\varphi(\alpha)) = \varphi(0) = 0,$$

получим, что  $\varphi(\alpha)$  сопряжено с  $\alpha$ . Обратно, пусть  $\alpha_j$  — любое сопряжённое с  $\alpha \in L$ . Существует ли вложение  $L \rightarrow \mathbb{C}$ , переводящее  $\alpha$  в  $\alpha_j$ ? Такое вложение должно задаваться в поле  $\mathbb{Q}(\alpha)$  правилом  $f(\alpha) \mapsto f(\alpha_j)$ , где  $f \in \mathbb{Q}[x]$  (по теореме 3 всякое число из  $\mathbb{Q}(\alpha)$  имеет такой вид). С другой стороны, это правило корректно (не зависит от выбора многочлена  $f$ ) и задаёт вложение  $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ , так как для всех  $f, g \in \mathbb{Q}[x]$ :

$$\begin{aligned} f(\alpha) = g(\alpha) &\Leftrightarrow f(x) - g(x) \mid \mu_\alpha(x) \Leftrightarrow f(\alpha_j) = g(\alpha_j), \\ f(\alpha) + g(\alpha) &= (f + g)(\alpha), \quad f(\alpha)g(\alpha) = (fg)(\alpha). \end{aligned}$$

Не очевидно, впрочем, что это вложение продолжается с  $\mathbb{Q}(\alpha)$  на  $L$ , но во всяком случае уже можно описать вложения *простых* расширений поля  $\mathbb{Q}$  (порождённых одним числом).

**Теорема 3.** Пусть  $\theta_1 = \theta, \dots, \theta_n$  — все сопряжённые с  $\theta \in \mathbb{A}$ . Тогда все вложения  $\mathbb{Q}(\theta) \rightarrow \mathbb{C}$  суть

$$\varphi_j: f(\theta) \mapsto f(\theta_j) \quad (f \in \mathbb{Q}[x]), \quad j = 1, \dots, n.$$

К счастью, расширение, порождённое конечным числом алгебраических чисел, порождается одним числом (т. н. *примитивный элемент*).

**Пример 12.** Покажем, что  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . Включение  $\supseteq$  очевидно. Обратно,

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \ni \frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \implies \mathbb{Q}(\sqrt{2} + \sqrt{3}) \ni \frac{\sqrt{3} + \sqrt{2}}{2} \pm \frac{\sqrt{3} - \sqrt{2}}{2} = \sqrt{3}, \sqrt{2}.$$

**Теорема 4** (о примитивном элементе). *Существует такое  $\theta \in L$ , что  $L = \mathbb{Q}(\theta)$ .*

*Доказательство.* Достаточно для данных  $\alpha, \beta \in L$  найти такое  $\theta = \alpha + c\beta \in L$ , что  $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$  (далее — индукция по числу порождающих). Пусть  $\alpha = \alpha_1, \dots, \alpha_m$  и  $\beta = \beta_1, \dots, \beta_n$  — все сопряжённые с  $\alpha$  и  $\beta$ . Общие корни многочленов  $\mu_\beta(x)$  и  $\mu_\alpha(\theta - cx)$  — такие  $\beta_j$ , что  $\theta - c\beta_j = \alpha_i$  для некоторого  $i$ . Подберём  $c$  так, чтобы  $\alpha + c\beta \neq \alpha_i + c\beta_j$  при  $(i, j) \neq (1, 1)$ . Тогда  $\beta$  — единственный корень указанных многочленов и с учётом отсутствия у многочлена  $\mu_\beta(x)$  кратных корней (замечание после (13))

$$(\mu_\beta(x), \mu_\alpha(\theta - cx)) = x - \beta \in \mathbb{Q}(\theta)[x].$$

Итак,  $\beta \in \mathbb{Q}(\theta)$ , откуда  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ . □

На практике бывает проще работать с несколькими порождающими, но более просто устроеными.

**ЗАДАЧА 14.** Опишите все вложения полей  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ,  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ ,  $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ .

Докажем, что функция (20) обладает требуемыми свойствами. Линейность следа вытекает из линейности вложений. Докажем (18). Пусть  $\alpha \in L$ . По теореме 4  $\alpha = f(\theta)$ , где  $f \in \mathbb{Q}[x]$ . Далее  $\varphi_j(\alpha) = \varphi_j(f(\theta)) = f(\varphi_j(\theta))$ , что по теореме 3 равно  $f(\theta_j)$ . Итак,

$$\prod_{j=1}^n (x - \varphi_j(\alpha)) = \prod_{j=1}^n (x - f(\theta_j)) \stackrel{\text{теор. 5}}{=} \mu_{f(\theta)}(x)^d = \mu_\alpha(x)^d, \quad d \in \mathbb{N}. \quad (22)$$

Приравняв суммы корней (с кратностями) многочленов в левой и правой частях, получим (18).

## II подход (только линейная алгебра)

След  $\text{tr } A$  квадратной матрицы  $A = (a_{ij})$  — это сумма её диагональных элементов,  $\text{tr } A = \sum_i a_{ii}$ . Непосредственно проверяется, что  $\text{tr}(AB) = \text{tr}(BA)$  для матриц  $A$  и  $B$  одного размера. Отсюда следует, что след матрицы оператора не зависит от выбора базиса:  $\text{tr}(C^{-1}AC) = \text{tr}(C^{-1}CA) = \text{tr}(A)$ . Он называется следом этого оператора.

Из [4, теоремы 8 и 9] следует, что расширения, порождённые конечным числом алгебраических элементов, — это в точности конечные расширения, т. е. расширения конечной размерности. (Кстати, это ещё один способ понять, почему  $\mathbb{A}$  — поле.) Степень конечного расширения  $L \supseteq K$  обозначается  $[L : K]$ . Итак, пусть  $L \supseteq \mathbb{Q}$  — любое конечное расширение,  $L \subset \mathbb{C}$ . Пусть  $\alpha \in L \subset \mathbb{C}$ . След линейного оператора  $L \rightarrow L$ ,  $x \mapsto \alpha x$ , называется следом числа  $\alpha$  и обозначается  $\text{tr}_{\mathbb{Q}}^L(\alpha)$  или  $\text{tr}(\alpha)$ , если расширение  $L \supseteq \mathbb{Q}$  фиксировано.

**Пример 13.** Матрица умножения на  $\sqrt[3]{2}$  в базисе  $1, \sqrt[3]{2}, \sqrt[3]{4}$  расширения  $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$  есть  $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$ , так как  $1 \mapsto \sqrt[3]{2} \mapsto \sqrt[3]{4} \mapsto 2$ . Следовательно,  $\text{tr}(\sqrt[3]{2}) = \text{tr } A = 0$ .

Ясно, что  $\text{tr}(\alpha)$  линейно зависит от  $\alpha$ . Уточним смысл множителя  $d$  в (18) и докажем формулу

$$\boxed{\text{tr}(\alpha) = [L : \mathbb{Q}(\alpha)]\sigma(\alpha), \alpha \in L.} \quad (23)$$

Для этого выберем удобный базис в  $L/\mathbb{Q}$ . Сохраним обозначение (21). Тогда  $1, \alpha, \dots, \alpha^{m-1}$  — базис в  $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$ . Возьмём любой базис  $e_1, \dots, e_d$  в расширении  $L \supseteq \mathbb{Q}(\alpha)$ . По [4, теорема 9 о башне]

$$\underbrace{e_1, e_1\alpha, \dots, e_1\alpha^{m-1}}_{\text{1-й блок}}, \dots, \underbrace{e_d, e_d\alpha, \dots, e_d\alpha^{m-1}}_{\text{d-й блок}}$$

— базис в  $L \supseteq \mathbb{Q}$ . Векторы  $i$ -го блока при умножении на  $\alpha$  преобразуются внутри блока по правилу

$$e_i \mapsto e_i\alpha \mapsto e_i\alpha^2 \mapsto \dots \mapsto e_i\alpha^{m-1} \mapsto e_i\alpha^m = e_i(c_0 + c_1\alpha + \dots + c_{m-1}\alpha^{m-1}).$$

Поэтому в этом базисе матрица умножения на  $\alpha$  блочно-диагональная с  $d$  одинаковыми блоками

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & c_{m-2} \\ 0 & 0 & 0 & \dots & 1 & c_{m-1} \end{pmatrix}$$

и её след равен  $dc_{m-1}$ . Так как  $d = [L : \mathbb{Q}(\alpha)]$  и  $c_{m-1} = \sigma(\alpha)$ , то формула (23) доказана. Заметим, что она также следует из (22):

$$d = \frac{n}{\deg \mu_\alpha(x)} = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = [L : \mathbb{Q}(\alpha)].$$

Поэтому два данных определения следа эквивалентны.

В заключение отметим, что  $\mu_\alpha(x)$  — это минимальный многочлен оператора умножения на  $\alpha$ , а  $\mu_\alpha(x)^d$  — его характеристический многочлен.

## Список литературы

- [1] Э. Б. Винберг. Курс алгебры. МЦНМО, 2019.
- [2] Л. Камнев. Иррациональность суммы радикалов. Квант, 1972, №2.
- [3] А. Канунников. Алгебра и геометрия комплексных чисел. Квант, 2017, №5, 6.
- [4] А. Л. Канунников. Алгебраические числа как векторы. // Математическое просвещение. Сер. 3. Вып. 26. М.: МЦНМО. 2020. С. 91–122.

- [5] В. Олейников. Иррациональность и неприводимость. // Квант, 1986, №10.
- [6] В. А. Уфнаровский. Математический аквариум. МЦНМО, 2010.
- [7] I. Richards. An Application of Galois Theory to Elementary Arithmetic. Advances in Mathematics 13, p. 268–273. 1974.

## Решения задач

**1.** Все три суммы радикалов иррациональны, так как в каждой из них все радикалы и их отношения иррациональны по лемме 1. Для радикала  $\sqrt[17]{2021!}$  в последней сумме для этого достаточно заметить, что простое  $p = 2011$ , входит в разложение  $2021!$  в первой степени.

**2.** а) Один набор получается из другого умножением на некоторый радикал, например,  $(\sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}) = \sqrt{5}(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ . б) Чтобы нарисовать гиперкуб, изобразим трёхмерный куб, поместив один квадрат внутрь другого и соединив соответственные вершины (рис. 1а). (Это вид сверху на куб, сделанный из желе и немного расплывшийся после падения на стол.) Теперь аналогично рисуем один куб внутри другого и, соединяя соответственные вершины, получаем гиперкуб. Радикалы на внутреннем кубе уже расставлены на рисунке 2б в статье. Домножая их на  $\sqrt{7}$ , получаем радикалы на соответственных вершинах внешнего куба.

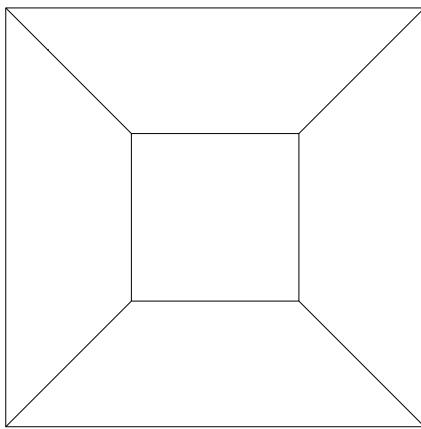


Рис. 1а

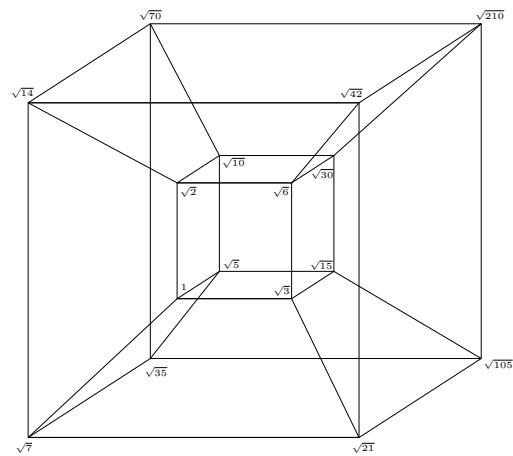


Рис 1б

**3.**  $1 \Rightarrow 2$ . Применим теорему 1 к  $\{Q_1, \dots, Q_N\} = \{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leq l_1, \dots, l_n < k\}$  и  $k_1 = \dots = k_N = k$ . Условие  $\sqrt[k]{Q_i/Q_j} \notin \mathbb{Q}$  при  $i \neq j$  верно по лемме 1.

$2 \Rightarrow 1$ . Пусть  $p_1, \dots, p_n$  — простые делители числителей и знаменателей в несократимых представлениях  $Q_1, \dots, Q_N$  и  $k = k_1 \dots k_N$ . Тогда  $\sqrt[k]{Q_i} = \sqrt[k]{Q_i^{k/k_i}}$  пропорционально с рациональным коэффициентом числу вида  $\sqrt[k]{p_1^{l_1} \dots p_n^{l_n}}$ , где  $0 \leq l_1, \dots, l_n < k$ .

**4.** а) При нуле можно взять ненулевой коэффициент, а при пропорциональных числах  $kx$  и  $lx$  ( $0 \neq k, l \in K$ ) — коэффициенты  $l$  и  $-k$  соответственно. Взяв нулевые коэффициенты при остальных элементах системы, получим её нулевую линейную комбинацию, в которой не все коэффициенты равны 0.

б) Пусть система  $x_1, \dots, x_m, x_{m+1}, \dots, x_n$  линейно независима над  $K$  и  $a_1x_1 + \dots + a_mx_m = 0$ . Тогда из равенства  $a_1x_1 + \dots + a_mx_m + 0x_{m+1} + \dots + 0x_n = 0$  следует, что  $a_1 = \dots = a_m = 0$ .

в) Если  $x \in K$ , то положив в равенстве  $a \cdot 1 + b \cdot x = 0$  значения  $a = x$  и  $b = -1$ , получим, что 1 и  $x$  линейно зависимы над  $K$ . Обратно, если  $x \notin K$ , то из равенства  $a \cdot 1 + b \cdot x = 0$ , где  $a, b \in K$ , следует, что  $b = 0$  (иначе  $x = -a/b \in K$ ), а тогда и  $a = 0$ .

г) Если  $a_1x_1 + \dots + a_nx_n = b_1x_1 + \dots + b_nx_n$ , где  $a_1, b_1, \dots, a_n, b_n \in K$ , то  $(a_1 - b_1)x_1 + \dots + (a_n - b_n)x_n = 0$ . Линейная независимость чисел  $x_1, \dots, x_n$  равносильна равенствам  $a_1 - b_1 = \dots = a_n - b_n = 0$ .

**5.** Пусть для  $n - 1$  простых чисел теорема доказана и  $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})$ . Каждое число в этом поле по предположению индукции однозначно представляется в виде суммы  $2^{n-1}$  слагаемых вида  $a\sqrt{p_1}^{l_1} \dots \sqrt{p_{n-1}}^{l_{n-1}}$ ,  $a \in \mathbb{Q}$ ,  $l_i = 0, 1$ . Число  $\sqrt{p_n}$  равно сумме чисел такого вида, но не равно ни одному из них по лемме 1. Значит, в сумме хотя бы два слагаемых, поэтому какой-то из радикалов  $\sqrt{p_1}, \dots, \sqrt{p_{n-1}}$  в какое-то слагаемое входит, а в какое-то — нет. Пусть это радикал  $\sqrt{p_{n-1}}$ . Тогда  $\sqrt{p_n} = A + B\sqrt{p_{n-1}}$ , где  $A, B \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-2}}) = K$ , причём  $AB \neq 0$ . Возведём в квадрат:  $p_n = A^2 + B^2p_{n-1} + 2AB\sqrt{p_{n-1}}$ , откуда  $AB = 0$  — противоречие.

**6.** Проблема — в определении сопряжённого числа. Внутри *каждого конкретного* поля  $K(\sqrt{d})$  сопряжение определено формулой  $f_d(a + b\sqrt{d}) = a - b\sqrt{d}$  ( $a, b \in K$ ). Это корректно:  $a, b$  определены

однозначно, так как  $\sqrt{d} \notin K$ . Но не обосновано приравнивание сопряжённых в разных смыслах: если  $\alpha = a + b\sqrt{d} = a' + b'\sqrt{d'}$ , то почему  $f_d(\alpha) = a - b\sqrt{d}$  должно равняться  $f_{d'}(\alpha) = a - b\sqrt{d'}$ ?

Можно данное определение понимать в таком смысле: если  $\alpha$  представимо в виде  $a + b\sqrt{d}$ , где  $a, b, d \in K$ ,  $\sqrt{d} \notin K$ , то положим сопряжённое к  $\alpha$  равным  $a - b\sqrt{d}$ . Но тогда вывод

$$a + b\sqrt{d} = a' + b'\sqrt{d'} \implies a - b\sqrt{d} = a' - b'\sqrt{d'}$$

есть не что иное как проверка корректности этого определения!

Выход из положения в том, чтобы определить сопряжённое инвариантным способом, не привязанным к конкретному выражению в виде квадратичной иррациональности. Именно, пусть  $\alpha \notin K$  является корнем многочлена степени 2 над  $K$ . Тогда определим сопряжённое к  $\alpha$  как второй корень этого многочлена. Корректность такого определения сводится к очевидной проверке того, что такой многочлен определён однозначно с точностью до числового множителя. Действительно, если  $x^2 + px + q$  и  $x^2 + p'x + q'$  — два многочлена с корнем  $\alpha$  над  $K$ , то их разность  $(p - p')x + q - q' \in K$  тоже имеет корень  $\alpha$ , откуда  $p = p'$  (иначе  $\alpha = \frac{q' - q}{p - p'} \in K$ ), а тогда и  $q = q'$ . Фактически так и вводятся сопряжённые в общей ситуации.

**7.** Идея — перейти к сопряжённым числам:  $(a - b\sqrt{2})^2 + (c - d\sqrt{2})^2 = 7 - 5\sqrt{2} < 0$  — противоречие. Концептуальное обоснование такого перехода — проверка того, что сопряжение  $f(a + b\sqrt{2}) = a - b\sqrt{2}$  ( $a, b \in \mathbb{Q}$ ) является вложением (см. определение на с. 9).

**8.** Сложим данное число с сопряжённым к нему:  $(6 + \sqrt{35})^{1000} + (6 - \sqrt{35})^{1000}$ . Эта сумма целая (из формулы бинома Ньютона). С другой стороны, сопряжённое число очень мало:

$$(6 - \sqrt{35})^{1000} = \frac{1}{(6 + \sqrt{35})^{1000}} < \frac{1}{10^{1000}},$$

Значит, у исходного числа первые 1000 цифр после запятой — девятки.

**9.** Рассмотрим  $2^{99}$  многочленов  $1 + \varepsilon_2 x_2 + \dots + \varepsilon_{100} x_{100}$ , где  $\varepsilon_i \in \{\pm 1\}$ . Их произведение — чётный многочлен по каждой из переменных, поэтому он имеет вид  $f(x_2^2, \dots, x_{100}^2)$ , где  $f$  — многочлен с целыми коэффициентами. В частности, при  $x_2 = \sqrt{2}, \dots, x_{100} = \sqrt{100}$  получается целое число, обозначим его  $d$ . Повторив рассуждение с противоположными по знаку многочленами  $-1 + \varepsilon_2 x_2 + \dots + \varepsilon_{100} x_{100}$ , получим то же число  $d$  (поскольку количество многочленов чётно). Значит, произведение из условия равно  $d^2$ .

$$\text{10. a)} \frac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}} = \frac{1}{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{(1+\sqrt{2})^2-3(\sqrt{2}-1)^2} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{8\sqrt{2}-6} = \frac{(1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3})(4\sqrt{2}+3)}{46}.$$

$$\text{б) Ответ: } \frac{1}{7}(3\sqrt[4]{27} + 8\sqrt[4]{9} + 5\sqrt[4]{3} + 8).$$

$$\text{11. } m = k^5, n = (2021 - k)^5, k = 1, \dots, 2020. \text{ Решение аналогично примеру 7.}$$

**12.** Поделим обе части на  $\sqrt[3]{2}$ :  $C\sqrt[6]{3/4} = a + b\sqrt[6]{2}$ . Теперь противоречие выводится аналогично примеру 7.

**13.** Докажем общее утверждение.

**Лемма 6.** Пусть  $K$  — подполе в  $\mathbb{C}$ ,  $r \in \mathbb{C} \setminus K$ ,  $r^2 \in K$ . Тогда все вложения  $K(r) \rightarrow \mathbb{C}$  над  $K$  (т. е. тождественные на  $K$ ) суть  $a + br \mapsto a \pm br$ .

**Доказательство.** Ясно, что  $K(r) = \{a + br \mid a, b \in K\}$  и что всякое вложение  $\varphi: K(r) \rightarrow \mathbb{C}$  над  $K$  определяется значением на  $r$ . При этом  $\varphi(r)^2 = \varphi(r^2) = r^2$ , откуда  $\varphi(r) = \pm r$ . Для знака плюс получаем тождественное вложение, для знака минус — аналог комплексного сопряжения ( $K = \mathbb{R}$ ,  $r = i$ ):  $\varphi(a + br) = a - br$ . Это вложение над  $K$ : свойства  $\varphi(x + y) = \varphi(x) + \varphi(y)$  и  $\varphi(k) = k$  при  $k \in K$  очевидны. Далее

$$\varphi((a + br)(c + dr)) = \varphi(ac + bdr^2 + (ad + bc)r) = ac + bdr^2 - (ad + bc)r = (a - br)(c - dr) = \varphi(a + br)\varphi(c - dr)$$

для всех  $a, b, c, d \in K$ . □

а) Применяем лемму 6 для  $K = \mathbb{Q}$  и  $r = i$ ;  $\text{tr}(1 + i) = (1 + i) + (1 - i) = 2$ .

б) Обозначим  $\varepsilon = \frac{1+i}{\sqrt{2}}$ . Так как  $\varepsilon^2 = i$ , то  $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\varepsilon, i) = \mathbb{Q}(\sqrt{2}, i)$ . При любом вложении поля  $\mathbb{Q}(\sqrt{2}, i)$  имеем  $\sqrt{2} \mapsto \pm\sqrt{2}$  и  $i \mapsto \pm i$ . Существуют 4 вложения, дающие все комбинации знаков: тождественное  $\varphi_{++}$ , вложения, которые даёт лемма 6,

$$\begin{aligned} \varphi_{+-}: a + bi &\mapsto a - bi, & a, b \in \mathbb{Q}(\sqrt{2}) \\ \varphi_{-+}: a' + b'\sqrt{2} &\mapsto a' - b'\sqrt{2}, & a', b' \in \mathbb{Q}(i), \end{aligned}$$

и их композиция  $\varphi_{--} = \varphi_{+-} \circ \varphi_{-+}$ . Отсюда  $\text{tr}(1 + i) = (\varphi_{++} + \varphi_{+-} + \varphi_{-+} + \varphi_{--})(1 + i) = 4$ .

Заметим, что образы числа  $\varepsilon$  при всех вложениях образуют набор сопряжённых  $\left\{ \frac{1 \pm i}{\sqrt{2}} \right\} = \{\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7\}$  — корней многочлена  $\mu_\varepsilon(x) = x^4 + 1$ . Это все первообразные корни 8-й степени из 1 (рис. 2).

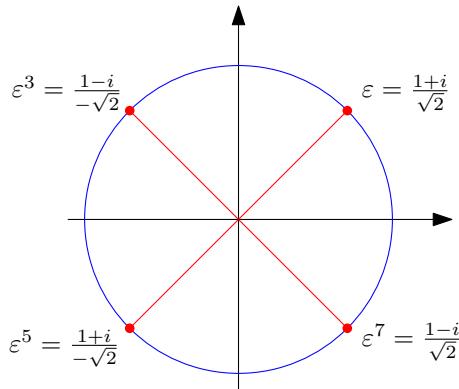


Рис. 2

**14.** Аналогично решению задачи 13б) получаем 4 вложения поля  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , при которых  $\sqrt{2} \mapsto \pm\sqrt{2}$  и  $\sqrt{3} \mapsto \pm\sqrt{3}$ . Каждое из них продолжается до вложения поля  $K(\sqrt{5})$  двумя способами:  $\sqrt{5} \mapsto \pm\sqrt{5}$  (аналогично по лемме 6 берём три вложения, меняющие знак у одного из трёх радикалов, и составляем их всевозможные  $2^3$  композиций).

Опишем вложения поля  $L = \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ . Обозначим  $r = \sqrt[12]{2}$ . Тогда  $\sqrt[4]{2} = r^3$ ,  $\sqrt[6]{2} = r^2$  и  $L = \mathbb{Q}(r^3, r^2) = \mathbb{Q}(r)$ . Согласно примеру 5  $\mu_r(x) = x^6 - 2$ , поэтому по теореме 3 все вложения  $\varphi_0, \dots, \varphi_5$  поля  $\mathbb{Q}(r)$  определяются условиями  $\varphi_j: r \mapsto r\varepsilon^j$ , где  $\varepsilon = \frac{1+i\sqrt{3}}{2} \in \sqrt[6]{1}$ .

# Algebraic numbers as vectors

The Jury of the project: I. Vorobyov, S. Dorichenko, A. Kanel–Belov, A. Kanunnikov, B. Frenkin, A. Zhilina

## Introduction

In geometry, we are used to add *vectors* and multiply them by *scalars* (numbers). This geometrical language often occurs to be useful in quite non-geometrical situations. In this project the role of vectors is played by *algebraic numbers*, that is, the roots of polynomials with rational coefficients. Rational numbers then are in the role of scalars.

We call complex numbers  $x_1, \dots, x_n$  *linearly independent* over the field of rational numbers  $\mathbb{Q}$  if the equation  $a_1x_1 + \dots + a_nx_n = 0$  with  $a_1, \dots, a_n \in \mathbb{Q}$  holds only for  $a_1 = \dots = a_n = 0$  (cf. non-complanar vectors at Fig. 1). Consideration of algebraic numbers as vectors occurs to be very natural and productive in general because it enables us to apply geometrical ideas in algebraic problems.

The project is arranged as follows. To warm up, we start with some olympiad problems on radicals. Some of them are solvable by usual school methods, and the others require further background, namely some information about algebraic numbers and fields, presented in the second section. You will learn to apply some suitable language and tools for a wide scope of problems. This is the preliminary part of the project.

The further section will be presented at the conference for the participants having chosen this project. In the third section we formulate the main theorem and suggest to prove it according to the outline based on the preceding information. Finally we present a research problem which develops and generalizes the main theorem. For participation in the project it is not required to solve any definite number of problems from the preliminary part.

The necessary background amounts to basic facts about complex numbers and polynomials. The most relevant operations are rootsquaring of complex numbers and division of polynomials with remainder. The problems on square radicals will be available for you even if you have little knowledge of complex numbers.

The foundations of the theory of algebraic numbers were laid by Karl Gauss's treatise "Disquisitiones arithmeticae" (1801) which has played the great role in number theory. Together with Lagrange's works, it prepared the discoveries of Évarist Galois who established the criterion for solvability of equations in radicals (1830) and laid the foundations of branches of modern algebra, such as group theory and field theory. Galois theory and theory of algebraic number fields were developed and systematized in the second half of XIX and the beginning of XX century due to Kummer, Kronecker, Hilbert e.a.

## 1. Warmup problems

If some of these problems create difficulties for you then you may return to them after Section 2.

- 1.1.** Prove irrationality of the following numbers: **a)**  $\sqrt[3]{1001}$ ; **b)**  $\sqrt{2} + \sqrt{3} + \sqrt{6}$ ; **c)**  $\sqrt{2} + \sqrt[3]{3}$ ;  
**d)\***  $\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7} + \sqrt{11}$ ; **e)\***  $\sqrt[5]{3} - \sqrt[5]{2}$ ; **f)\*\***  $\sqrt{\frac{3}{5}} + \frac{\sqrt[17]{2020!}}{2020} + \sqrt[5]{7^{77}}$ .

If you have no idea how to deal with the last markedly weird number then the first hint is as follows: it is worth while to prove a stronger assertion regarding linear independence. For instance, in part **b)** it would be as follows:

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \text{ where } a, b, c, d \in \mathbb{Q} \implies a = b = c = d = 0.$$

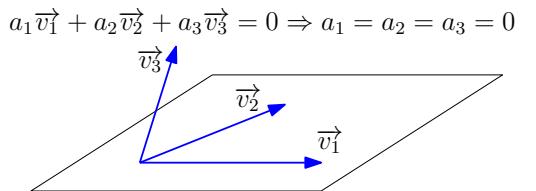


Fig. 1

- 1.2.** Find the polynomial of minimum degree with rational coefficients and the following root:
- a)  $\sqrt[3]{4}$ ;
  - b)  $\sqrt{2} + \sqrt{3}$ ;
  - c)  $\sqrt[3]{2} + \sqrt[3]{4}$ ;
  - d)  $\sqrt[8]{8} + \sqrt[9]{9}$ ;
  - e)  $\sqrt{6} + \sqrt{10} + \sqrt{15}$ ;
  - f)  $\sqrt[3]{1 + \sqrt{2}} + \sqrt[3]{1 - \sqrt{2}}$ ;
  - g)  $\sqrt[3]{7 + 5\sqrt{2}} + \sqrt[3]{7 - 5\sqrt{2}}$  (similarity in appearance is misleading!);
  - h)  $\cos \frac{2\pi}{5}$ ;
  - i)  $\cos \frac{2\pi}{9}$ ;
  - j)  $\cos \frac{2\pi}{97}$ ;
  - k)  $\cos \frac{2\pi}{n}$  for any  $n \in \mathbb{N}$ .

Present the polynomial found even if you aren't sure in minimality of its degree. In all parts except c), d), j), k write down the polynomial in standard form. Surprisingly, in parts j), k) it is worth while to pass to the complex plane.

- 1.3.** Which numbers of the form  $\frac{a+bi}{a-bi}$  with  $a, b \in \mathbb{Z}$  are roots of unity?

Below are some problems on square irrationalities. They contain an important idea... (let us avoid spoilers).

- 1.4.** Are there any rational numbers  $a, b, c, d$  such that  $(a + b\sqrt{2})^2 + (c + d\sqrt{2})^2 = 7 + 5\sqrt{2}$ ?

- 1.5.** Determine first 1000 decimal places of  $(6 + \sqrt{37})^{1001}$ .

- 1.6.** Prove that the product of all  $2^{100}$  expressions of the form

$$\pm\sqrt{1} \pm \sqrt{2} \pm \dots \pm \sqrt{99} \pm \sqrt{100}$$

(for all combinations of signs) is a) an integer; b) a squared integer.

## 2. A bit of theory: fields and algebraic numbers

Linear independence of 1 and  $\sqrt{2}$  (over  $\mathbb{Q}$ ) is nothing but irrationality of  $\sqrt{2}$  which has been known already by ancient Greeks. Let us increase the number of radicals.

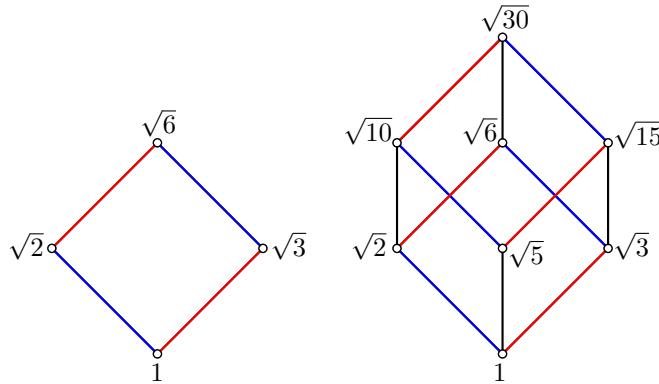


Fig. 2a

Fig. 2b

- 2.1.** Fill in the gaps in the following argument.

Let us prove that  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  are linearly independent over  $\mathbb{Q}$ . Suppose

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0 \text{ with } a, b, c, d \in \mathbb{Q}.$$

Separate the radical  $\sqrt{3}$ :

$$a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0.$$

If  $c + d\sqrt{2} = 0$  then \_\_\_\_\_

On the other hand, if  $c + d\sqrt{2} \neq 0$  then

$$\sqrt{3} = -\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = A + B\sqrt{2} \text{ with } A = \text{_____} \in \mathbb{Q}, B = \text{_____} \in \mathbb{Q}.$$

There are various ways to complete the proof.

The above example demonstrates certain ideas. Linear independence of the numbers from Fig. 2a has been reduced to the fact that  $\sqrt{3}$  is «alien» for the set

$$\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

(more formally,  $\sqrt{3}$  doesn't belong to it) just as  $\sqrt{2}$  is alien for  $\mathbb{Q}$ . And it was of importance that in the set  $\mathbb{Q} + \mathbb{Q}\sqrt{2}$  we are able not only to add, subtract, multiply but moreover divide (not by 0) as in  $\mathbb{Q}$  by removing the irrationality from the denominator.

A *number field* is a set of numbers which contains 0 and 1 and is closed under four arithmetic operations. We will omit the word „number“<sup>1</sup>. Thus  $K$  is a field if  $0, 1 \in K$  and for any  $a, b \in K$  we have  $a \pm b, ab \in K$  and  $a/b \in K$  for  $b \neq 0$ . Clearly  $\mathbb{Q}$  is a field and moreover a „minimal“ one: any (number) field contains it. If  $K \subseteq L$  are two fields then  $K$  is called a *subfield* of  $L$ .

We say that a system of numbers<sup>2</sup>  $x_1, \dots, x_n \in \mathbb{C}$  is *linearly independent over  $K$*  if the equation  $a_1x_1 + \dots + a_nx_n = 0$  with  $a_1, \dots, a_n \in K$  is satisfied only by  $a_1 = \dots = a_n = 0$ . For instance, numbers 1 and  $\sqrt{2}$  are linearly independent over  $\mathbb{Q}$  but linearly dependent over  $\mathbb{R}$ .

**2.2. Elementary properties of linear dependence.** Let  $K$  be a field. Prove the following:

- a) a system containing 0 or two numbers proportional over  $K$  is linearly dependent over  $K$ ;
- b) a subsystem of a linearly independent system is linearly independent (over the same field);
- c) the system  $1, x$  is linearly independent over  $K$  iff  $x \notin K$ ;
- d) the factors  $a_1, \dots, a_n \in K$  in the expression  $a_1x_1 + \dots + a_nx_n$  are uniquely determined iff the system  $x_1, \dots, x_n$  is linearly independent over  $K$ .

To *adjoin the numbers  $\alpha_1, \dots, \alpha_n$  to the field  $K$*  means to consider the least field (by inclusion) that contains  $K$  and these numbers. Notation:  $K(\alpha_1, \dots, \alpha_n)$ .

**2.3. Adjoining a square radical.** Let  $K$  be a subfield in  $\mathbb{R}$ ,  $0 < d \in K$  and  $\sqrt{d} \notin K$  (for instance,  $K = \mathbb{Q}$  and  $d = 2$ ). Prove that

$$K(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\},$$

where  $a, b \in K$  in  $a + b\sqrt{d}$  are determined uniquely.

**2.4.** Prove that  $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ .

**2.5.** Remove the irrationality from the denominator:  $\frac{1}{1 + \sqrt{2} - \sqrt{3} + \sqrt{6}}$ .

**2.6. a)** Prove that the numbers at the vertices of the cube at Fig. 2b are linearly independent over  $\mathbb{Q}$ .

**b)\*** Add  $\sqrt{7}$  to the above set of numbers, try to draw a hypercube and prove the assertion similar to part **a)**.

Perhaps it is time to formulate a general theorem on radicals of primes and to prove it by induction. In particular it would imply the solution of Problem **1.1d**).

What is the sense of linear independence over  $K$  for powers  $1, \alpha, \alpha^2, \dots, \alpha^n$  of a certain number  $\alpha$ ? It is the existence of numbers  $c_0, c_1, \dots, c_n \in K$  such that at least one of them is nonzero and

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_n\alpha^n = 0.$$

In other words,  $\alpha$  is a root of a nonzero polynomial with coefficients from  $K$ . Such  $\alpha$  is called *algebraic over  $K$* . Among these polynomials there is a unique one having the lowest degree and leading coefficient 1 (why?). It is called *the minimal polynomial* of  $\alpha$  over  $K$  and is often denoted  $\mu_\alpha^K(x)$ . For instance,  $\mu_i^\mathbb{R}(x) = x^2 + 1$ ,  $\mu_i^\mathbb{C}(x) = x - i$ . The degree  $\deg \mu_\alpha^K(x)$  of this polynomial also is called *the degree* of  $\alpha$  over  $K$  and is denoted  $\deg_K(\alpha)$ . The roots of  $\mu_\alpha^K(x)$  are called *conjugate* with  $\alpha$  over  $K$ .

For  $K = \mathbb{Q}$  we simply say that such  $\alpha$  are algebraic numbers.

**2.7.** Let a number  $\alpha \in \mathbb{C}$  be algebraic over a field  $K \subseteq \mathbb{C}$ . Prove the following:

- a)  $\deg_K(\alpha)$  is the least  $n \in \mathbb{N}$  such that  $1, \alpha, \dots, \alpha^n$  are linearly dependent over  $K$ ;
- b) the polynomial  $\mu_\alpha^K(x)$  is irreducible over  $K$  (i.e., is not a product of polynomials from  $K[x]$  of strictly lower degrees);
- c) every polynomial from  $K[x]$  with the root  $\alpha$  is a multiple of  $\mu_\alpha^K(x)$ ;
- d) a polynomial with the root  $\alpha$  and the leading coefficient 1, irreducible over  $K$  equals  $\mu_\alpha^K(x)$ .

The following criterion for irreducibility of a polynomial over  $\mathbb{Q}$  may be used without proof.

<sup>1</sup>There exist other fields as well, for instance fields of residues, fields of rational functions e.a.

<sup>2</sup>A non-ordered tuple of numbers, perhaps with some repetitions.

**Theorem 1** (Eisenstein's criterion). Let the coefficients of a polynomial  $a_nx^n + \dots + a_1x + a_0 \in \mathbb{Z}[x]$  satisfy the following conditions for some prime  $p$ :

- $p \nmid a_n$ ,
- $p \mid a_{n-1}, \dots, p \mid a_0$ ,
- $p^2 \nmid a_0$ .

Then this polynomial is irreducible over  $\mathbb{Q}$ .

**2.8. a)** Complete the solution of Problem 1.1e). Hint. Suppose  $\sqrt[5]{3} - \sqrt[5]{2} = a \in \mathbb{Q}$ , then  $\sqrt[5]{3} = \sqrt[5]{2} + a$ . Determine the minimal polynomials for the numbers in the left and right sides.

**b)** Solve in positive integers:  $\sqrt[5]{m} + \sqrt[5]{n} = 2020$ .

Let us now generalize Problem 2.3.

**Theorem 2** (on disposal of the irrationality from the denominator). Let a number  $\alpha$  be algebraic over a field  $K$  and have the degree  $n$ . Then any number from  $K(\alpha)$  is uniquely expressed in the form

$$c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1}, \text{ where } c_0, c_1, \dots, c_{n-1} \in K.$$

**2.9. a)** Remove the irrationality from the denominator of  $\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3}$ .

Hint. The usual multiplication by the conjugate doesn't work in this case. Find polynomials  $u(x), v(x) \in \mathbb{Q}[x]$  such that  $u(x)(x^2 + x + 3) + v(x)(x^3 - 2) = 1$ . For this, use either Euclidean algorithm in converse succession or the method of undetermined coefficients.

**b)** Prove Theorem 2.

By the fundamental theorem of algebra, every polynomial over  $\mathbb{C}$  of degree  $n > 0$  has  $n$  roots counted with multiplicities. By the following theorem, the polynomial  $\mu_\alpha^K(x)$  has no multiple roots and thus *every algebraic number of degree  $n$  has just  $n$  conjugates (including itself)*.

**Theorem 3.** A polynomial irreducible over some subfield of  $\mathbb{C}$  has no multiple complex roots.

**2.10.** Decompose the binomial  $x^4 - 2$  into irreducible ones and divide its roots into classes of conjugates over each of the fields  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ .

Now we have to emphasize on the roots of unity. As is well-known, the complex roots of  $x^n = 1$  are of the form

$$1, \varepsilon_n, \varepsilon_n^2, \dots, \varepsilon_n^{n-1}, \text{ where } \varepsilon_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

(a partial case of de Moivre's formula). Divide these into the classes of conjugates over  $\mathbb{Q}$ . For this, decompose the binomial  $x^n - 1$  into irreducible factors over  $\mathbb{Q}$ : then the roots of each factor form a class of conjugate algebraic numbers. Let us consider examples for little  $n$ . At Fig. 3, each irreducible factor and its roots are marked with a specific color.

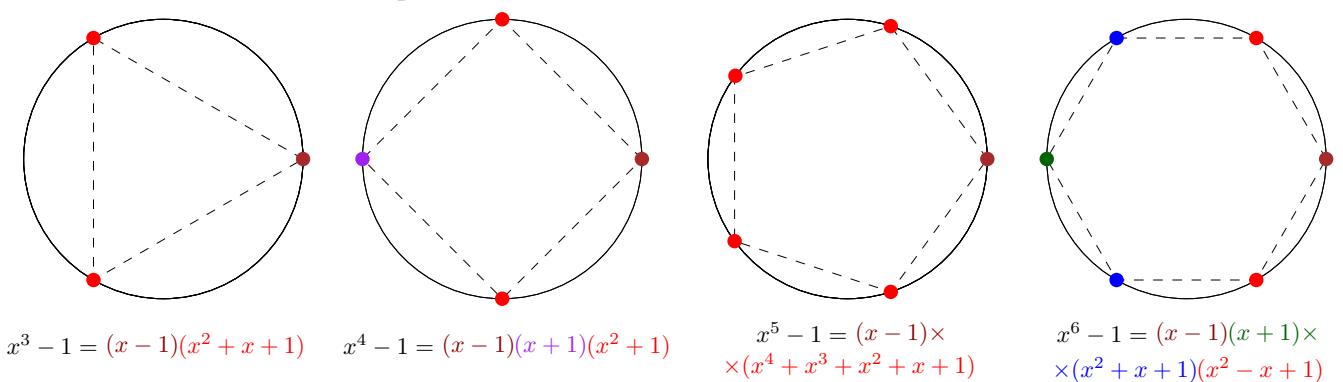


Fig. 3

Only irreducibility of  $x^4 + x^3 + x^2 + x + 1$  requires explanation. Below is a more general fact.

**2.11.** Prove that for any prime  $p$  the polynomial

$$\Phi_p(x) = x^{p-1} + \dots + x + 1$$

is irreducible over  $\mathbb{Q}$ . Hint. Apply Eisenstein's criterion (Theorem 1). Think a little how to do this since all coefficients of  $\Phi_p(x)$  are 1.

**2.12.** Decompose  $x^{12} - 1$  into binomials irreducible over  $\mathbb{Q}$ . Draw the picture similar to Fig. 3.

Let  $\varepsilon$  be a root of unity. Its *order* is the least  $n \in \mathbb{N}$  such that  $\varepsilon^n = 1$ . The roots of order  $n$  are called the *primitive roots* of degree  $n$ . It is easy to show that all these roots are of the form  $\varepsilon_n^k$  where  $k$  is mutually prime with  $n$ . The number of integers among  $1, \dots, n$  that are mutually prime with  $n$  is denoted  $\varphi(n)$ , and the function  $\varphi$  is called *Euler function*.

**Theorem 4.** Roots of unity having degree  $n$  are conjugate over  $\mathbb{Q}$  iff they have the same order. In particular,  $\deg_{\mathbb{Q}}(\varepsilon_n) = \varphi(n)$  for all  $n \in \mathbb{N}$ .

This theorem is equivalent to irreducibility over  $\mathbb{Q}$  for the so called *cyclotomic polynomials*

$$\Phi_n(x) = \prod_{1 \leq k \leq n, (k,n)=1} (x - \varepsilon_n^k).$$

Problem 2.11 is a simple particular case of it. In general case it is even obvious immediately that the coefficients of  $\Phi_n(x)$  are rational. Theorem 4 in general form may be proved at the Conference but you may use it just now. Theorem 4 enables to solve Problem 1.3 very quickly.

Now fill in the blanks in the solution of Problem 1.2c). Determine the polynomial  $\mu_{\sqrt[3]{4} + \sqrt[3]{2}}(x)$  (by default, over  $\mathbb{Q}$ ). The key idea is as follows:  $\sqrt[3]{2}$  is a root of  $\mu_{\sqrt[3]{4} + \sqrt[3]{2}}(x^2 + x)$  which consequently is a multiple of  $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$ , and so has also the roots  $\sqrt[3]{2}\varepsilon$  и  $\sqrt[3]{2}\varepsilon^2$ , where  $\varepsilon = \varepsilon_3$ . Hence the numbers  $\sqrt[3]{4} + \sqrt[3]{2}$ ,  $\sqrt[3]{4}\varepsilon^2 + \sqrt[3]{2}\varepsilon$ ,  $\sqrt[3]{4}\varepsilon + \sqrt[3]{2}\varepsilon^2$  are conjugate. Furthermore all of them are distinct (why?). It remains to show that the polynomial

$$(x - \sqrt[3]{4} - \sqrt[3]{2})(x - \sqrt[3]{4}\varepsilon^2 - \sqrt[3]{2}\varepsilon)(x - \sqrt[3]{4}\varepsilon - \sqrt[3]{2}\varepsilon^2)$$

has rational coefficients; then it equals  $\mu_{\sqrt[3]{4} + \sqrt[3]{2}}(x)$ . Show this.

The following theorem, one of the main theorems in this project, is a generalization of the above argument.

**Theorem 5.** If  $\alpha = \alpha_1, \dots, \alpha_n$  are all conjugates of  $\alpha$  over a field  $K$  then for every polynomial  $f(x) \in K[x]$  the number  $f(\alpha)$  is algebraic over  $K$  and its conjugates are  $f(\alpha_1), \dots, f(\alpha_n)$ . This list may consider repetitions but then each element occurs the same number of times.

**2.13.** Prove Theorem 5: **a)** for the case when  $\alpha$  is a root of an irreducible binomial; **b)** for the general case. (Investigation of linear independence of radicals requires only the more simple part **a**). For part **b**) you may use the main theorem on symmetrical polynomials.)

Below is the outline of the proof.

1) To prove that  $f(\alpha)$  is algebraic and all its conjugates are among  $f(\alpha_1), \dots, f(\alpha_n)$ , consider the polynomial

$$F(x) = (x - f(\alpha_1)) \dots (x - f(\alpha_n))$$

and prove that  $F(x) \in K[x]$ .

2) To prove that  $f(\alpha_1), \dots, f(\alpha_n)$  all are conjugate over  $K$ , consider the polynomial  $\mu_{f(\alpha)}f(x)$ .

3) To prove that all roots of  $F(x)$  are of the same multiplicity, consider the polynomial  $F(x)/\mu_{f(\alpha)}(x)$ .

Consider how to solve Problem 1.2i) using Theorems 4 and 5. This problem is the crucial one in the proof for the part «only if» in Gauss — Wantzel theorem: *a regular  $n$ -gon can be constructed with compass and ruler iff  $\varphi(n)$  is a power of 2, that is, if  $n$  is a product of a power of 2 and of some Fermat primes*. Fermat integers are integers of the form  $2^{2^k} + 1$ . First five of them are primes: 3, 5, 17, 257, 65537. Gauss has given the construction of the regular 17-gon. It would be of interest to construct the regular 257- and 65537-gons (a task for programmers).

**2.14.** Determine all  $n \in \mathbb{N}$  such that  $\cos \frac{2\pi}{n}$ : **a)** is rational; **b)** can be expressed as  $a + \sqrt{b}$ , where  $a, b \in \mathbb{Q}$ , that is,  $\deg_{\mathbb{Q}}(\cos \frac{2\pi}{n}) \leq 2$ .

### 3. Construction of regular polygons

Let us think how theorems 4 and 5 can be used to solve problem 1.2i). This problem is crucial in the proof of the «only if» part of Gauss — Wantzel theorem: *a regular n-gon can be constructed by compass and ruler iff  $\varphi(n)$  is a power of 2, that is, iff n is a product of a power of 2 and some Fermat primes.* The Fermat primes are the primes of the form  $2^{2^k} + 1$ . First 5 integers of this form are primes: 3, 5, 17, 257, 65537.

**3.1.** Using compass and ruler, construct a regular **a) pentagon; b) 17-gon.**

**3.2.** Develop an algorithm for construction of a regular  $p$ -gon for **a)  $p = 17$ ; b)  $p = 257$ ; c)  $p = 65537$ .**

Gauss constructed the regular 17-gon and proved constructibility of the regular  $p$ -gon for all Fermat primes  $p$ . This case (part a) is not estimated separately but forms an important step, so we recommend to analyze it.

The regular 257-gon was constructed by F.J. Richelot in the XIX century.

**3.3.** Using compass, ruler and trisector (the instrument for dividing an angle into three equal angles), construct the roots of the following polynomials: **a)  $8x^3 - 6x + 1$ ; b)  $512x^9 - 1152x^7 + 864x^5 - 240x^3 + 18x + 1$ .** (The problem is related to 9- and 27-gons.)

**3.4.** Find all primes  $p$  such that there exists a unique  $a \in \{1, \dots, p-1\}$  with  $p \mid a^3 - 3a + 1$ .

**3.5.** Using compass, ruler and trisector, construct a regular **a) 7-gon; b) 13-gon.**

“A too persistent research student drove his supervisor to say “Go away and work out the construction for a regular polygon of 65537 sides”. The student returned 20 years later with a construction” (J. Littlewood “A mathematician’s miscellany”, p. 42-43). The library of Goettingen university possesses the manuscript on more than 200 pages which was written by I. G. Hermes in 1894 after more than 10 years of research and contains the construction of the regular 65537-gon. Now computers enable us to do this much quicker.

### 4. Linear independence of radicals

**Theorem 6.** Suppose  $N, k_1, \dots, k_N \in \mathbb{N}$ ,  $N > 1$ ,  $Q_1, \dots, Q_N \in \mathbb{Q}_+$ , and furthermore  $\sqrt[k_1]{Q_i} / \sqrt[k_2]{Q_j} \notin \mathbb{Q}$  for all  $i \neq j$ . Then the equality

$$a_1 \sqrt[k_1]{Q_1} + \dots + a_N \sqrt[k_N]{Q_N} = 0 \text{ for } a_1, \dots, a_N \in \mathbb{Q}$$

holds only if  $a_1 = \dots = a_N = 0$ .

In particular, for  $Q_1 = 1$  we have that the sum  $\sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N}$  is irrational since the equality  $a_1 \sqrt[k_1]{1} + \sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N} = 0$  fails for all  $a_1 \in \mathbb{Q}$ .

Irrationality of a single radical is a simple, purely arithmetical question which amounts to uniqueness of prime factorization.

**Lemma 1.** For all  $k \in \mathbb{N}$  and  $Q \in \mathbb{Q}_+$  we have  $\sqrt[k]{Q} \in \mathbb{Q}$  iff the degrees of all prime factors of the numerator and the denominator in the irreducible representation of  $Q$  are multiples of  $k$ .

**4.1.** Prove Lemma 1.

**4.2.** Using Theorem 6 and Lemma 1, deduce irrationality of the numbers from Problem 1.1.

Without loss of generality, in Theorem 6 we may assume that all  $Q_i$  are positive integers and the degrees  $k_i$  are equal, obtaining the following equivalent formulation.

**Theorem 7.** Suppose  $k, n \in \mathbb{N}$ ,  $p_1, \dots, p_n$  are distinct primes,  $r_i = \sqrt[k]{p_i}$  for  $i = 1, \dots, n$ . Then the system  $\{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leq l_1, \dots, l_n < k\}$  of  $k^n$  numbers is linearly independent over  $\mathbb{Q}$ .

It is convenient to represent this system as an  $n$ -dimensional grid, see examples at fig. 2 and 4.

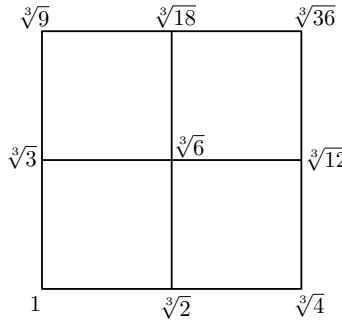


Fig. 4

**4.3.** Deduce Theorems 6 and 7 from each other.

**4.4.** Similarly to Problem 2.6, reduce Theorem 7 for  $k = 2$  to the following statement and prove it:

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}).$$

(We recommend to use conjugates, this helps to understand the case  $k > 2$ .)

**4.5.** Prove that Theorem 7 is equivalent to the following **Theorem 7'**: *in the notation from 7, the powers  $1, r_n, \dots, r_n^{k-1}$  are linearly independent over  $\mathbb{Q}(r_1, \dots, r_{n-1})$ .*

**4.6.** Suppose  $K$  is a subfield of  $\mathbb{R}$ ,  $r \in \mathbb{R}$ ,  $r^k \in K$  and  $r, \dots, r^{k-1} \notin K$ . Prove that the binom  $x^k - r^k$  is irreducible over  $K$ , and the powers  $1, r, \dots, r^{k-1}$  are linearly independent over  $K$ .

Thus Theorem 7' amounts to the following **Theorem 7''**: *in the above notation*

$$r_n^l \notin \mathbb{Q}(r_1, \dots, r_{n-1}) \text{ for all } l \in \{1, \dots, k-1\}.$$

Suppose the contrary. By induction, every number from  $\mathbb{Q}(r_1, \dots, r_{n-1})$  is uniquely represented as a sum of products of the form  $ar_1^{l_1} \dots r_{n-1}^{l_{n-1}}$ , where  $a \in \mathbb{Q}$  and all  $l_i \in \{0, \dots, k-1\}$ .

**4.7.** Obtain a contradiction if the above sum contains a single summand.

If the sum contains at least two summands then up to a permutation of radicals  $r_1, \dots, r_{n-1}$  we may assume

$$r_n^l = A_0 + A_1 r_{n-1} + \dots + A_{k-1} r_{n-1}^{k-1}, \text{ where } A_0, \dots, A_{k-1} \in \mathbb{Q}(r_1, \dots, r_{n-2}), \quad (1)$$

and at least two of  $A_0, \dots, A_{k-1}$  are nonzero.

**4.8. a)** Prove that  $A_0 = 0$ .

**b)** Suppose  $A_j$  is the first nonzero coefficient in (1). Obtain a contradiction by proving that  $A_j = 0$  (try to reduce this part to the preceding one). This completes the proof of Theorem 7.

**4.9.** Does Theorem 7 hold if each  $r_j$  ( $j = 1, \dots, n$ ) is some complex value of  $\sqrt[k]{p_j}$ ?

## 5. Dimension of field extensions

For deeper comprehension of algebraic numbers and dealing with more difficult problems we will consider the notion of vector space and its dimension as well as the technique of field extensions (everything for the case of number sets).

A set  $V \subseteq \mathbb{C}$  containing a field  $K$  is called a *vector space over  $K$* , and its elements are called *vectors* if  $V$  is closed under addition and multiplication by numbers from  $K$  and addition, that is,  $a + b, ka \in V$  for any  $a, b \in V$  and  $k \in K$ . For instance, every field is a vector space over any its subfield.

Suppose that a space  $V \subseteq \mathbb{C}$  over a field  $K$  contains numbers  $e_1, \dots, e_n$  such that any  $\alpha \in V$  can be represented as

$$\alpha = k_1 e_1 + \dots + k_n e_n \quad (2)$$

with uniquely determined coefficients  $k_1, \dots, k_n \in K$ . Then the system  $e_1, \dots, e_n$  is called a *basis* of  $V$  over  $K$ , and the equality (2) is called the *decomposition* of  $\alpha$  relative to this basis.

**5.1.** Prove that a basis of a space may be defined equivalently as a maximal (by inclusion) linearly independent system of elements. In other words, a system  $e_1, \dots, e_n$  is a basis of  $V$  over  $K$  iff it is linearly independent over  $K$  and the system  $e_1, \dots, e_n, \alpha$  is linearly dependent over  $K$  for any  $\alpha \in V$ .

A space having a finite basis is called finite-dimensional. An extension of the field having a finite basis is called a *finite extension*. The number of elements in a basis of a space  $V$  over  $K$  is called its *dimension* and is denoted  $\dim_K L$ . Correctness of this definition, that is, its independence of the choice of a basis is implied by the following lemma.

**Lemma 2** (the basic lemma on linear dependence). *If the numbers  $f_1, \dots, f_m$  are linearly expressed over a field  $K$  through the numbers  $e_1, \dots, e_n$  with  $m > n$  then  $f_1, \dots, f_m$  are linearly dependent over  $K$ .*

Let  $U \subseteq W$  be finite-dimensional spaces over a field  $K$ . It is not difficult to check that any basis of  $U$  can be completed up to a basis of  $V$ . Thus  $\dim_K U \leq \dim_K V$  and  $\dim_K U = \dim_K V \Leftrightarrow U = V$ .

If  $K$  is a subfield of a field  $L$  then we say that  $L/K$  is a field extension. Then clearly  $L$  is a vector space over  $K$ . The dimension of a finite extension  $L/K$  is also called its *degree* and is denoted  $[L : K]$ .

**5.2.** Let  $L/K$  be a finite extension. Prove that  $[L : K] = 2 \Leftrightarrow L = K(\alpha)$  for some  $\alpha \in L \setminus K$  such that  $\alpha^2 \in K$ .

**5.3.** Prove that the numbers  $1, \alpha, \dots, \alpha^{n-1}$  form a basis of the extension  $K(\alpha)/K$  iff  $\alpha$  is algebraic over  $K$  of degree  $n$ . Thus if  $\alpha$  is algebraic over  $K$  then  $\deg_K(\alpha) = [K(\alpha) : K]$ .

The following theorem is a useful tool in the theory of finite extensions (prove this theorem).

**Theorem 8** (on dimension of a tower). *If  $K \subseteq P \subseteq L$  are finite extensions of fields then*

$$\dim_K L = \dim_K P \cdot \dim_P L.$$

Compare this with the property of logarithms  $\log_a c = \log_a b \cdot \log_b c$ .

Let us return to the warmup problem **1.1c**).

**5.4.** Find all subfields of the fields: **a)**  $\mathbb{Q}(\sqrt[11]{1024})$ ; **b)**  $\mathbb{Q}(\sqrt[4]{3})$ ; **c)**  $\mathbb{Q}(\varepsilon_5)$ ; **d)**  $\mathbb{Q}(\varepsilon_8)$ .

**5.5\***. Denote  $\varepsilon = \varepsilon_{17}$ . Theorem 2 and Problem 2.11 imply  $\deg(\varepsilon) = 16$ .

**a)** Find all  $\alpha \in \mathbb{Q}(\varepsilon)$  such that  $\deg(\alpha) = 2, 4, 8$ . Hint: use Theorem 5 and consider the basis  $\varepsilon, \varepsilon^3, \varepsilon^{3^2}, \dots, \varepsilon^{3^{15}}$  in  $\mathbb{Q}(\varepsilon)$  over  $\mathbb{Q}$  (prove that this is a basis). This ordering is due to Gauss.

**5.6.** Find all conjugates over  $\mathbb{Q}$  for the numbers **a)**  $\sqrt{6} + \sqrt{10} + \sqrt{15}$ ; **b)**  $\sqrt[3]{2} + \sqrt[3]{3}$ .

**b)** Suppose  $U_k = \{\alpha \in \mathbb{Q}(\varepsilon) \mid \deg(\alpha) \text{ divides } k\}$ ,  $k = 1, 2, 4, 8, 16$ . In particular,  $U_1 = \mathbb{Q}$  and  $U_{16} = \mathbb{Q}(\alpha)$ . Prove that  $U_1 \subset U_2 \subset U_4 \subset U_8 \subset U_{16}$  is a chain of quadratic (that is, of degree 2) extensions of fields. This enables us to construct a regular 17-gon using compass and ruler (discovery of Gauss).

**A research problem.** What regular  $n$ -gons can be constructed by compass, ruler and trisector? Particular cases:  $n = 7, 13, 19, 37$ .

**A research problem.** Develop an algorithm for determination of the degree of any algebraic number in the extension  $\mathbb{Q}(\sqrt[k]{p_1}, \dots, \sqrt[k]{p_n})$ , where  $p_1, \dots, p_n$  are distinct primes. Particular cases:  $k = 2$ ;  $k$  is a prime.

# Algebraic numbers as vectors

A. Kanunnikov, I. Vorobyov

## §1. Introduction

How can we prove irrationality of the numbers

$$\sqrt[3]{\frac{121}{111}}, \sqrt{2} + \sqrt{3}, \sqrt{2} + \sqrt[3]{3}, \sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7}, \sqrt[5]{3} - \sqrt[5]{2}, \sqrt{\frac{3}{5}} + \frac{\sqrt[17]{2021!}}{2021} + \sqrt[5]{\frac{7^7}{3^{33}}}?$$

Irrationality of a single radical is a simple purely arithmetical question which amounts to prime decomposition.

**Lemma 1.** Suppose  $A, B, k \in \mathbb{N}$  and  $\gcd(A, B) = 1$ . Then  $\sqrt[k]{A/B} \in \mathbb{Q}$  iff the degrees of all primes in decompositions of  $A$  and  $B$  are multiples  $k$ .

*Proof.* Suppose  $\sqrt[k]{A/B} = a/b$ , where  $a, b \in \mathbb{N}$ , then  $Ab^k = Ba^k$ . Each prime divisor  $p$  of  $A$  does not divide  $B$ , and its degrees in decompositions of  $a^k$  and  $b^k$  are multiples of  $k$ , so the degree of  $p$  in the decomposition of  $A$  also is a multiple of  $k$ . The argument for the prime divisors of  $B$  is similar. The converse is obvious.

The number  $\sqrt[3]{\frac{121}{111}} = \sqrt[3]{\frac{11^2}{3 \cdot 37}}$  is irrational by lemma 1. Irrationality of the sum  $\sqrt{2} + \sqrt{3}$  is reduced to the irrationality of  $\sqrt{6}$  by squaring.

Suppose that  $\sqrt{2} + \sqrt[3]{3} = a \in \mathbb{Q}$  and cube the equality  $\sqrt[3]{3} = a - \sqrt{2}$ : we have  $3 = a^3 + 6a - (3a^2 + 2)\sqrt{2}$  and arriving to a contradiction:  $\sqrt{2} = \frac{a^3 + 6a - 3}{3a^2 + 2} \in \mathbb{Q}$ .

However the remaining numbers are not handled so simply: the straightforward exponentiation would only increase the number of radicals.

Perhaps a reader thinks: „Is it possible that after reading this article I will understand the reason of irrationality even for the last, especially weird number?“ „Yes, — we would answer, — but if you know how to divide polynomials with a remainder and extract roots from complex numbers. If it is not the case for this moment then you can at any rate deal with arbitrarily long sums of square radicals.“

In fact we will prove more: between the roots from rational numbers no linear relations with rational coefficients exist, except the obvious proportionalities, for instance  $\sqrt{8} = 2\sqrt{2}$ . The precise formulation is as follows.

**Theorem 1.** Suppose  $N, k_1, \dots, k_N \in \mathbb{N}$ ,  $N > 1$ ,  $0 < Q_1, \dots, Q_N \in \mathbb{Q}$  and  $\sqrt[k_i]{Q_i}/\sqrt[k_j]{Q_j} \notin \mathbb{Q}$  for  $i \neq j$ . Then the equality

$$a_1 \sqrt[k_1]{Q_1} + \dots + a_N \sqrt[k_N]{Q_N} = 0, \text{ where } a_1, \dots, a_N \in \mathbb{Q},$$

holds only for  $a_1 = \dots = a_N = 0$ .

In particular, for  $Q_1 = 1$  we have that the sum  $\sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N}$  is irrational since the equality  $a_1 \sqrt[k_1]{1} + \sqrt[k_2]{Q_2} + \dots + \sqrt[k_N]{Q_N} = 0$  fails for all  $a_1 \in \mathbb{Q}$ .

To apply Theorem 1, we have to check irrationality of specific radicals  $\sqrt[k_i k_j]{Q_i^{k_j}/Q_j^{k_i}}$  by lemma 1.

PROBLEM 1. Deduce from Theorem 1 and Lemma 1 irrationality of three numbers before Lemma 1.

In terms of vectors, the formulation of Theorem 1 is as follows: the numbers  $\sqrt[k_1]{Q_1}, \dots, \sqrt[k_N]{Q_N}$  are linearly independent over  $\mathbb{Q}$  (cf. non-complanar vectors at fig. 1). In these terms, the condition  $\sqrt[k_i]{Q_i}/\sqrt[k_j]{Q_j} \notin \mathbb{Q}$  expresses linear independence of  $\sqrt[k_i]{Q_i}$  and  $\sqrt[k_j]{Q_j}$  over  $\mathbb{Q}$  (linear independence of two vectors amounts to their non-collinearity).

In general, it is natural and productive to consider algebraic numbers (in particular radicals) as vectors: it enables us to apply geometric methods in algebraic problems.

Now we formulate a theorem which is more convenient for proving but occurs to be equivalent.

**Theorem 2.** Suppose  $k, n \in \mathbb{N}$ ,  $p_1, \dots, p_n$  are distinct primes,  $r_1 = \sqrt[k]{p_1}, \dots, r_n = \sqrt[k]{p_n}$ . Then the system  $\{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leq l_1, \dots, l_n < k\}$  of  $k^n$  numbers is linearly independent over  $\mathbb{Q}$ .

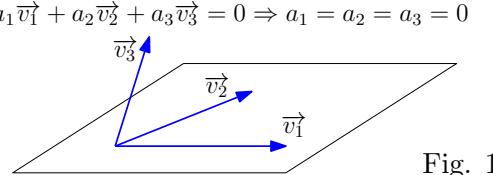


Fig. 1

It is convenient to represent this system as an  $n$ -dimensional lattice, see examples at fig. 2.

PROBLEM 2. a) What is the relation between the tuples of numbers at the parallel sides of the square at fig. 2a and at parallel edges and faces of the cube at fig. 2b? b) Try to draw a hypercube (4-dimensional cube) and place radicals in its vertices on the same principle.

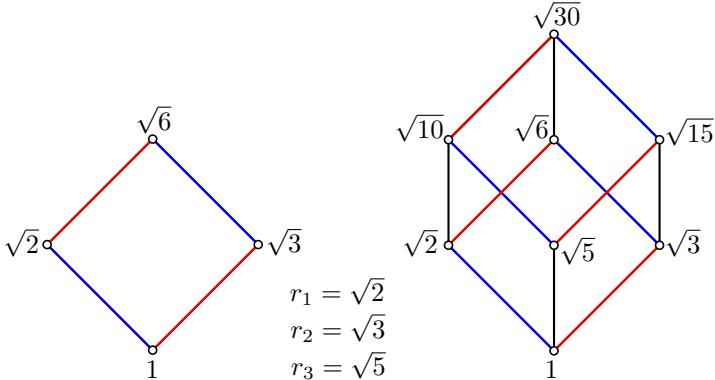


Fig. 2ab

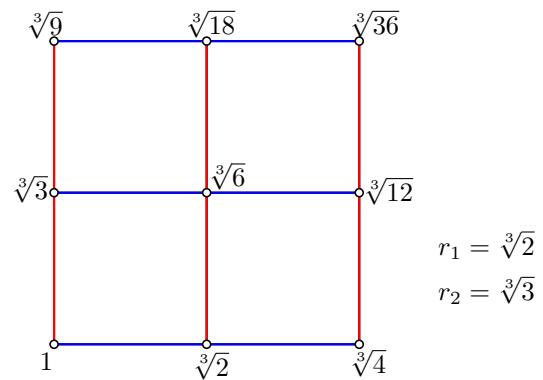


Fig. 2c

PROBLEM 3. Deduce Theorems 1 and 2 from each other. Hint.  $1 \Rightarrow 2$ : the numbers for the system in Theorem 2 are pairwise non-proportional over  $\mathbb{Q}$ ;  $2 \Rightarrow 1$ : generalize the argument from the following example.

**Example 1.** Let us reduce linear independence (by default, over  $\mathbb{Q}$ ) of  $1, \sqrt{1/2}, \sqrt[3]{4/3}$  to Theorem 2. Equalize the exponents of roots:  $1, \sqrt[6]{1/2^3}, \sqrt[6]{2^4/3^2}$ , multiply the second number by 2, and the third number by 3:  $1, \sqrt[6]{2^3}, \sqrt[6]{2^4 \cdot 3^4}$  (this does not influence linear independence). We obtain a subsystem of the system  $\{\sqrt[6]{2}^{l_1} \sqrt[6]{3}^{l_2} \mid 0 \leq l_1, l_2 \leq 5\}$ , which is linearly independent by Theorem 2.

The case of square radicals has been repeatedly discussed in the literature for school students [2, 4, 6]. In §2 we will consider it for some examples arriving to some (although not all) ideas for the general situation. One more important idea appears in [5], where Theorem 2 is proved for  $n = 1$ . The general case is considered for instance in a research paper [7] which requires deep background (Galois theory). In §3 we prove Theorem 2 in a rather elementary way together with necessary information on algebraic numbers, which is interesting in its own. Finally we give a quite short proof of Theorem 1 available for a freshman. Everything necessary for understanding is gathered in §4.

## §2. The case of square radicals

Theorem 2 for  $k = 2$  can be proved by induction on  $n$ . The base  $n = 1$ : linear independence of 1 and  $\sqrt{p_1}$  just denotes irrationality of  $\sqrt{p_1}$  and is true by Lemma 1. Consider the cases  $n = 2, 3$  for specific examples, this makes the ideas of the proof more clear. The complete argument for an arbitrary  $k$  by induction on  $n$  see below in §3.

**Example 2.** Let us prove that  $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$  (fig. 2a) are linearly independent. Suppose  $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ , where  $a, b, c, d \in \mathbb{Q}$ . Separate  $\sqrt{3}$ :  $a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0$ . If  $c + d\sqrt{2} = 0$  then  $a + b\sqrt{2} = 0$ , and then by irrationality  $\sqrt{2}$ ,  $c = d = 0$  and  $a = b = 0$ . And if  $c + d\sqrt{2} \neq 0$  then

$$\sqrt{3} = -\frac{a + b\sqrt{2}}{c + d\sqrt{2}} = -\frac{(a + b\sqrt{2})(c - d\sqrt{2})}{c^2 - 2d^2} = A + B\sqrt{2}, \text{ where } A = \frac{2bd - ac}{c^2 - 2d^2}, B = \frac{ad - bc}{c^2 - 2d^2} \in \mathbb{Q}.$$

Square the equality  $\sqrt{3} = A + B\sqrt{2}$ :

$$3 = A^2 + 2B^2 + 2AB\sqrt{2} \implies AB = 0, \text{ otherwise } \sqrt{2} \in \mathbb{Q}.$$

For  $A = 0$  we have  $\sqrt{3/2} = B \in \mathbb{Q}$ , and for  $B = 0$  we have  $\sqrt{3} = A \in \mathbb{Q}$ , a contradiction with Lemma 1.

We have reduced linear independence of the numbers at Fig. 2a to the fact that  $\sqrt{3}$  is „foreign“ for the set  $\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$  (formally,  $\sqrt{3}$  does not lie in it), just as  $\sqrt{2}$  is „foreign“ for  $\mathbb{Q}$ . Moreover it occurs important that in the set  $\mathbb{Q} + \mathbb{Q}\sqrt{2}$  we can not only add, subtract, multiply but also divide (not by 0) as in  $\mathbb{Q}$ . Before the next step, let us introduce some notions.

**A bit of theory.** A set of numbers containing 0 and 1 and closed under four arithmetical operations is called a *umber field*. In the sequel the word „number“ will be omitted. Thus  $K$  is a field iff  $0, 1 \in K$  and for any  $a, b \in K$  we have  $a \pm b, ab \in K$  and  $a/b \in K$  for  $b \neq 0$ . It is easily seen that  $\mathbb{Q}$  is a field, and moreover „the

least one“: any number field includes it<sup>1</sup>. In a field  $K$  is included in a field  $L$  then we say that  $K$  is a *subfield* in  $L$ . In the section, all fields lie in the field  $\mathbb{R}$  of rationals.

Numbers  $x_1, \dots, x_n$  are called *linearly independent over a field  $K$*  if the equality  $a_1x_1 + \dots + a_nx_n = 0$  where  $a_1, \dots, a_n \in K$  holds only for  $a_1 = \dots = a_n = 0$ . For example, the numbers 1 and  $\sqrt{2}$  are linearly independent over  $\mathbb{Q}$  but linearly dependent over  $\mathbb{R}$  (the equality  $a_1 \cdot 1 + a_2\sqrt{2} = 0$  holds for  $a_1 = \sqrt{2}$  and  $a_2 = -1$ ).

**PROBLEM 4.** Check the property of linear dependence/independence over an arbitrary field  $K$ :

- a) if a system contains zero or two numbers whose ratio lies in  $K$  then it is linearly dependent over  $K$ ;
- b) a subsystem of a linearly independent system is linearly independent;
- c) a system  $1, x$  is linearly independent over  $K$  iff  $x \notin K$ ;
- d) the coefficients  $a_1, \dots, a_n \in K$  in the expression  $a_1x_1 + \dots + a_nx_n$  are uniquely determined iff the system  $x_1, \dots, x_n$  is linearly independent over  $K$ .

The least (by inclusion) field including a field  $K$  and numbers  $\alpha_1, \dots, \alpha_n$ , is denoted  $K(\alpha_1, \dots, \alpha_n)$  and is called the field generated by these numbers over  $K$ . Let us describe the field generated over  $K$  by a single square radical  $\sqrt{d} \notin K$  where  $d \in K$ . Obviously the field  $K(\sqrt{d})$  consists of ratios of numbers having the form  $a + b\sqrt{d}$ , where  $a, b \in K$ . We can remove irrationality in the denominator multiplying it by the *conjugate*  $a - b\sqrt{d}$ :  $\frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - db^2}$  (as in Example 2). Hence

$$K(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\}.$$

**Example 3.** Suppose  $p, q$  are distinct primes. Similarly to Example 2,  $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$  and the numbers  $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$  are linearly independent over  $\mathbb{Q}$ . Hence

$$\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p})(\sqrt{q}) = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \mid a, b, c, d \in \mathbb{Q}\},$$

and such representation is unique.

**Example 4.** Let us prove that the numbers at Fig. 2b are linearly independent over  $\mathbb{Q}$ . Suppose

$$a_1 + a_2\sqrt{2} + \dots + a_8\sqrt{30} = 0, \text{ where } a_1, a_2, \dots, a_8 \in \mathbb{Q}.$$

**Step 1.** Put  $\sqrt{5}$  out of brackets to obtain an equality of the form  $A + B\sqrt{5} = 0$ , where  $A, B \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ :

$$\underbrace{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_5\sqrt{6}}_A + \underbrace{(a_4 + a_6\sqrt{2} + a_7\sqrt{3} + a_8\sqrt{6})\sqrt{5}}_B = 0. \quad (1)$$

It suffices to prove that  $A = B = 0$ . Then according to Example 2, we have  $a_1 = a_2 = a_3 = a_5 = 0$  and  $a_4 = a_6 = a_7 = a_8 = 0$ .

**Step 2.** We have to prove that 1 and  $\sqrt{5}$  are linearly independent over  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ . This is equivalent to condition  $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$  (Problem 4c).

**Step 3.** Suppose  $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ , and in view of the description of this field in Example 3 we have

$$\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \text{ where } a, b, c, d \in \mathbb{Q}. \quad (2)$$

A big number of radicals does not stimulate to square. But we can perform this more cleverly grouping the summands in one of two ways:

$$\underbrace{a + b\sqrt{2}}_C + \underbrace{(c + d\sqrt{2})\sqrt{3}}_D = \sqrt{5} = \underbrace{a + c\sqrt{3}}_{C'} + \underbrace{(b + d\sqrt{3})\sqrt{2}}_{D'}, \quad (3)$$

not „troubling“  $C, D, C', D'$ . Square the first equality:

$$C^2 + 3D^2 + 2CD\sqrt{3} = 5.$$

Since 1 and  $\sqrt{3}$  are linearly independent over  $\mathbb{Q}(\sqrt{2})$ , we have  $CD = 0$ . Similarly  $C'D' = 0$ . We have 4 cases:  $C = C' = 0$ ,  $C = D' = 0$ ,  $C' = D = 0$  or  $D = D' = 0$ . If  $C = C' = 0$  then  $a = b = c = 0$ , hence  $\sqrt{5} = d\sqrt{6}$ , and this contradicts Lemma 1. In the other cases we obtain a similar contradiction because the right side of (2) reduces to a single nonzero summand.

<sup>1</sup>There exist other fields as well: the fields of residues  $\mathbb{Z}_p$ , the field of rational functions etc. Any field includes either  $\mathbb{Q}$  or  $\mathbb{Z}_p$  for some  $p$ .

PROBLEM 5. Prove Theorem 2 for  $k = 2$ : perform an induction step from  $n - 1$  to  $n$  similarly to Example 4.

Before consideration of radicals of higher exponents, let us discuss how to perform the last step without squaring, with the general case in mind. Perhaps you would agree that a straightforward exponentiating by 5 would hardly lead to a contradiction for equality as harmless as  $\sqrt[5]{3} = a + b\sqrt[5]{2}$  ( $a, b \in \mathbb{Q}$ )... So let us try to deal with the equality (3) using conjugates.

Numbers of the form  $a \pm b\sqrt{d}$  over a field  $K$  where  $a, b, d \in K$ ,  $\sqrt{d} \notin K$  are called conjugate. In (3) the conjugate to  $C + D\sqrt{3}$  over  $\mathbb{Q}(\sqrt{2})$  is  $C - D\sqrt{3}$ , and the conjugate for  $C' + D'\sqrt{2}$  over  $\mathbb{Q}(\sqrt{3})$  is  $C' - D'\sqrt{2}$ . At the same time, the conjugate to  $\sqrt{5}$  over both fields is  $-\sqrt{5}$ . Since the numbers are equal, their conjugates are equal as well:

$$C - D\sqrt{3} = -\sqrt{5} = C' - D'\sqrt{2}. \quad (4)$$

This and (3) imply that  $C = C' = 0$ , which is impossible as was shown above.

Unfortunately this argument only seems strict by contains a „hole“. However it can be closed. The logical error is rather subtle, and a reader may be proud if he would manage to find and improve it.

PROBLEM 6. Why the transition from (3) to (4) is not justified and how to improve this?

Using of conjugates often is effective. Below are some olympiad problems on this subject.

PROBLEM 7. Do there exist rational numbers  $a, b, c, d$  such that  $(a + b\sqrt{2})^2 + (c + d\sqrt{2})^2 = 7 + 5\sqrt{2}$ ?

PROBLEM 8. Find 1000 first digits after the point in the decimal record of  $(6 + \sqrt{35})^{1000}$ .

PROBLEM 9. prove that the product of  $2^{100}$  numbers  $\pm\sqrt{1} \pm \sqrt{2} \pm \dots \pm \sqrt{99} \pm \sqrt{100}$  is a perfect square.

### §3. The general case

Let us start the proof of Theorem 2 for an arbitrary  $k$  according to the plan from Example 4. Each step will enlarge our difficulties.

**Step 1: splitting of the last radical.** The linear relation over  $\mathbb{Q}$  (that is, with coefficients from  $\mathbb{Q}$ ) for the nine numbers at fig.c 2c can be represented as

$$f_0(\sqrt[3]{2}) + f_1(\sqrt[3]{2})\sqrt[3]{3} + f_2(\sqrt[3]{2})\sqrt[3]{9} = 0,$$

where  $f_0, f_1, f_2$  are polynomials of degrees less than 3 over  $\mathbb{Q}$  (grouping the summands as in (1)). So the linear independence of these numbers would follow from two facts:

the numbers  $1, \sqrt[3]{3}, \sqrt[3]{9}$  are linearly independent over the field  $\mathbb{Q}(\sqrt[3]{2})$ ; (5)

the numbers  $1, \sqrt[3]{2}, \sqrt[3]{4}$  are linearly independent over the field  $\mathbb{Q}$ . (6)

In fact, (5) implies  $f_0(\sqrt[3]{2}) = f_1(\sqrt[3]{2}) = f_2(\sqrt[3]{2}) = 0$ , and then (6) implies that the coefficients of  $f_0, f_1, f_2$  are zero. Let us generalize this argument to show that it suffices to prove **Theorem 2'**: *in the notation of Theorem 2 the numbers  $1, r_n, \dots, r_n^{k-1}$  are linearly independent over the field  $\mathbb{Q}(r_1, \dots, r_{n-1})$ .*

Suppose that Theorem 2' has been proven. Let us prove Theorem 2 by induction on  $n$ . For  $n = 1$  the theorems are identical:  $\mathbb{Q}(r_1, \dots, r_{n-1}) = \mathbb{Q}$ . Let  $n > 1$ . Reformulate Theorem 2: *if  $F(x_1, \dots, x_n)$  is a polynomial over  $\mathbb{Q}$  such that the degree of each variable is less than  $k$ , and  $F(r_1, \dots, r_n) = 0$  then  $F = 0$  (that is, all coefficients of  $F$  are zero).* Express  $F$  in the form

$$F(x_1, \dots, x_n) = f_0(x_1, \dots, x_{n-1}) + f_1(x_1, \dots, x_{n-1})x_n + \dots + f_{k-1}(x_1, \dots, x_{n-1})x_n^{k-1}.$$

By condition  $F(r_1, \dots, r_n) = 0$ . By Theorem 2' we have  $f_j(r_1, \dots, r_{n-1}) = 0$  for all  $j = 0, \dots, k - 1$ . By induction  $f_0 = \dots = f_{n-1} = 0$ , thus  $F = 0$ .

**Step 2: „otherness“ of the last radical.** Let  $K$  is any field,  $r$  is a number such that  $r^k \in K$ . Let us determine when

$$\text{the numbers } 1, r, \dots, r^{k-1} \text{ are linearly independent } K. \quad (7)$$

In other words,  $r$  must not be a root of a polynomial with degree less than  $k$  and coefficients from  $K$ . For  $k = 2$  this means simply that  $r \notin K$  (Problem 4c). For  $k > 2$  the situation is much more complicated and interesting.

**A bit of theory.** The set of the polynomials over a field  $K$  is denoted  $K[x]$ . A polynomial over  $K$  of positive degree, which is not a product of polynomials of lower degrees is called *irreducible* over  $K$ . Polynomials over a field allow division with remainder („long division“).

Suppose a number  $\alpha$  is a root of a nonzero polynomial over a field  $K$ . Then it is called *an algebraic number over  $K$* . Among these polynomials there is a single polynomial of minimal degree with the leading coefficient 1 (if there were two then their difference would be a polynomial of lesser degree with the root  $\alpha$ ). It is called *the minimal polynomial* of the number  $\alpha$  over  $K$  and will be denoted  $\mu_\alpha^K(x)$  or  $\mu_\alpha(x)$  if the field  $K$  is clear. The degree of this polynomial is the least  $m \in \mathbb{N}$  such that the numbers  $1, \alpha, \dots, \alpha^m$  are linearly dependent over  $K$ . The basic properties of  $\mu_\alpha^K(x) = \mu_\alpha(x)$  are as follows:

- 1) the polynomial  $\mu_\alpha(x)$  is irreducible over  $K$ ;
- 2) every polynomial from  $K[x]$  with the root  $\alpha$  is a multiple of  $\mu_\alpha(x)$ ;
- 3) the polynomial  $p(x)$  irreducible over  $K$  and having the root  $\alpha$  and the leading coefficient 1 equals  $\mu_\alpha(x)$ .

*Proof.* 1) If  $\mu_\alpha$  decomposes into a product of polynomials over  $K$  of lesser degrees then  $\alpha$  is a root of one of the factors which contradicts to minimality of degree of  $\deg \mu_\alpha$ .

2) Suppose  $f \in K[x]$  and  $f(\alpha) = 0$ . Divide  $f$  by  $\mu_\alpha$  with a remainder:  $f = \mu_\alpha q + s$ , where  $q, s \in K[x]$  and either  $s = 0$  or  $\deg s < \deg \mu_\alpha$ . The second case is impossible because  $s(\alpha) = f(\alpha) - \mu_\alpha(\alpha)q(\alpha) = 0$ .

3) By part 2),  $p(x)$  is a multiple of  $\mu_\alpha(x)$ , and since  $p(x)$  is irreducible over  $K$ , we have  $p(x)/\mu_\alpha(x) = c \in K$ . Since the leading coefficients of  $p(x)$  and  $\mu_\alpha(x)$  are equal to 1, we have  $c = 1$ .  $\square$

Thus (7)  $\Leftrightarrow \mu_r^K(x) = x^k - r^k \Leftrightarrow$  the binomial  $x^k - r^k$  is irreducible over  $K$ .

For instance, statements (5) and (6) are respectively equivalent to irreducibility of the binomial  $x^3 - 3$  over  $\mathbb{Q}(\sqrt[3]{2})$  and of the binomial  $x^3 - 2$  over  $\mathbb{Q}$  which means that  $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$  and  $\sqrt[3]{2} \notin \mathbb{Q}$  (a cubic polynomial is irreducible over a field iff it has no roots in this field). In general, the condition of „otherness“  $r \notin K$  is necessary but not sufficient. Although in our case the actors  $K$  and  $r$  are in the field  $\mathbb{R}$ , we will leave it for the complex plane, the field  $\mathbb{C}$  where the binomial  $x^k - r^k$  decomposes into linear factors. By the de Moivre formula [3]

$$x^k - r^k = (x - r)(x - r\varepsilon) \dots (x - r\varepsilon^{k-1}), \text{ where } \varepsilon = \varepsilon_k = \cos \frac{2\pi}{k} + i \sin \frac{2\pi}{k}. \quad (8)$$

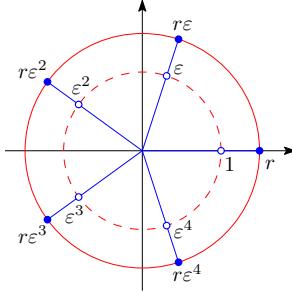


Fig. 3

**Lemma 2.** Suppose  $K$  is a subfield in  $\mathbb{R}$ ,  $r \in \mathbb{R}$ ,  $r^k \in K$  and  $r, \dots, r^{k-1} \notin K$ . Then the binomial  $x^k - r^k$  is irreducible over  $K$ .

*Proof.* Let  $x^k - r^k$  have a factor in  $K[x]$  with degree  $l \in \{1, \dots, k-1\}$  such that its intercept is  $c$ . From the decomposition (8) we have  $c = (-r)^l \varepsilon^s$  for some integer  $s$ . Since  $c \in K \subseteq \mathbb{R}$ ,  $r \in \mathbb{R}$  and  $|\varepsilon^s| = 1$ , we have  $r^l = \pm |c| \in K$  which contradicts the condition.  $\square$

*Remark.* For  $r \notin \mathbb{R}$  the lemma fails: for instance, for  $k = 3$  and  $r = \varepsilon$  we have  $\varepsilon, \varepsilon^2 \notin \mathbb{R}$  but the binomial  $x^3 - 1$  is irreducible.

**Example 5.** For any prime  $p$  and positive integer  $k > 1$  we have  $\sqrt[k]{p}, \dots, \sqrt[k]{p^{k-1}} \notin \mathbb{Q}$  (Lemma 1), hence the binomial  $x^k - p$  is irreducible over  $\mathbb{Q}$  (Lemma 2)<sup>2</sup>, hence  $\mu_{\sqrt[k]{p}}(x) = x^k - p$ .

In general Theorem 2' reduces to **Theorem 2''** by Lemma 2: *in the same notation*

$$r_n, \dots, r_n^{k-1} \notin \mathbb{Q}(r_1, \dots, r_{n-1}). \quad (9)$$

For  $n = 1$  this follows from Lemma 1. To arrive to a contradiction for  $n > 1$ , let us express the numbers from  $\mathbb{Q}(r_1, \dots, r_{n-1})$  in the form of polynomials in  $r_1, \dots, r_{n-1}$ . For instance, the condition  $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$  takes the form  $\sqrt[3]{3} \neq a + b\sqrt[3]{2} + c\sqrt[3]{4}$  with  $a, b, c \in \mathbb{Q}$ .

**Step 3: removal of the irrationality from the denominator.** The well-known multiplication by conjugates applies only for square radicals. The necessary operations for  $k > 2$  will be first shown by an example.

<sup>2</sup>In [5] linear independence  $1, \sqrt[k]{p}, \dots, \sqrt[k]{p^{k-1}}$  also is reduced to irreducibility of  $x^k - p$  which follows from the Eisenstein criterion.

**Example 6.** Let us remove irrationality from the denominator of  $\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3}$ . Denote  $r = \sqrt[3]{2}$  and  $f(x) = x^2 + x + 3$ . We have to find a polynomial  $u \in \mathbb{Q}[x]$  such that  $\frac{1}{f(r)} = u(r)$ . This means that  $f(x)u(x) - 1$  has the root  $r$  and so is a multiple of  $\mu_r^\mathbb{Q}(x) = x^3 - 2$  (Example 5). Thus

$$u(x)f(x) + v(x)(x^3 - 2) = 1$$

for some polynomial  $v \in \mathbb{Q}[x]$ . Polynomials  $u$  and  $v$  can be found using Euclid algorithm:

Euclid algorithm	Reversal of Euclid algorithm
$x^3 - 2 = (x^2 + x + 3)(x - 1) - 2x + 1$	$\frac{15}{4} = f(x) - (f(x)(x - 1) - (x^3 - 2))(\frac{1}{2}x + \frac{3}{4}) =$
$x^2 + x + 3 = (2x - 1)(\frac{1}{2}x + \frac{3}{4}) + \frac{15}{4}$	$= (x^3 - 2)(\frac{1}{2}x + \frac{3}{4}) + f(x)(-\frac{1}{2}x^2 - \frac{1}{4}x + \frac{7}{4})$

So  $(2x^2 + x - 7)(x^2 + x + 3) - (2x + 3)(x^3 - 2) = -15$ , and for  $x = r$  this implies

$$\frac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3} = \frac{7 - \sqrt[3]{2} - 2\sqrt[3]{4}}{15}.$$

Now we will prove a general assertion following the above example.

**Lemma 3** (on removal of an irrationality from the denominator). *If a number  $\alpha$  is algebraic over a field  $K$  and  $\deg \mu_\alpha(x) = k$  then every number from the field  $K(\alpha)$  is uniquely expressed as*

$$c_0 + c_1\alpha + \dots + c_{k-1}\alpha^{k-1}, \text{ where } c_0, c_1, \dots, c_{k-1} \in K. \quad (10)$$

*Proof.* The numbers of this form lie in  $K(\alpha)$ , so we have to check that they form a field. Obviously this set is closed under addition, subtraction and multiplication. Suppose  $f \in K[x]$  and  $f(\alpha) \neq 0$ . Then  $f(x)$  is not a multiple of  $\mu_\alpha(x)$ , hence these polynomials are mutually prime. Euclid algorithm provides polynomials  $u, v \in K[x]$  such that  $u(x)f(x) + v(x)\mu_\alpha(x) = 1$ . For  $x = \alpha$  we get  $1/f(\alpha) = u(\alpha)$  which is transformed to (10) when we replace  $u$  with its remainder of division by  $\mu_\alpha$ . The coefficients  $c_i$  are uniquely determined, otherwise  $\alpha$  would be a root of a polynomial of degree less than  $k$ .  $\square$

PROBLEM 10. Get rid of irrationality in the denominators: a)  $\frac{1}{1 + \sqrt{2} - \sqrt{3} + \sqrt{6}}$ ; b)  $\frac{1}{\sqrt[4]{27} + 2\sqrt[4]{3} - 1}$ .

Let us return to the proof of the Theorem 2''. By the inductive assumption, the binomial  $x^k - r_1^k$  is irreducible over  $\mathbb{Q}$ , the binomial  $x^k - r_2^k$  over  $\mathbb{Q}(r_1)$ , ..., the binomial  $x^k - r_{n-1}^k$  over  $\mathbb{Q}(r_1, \dots, r_{n-2})$ . Consecutively removing irrationalities from the denominators, we uniquely represent each number from  $\mathbb{Q}(r_1, \dots, r_{n-1})$  as a sum of numbers of the form

$$ar_1^{l_1} \dots r_{n-1}^{l_{n-1}}, \text{ where } a \in \mathbb{Q}, 0 \leq l_1, \dots, l_{n-1} < k. \quad (11)$$

Suppose (9) fails, that is,  $r_n^l$  for some  $l \in \{1, \dots, k-1\}$  equals a sum of numbers of the form (11). This sum contains more than one summand, otherwise  $r_n^l / (r_1^{l_1} \dots r_{n-1}^{l_{n-1}}) = a \in \mathbb{Q}$ , a contradiction to Lemma 1. Hence one of the radicals  $r_1, \dots, r_{n-1}$  appears in two summands with different degrees, let it be  $r_{n-1}$ . Thus

$$r_n^l = A_0 + A_1 r_{n-1} + \dots + A_{k-1} r_{n-1}^{k-1}, \quad (12)$$

where at least two of  $A_0, \dots, A_{k-1} \in \mathbb{Q}(r_1, \dots, r_{n-2})$  are nonzero. This is the most interesting, particularly difficult moment in comparison with the case  $k = 2$ . Indeed, for  $k = 2$  the equality (12) is not terrible at all:  $\sqrt{p_n} = A_0 + A_1 \sqrt{p_{n-1}}$ , the squaring is of no difficulty. But for  $k > 2$  even the idea of exponentiating of (12) to  $k$ th degree is unpleasant... Minimal polynomials again will help us. But if the minimal polynomial for the left part is found easily, for the right part even its algebraicity is not obvious.

**Example 7.** Let us obtain a contradiction in the above equality  $\sqrt[5]{3} = a + b\sqrt[5]{2}$ , where  $a, b \in \mathbb{Q}$ , this is a particular case of (12). By Lemma 1,  $a \neq 0$  and  $b \neq 0$ . By Example 5,  $\mu_{\sqrt[5]{3}}(x) = x^5 - 3$  and  $\mu_{\sqrt[5]{2}}(x) = x^5 - 2$ , hence  $\mu_{a+b\sqrt[5]{2}}(x) = (x - a)^5 - 2b^5$  (we have done the linear substitution  $x \mapsto \frac{x-a}{b}$  and multiplied by  $b^5$ ). A contradiction:

$$x^5 - 3 = (x - a)^5 - 2b^5 = x^5 - 5ax^4 + \dots \implies a = 0.$$

PROBLEM 11. Solve in positive integers:  $\sqrt[5]{m} + \sqrt[5]{n} = 2021$ .

PROBLEM 12. Disprove the equality  $\sqrt[6]{3} = a\sqrt[3]{2} + b\sqrt{2}$ , where  $a, b \in \mathbb{Q}$ .

In general, the way to the minimal polynomial of the right side in (12) passes through *conjugate numbers*. But we have defined this notion only for quadratic irrationalities, and also at the end of §2 we have indicated some argument using conjugates.

**A bit more of theory.** Suppose a number  $\alpha \in \mathbb{C}$  is algebraic over a field  $K$ , and

$$\mu_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_k)$$

(by the fundamental theorem of algebra, any polynomial over  $\mathbb{C}$  decomposes into linear factors<sup>3</sup>). The numbers  $\alpha_1, \dots, \alpha_k$  are called *conjugates for  $\alpha$*  over  $K$ . Denote their sum by  $\sigma(\alpha)$ . By Vieta theorem

$$\sigma(\alpha) = \alpha_1 + \dots + \alpha_k \iff \mu_\alpha(x) = x^k - \sigma(\alpha)x^{k-1} + \dots \quad (13)$$

Example (7) shows that just the coefficient  $-\sigma(\alpha)$  plays the key role.

*Remark.* The numbers  $\alpha_1, \dots, \alpha_k$  are different (this is not used in the proof): if  $\mu_\alpha(x) = (x - \alpha_j)^2 g(x)$  then the derivative  $\mu'_\alpha(x) = 2(x - \alpha_j)g(x) + (x - \alpha_j)^2 g'(x) \in K[x]$  has the root  $\alpha_j$  although  $\deg \mu'_\alpha < \deg \mu_\alpha$ .

Property 3) of the minimal polynomial implies that all numbers algebraic over  $K$  divide into classes of conjugates and each class consists of the roots of some polynomial irreducible over  $K$ .

**Example 8.** Decompose the binomial  $x^4 - 2$  into irreducible factors and divide its roots into classes of conjugates over each of the fields  $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$ :

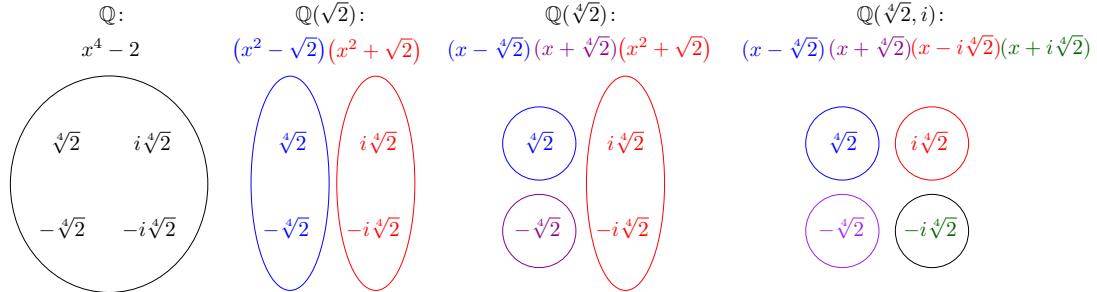


Fig. 4

**Example 9.** For square irrationalities  $a \pm b\sqrt{d}$  ( $a, b, d \in K$ ,  $b \neq 0$ ,  $\sqrt{d} \notin K$ ) this definition agrees with the usual notion of conjugacy:

$$\mu_{a \pm b\sqrt{d}}^K(x) = x^2 - 2ax + a^2 - db^2, \quad \sigma(a \pm b\sqrt{d}) = 2a.$$

(By the way, in the case  $K = \mathbb{R}$ ,  $d = -1$  we obtain complex conjugates  $a \pm bi$ .) This saves the above justification of the transition from (3) to (4).

**Example 10.** Suppose  $a, b \in \mathbb{Q}$ ,  $b \neq 0$ . The numbers  $a \pm b\sqrt[k]{2}$  are not of course conjugates when  $k > 2$  (as in the case of square irrationalities). The conjugates for  $a + b\sqrt[5]{2}$  are the roots of the polynomial  $\mu_{a+b\sqrt[5]{2}}(x) = (x - a)^5 - 2b^5$  (similarly to the example 7), that is, they are equal to  $a + b\sqrt[5]{2}\varepsilon^j$ ,  $j = 0, \dots, k-1$  (see an example at fig. 5).

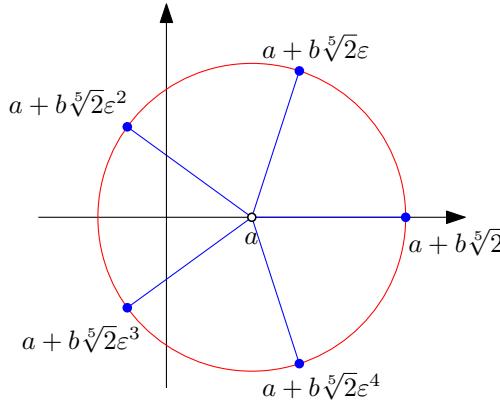


Fig. 5

<sup>3</sup>We will not use this: in the proof, all polynomials get explicit decompositions.

**Step 4: transition to conjugates.** Example 10 suggests the form of the conjugates for a number of the form (10).

**Example 11.** Let us disprove the equality  $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ , where  $a, b, c \in \mathbb{Q}$ . The conjugates for the left side are  $\sqrt[3]{3}, \sqrt[3]{3}\varepsilon, \sqrt[3]{3}\varepsilon^2$ , where  $\varepsilon = \varepsilon_3$ . On the other hand, consider the polynomial

$$F(x) = (x - (a + b\sqrt[3]{2} + c\sqrt[3]{4})) (x - (a + b\sqrt[3]{2}\varepsilon + c\sqrt[3]{4}\varepsilon^2)) (x - (a + b\sqrt[3]{2}\varepsilon^2 + c\sqrt[3]{4}\varepsilon)).$$

How can we prove  $F(x) \in \mathbb{Q}[x]$  without troublesome removal of bracelets? This is a purely algebraic issue: replace  $\sqrt[3]{2}$  by  $y$  and  $\sqrt[3]{4}$  by  $y^2$ . The resulting polynomial does not change under substitution of  $y\varepsilon$  instead of  $y$ , hence  $y$  appears in it only with degrees divided by 3. Replacing  $y^3$  by 2 we get a polynomial  $F(x) \in \mathbb{Q}[x]$ . Hence  $F(x)$  is a multiple of  $\mu_{\sqrt[3]{3}}(x) = x^3 - 3$ , and thus  $F(x) = x^3 - 3$ . But the sum of the roots of  $F$  equals  $3a$  (because  $1 + \varepsilon + \varepsilon^2 = 0$ ). Hence  $a = 0$  and  $\sqrt[3]{3} = b\sqrt[3]{2} + c\sqrt[3]{4}$ . Divide by  $\sqrt[3]{2}$ :  $\sqrt[3]{3/2} = b + c\sqrt[3]{2}$ . Similarly or as in Example 7 we obtain  $b = 0$ . Thus  $\sqrt[3]{3} = c\sqrt[3]{4}$  which is impossible by Lemma 1.

**Lemma 4.** Suppose  $K$  is a subfield in  $\mathbb{R}$ ,  $r \in \mathbb{R}$ ,  $r \notin K$ ,  $r^k \in K$  for some  $k \in \mathbb{N}$ . Then  $\sigma(r) = 0$ .

*Proof.* There exists the least  $m \in \mathbb{N}$  such that  $r^m \in K$ . By Lemma 2 the binomial  $x^m - r^m$  is irreducible over  $K$  and hence equal to  $\mu_r^K(x)$ . Since  $r \notin K$ , we have  $m > 1$  and  $\sigma(r) = 0$ .  $\square$

**Lemma 5.** Let  $\alpha_1 = \alpha, \dots, \alpha_k$  be all the conjugates for a number  $\alpha$  algebraic over a field  $K$ , and suppose  $f \in K[x]$ . Then  $f(\alpha)$  is algebraic over  $K$ , and we have for some  $d \in \mathbb{N}$

$$\mu_{f(\alpha)}(x)^d = (x - f(\alpha_1)) \dots (x - f(\alpha_k)). \quad (14)$$

*Proof.* For our goal, it suffices to consider the case  $\mu_\alpha(x) = x^k - r^k$  where  $r = \alpha$ . The equality (14) takes the form

$$\mu_{f(r)}(x)^d = (x - f(r))(x - f(r\varepsilon)) \dots (x - f(r\varepsilon^{k-1})). \quad (15)$$

1. Consider an auxiliary polynomial

$$G(x, y) = (x - f(y))(x - f(y\varepsilon)) \dots (x - f(y\varepsilon^{k-1})).$$

It does not change under replacement of  $y$  by  $y\varepsilon$  (the parentheses are moved cyclically), hence all degrees of  $y$  in it are multiples of  $k$ . Thus  $G(x, r)$  is a polynomial with coefficients in  $K$  and the root  $f(r)$ . Hence  $f(r)$  is algebraic over  $K$ , and  $\mu_{f(r)}(x)$  divides  $G(x, r)$ .

2. The polynomial  $\mu_{f(r)}(f(x)) \in K[x]$  has the root  $r$  and hence is a multiple of  $\mu_r(x) = x^k - r^k$ . Thus all roots  $r, r\varepsilon, \dots, r\varepsilon^{k-1}$  of this binomial are roots of the polynomial  $\mu_{f(r)}(f(x))$ , that is, the numbers  $f(r), f(r\varepsilon), \dots, f(r\varepsilon^{k-1})$  are conjugates.

3. Suppose  $d \in \mathbb{N}$  is the least integer such that  $\mu_{f(r)}(x)^d$  divides  $G(x, r)$ . Let us prove that  $G(x, r) = \mu_{f(r)}(x)^d$ . In fact, in the opposite case the polynomial  $G(x, r)/\mu_{f(r)}(x)^d \in K[x]$  has a root  $f(r\varepsilon^j)$  and hence is a multiple of  $\mu_{f(r\varepsilon^j)}(x) = \mu_{f(r)}(x)$ , a contradiction with minimality of  $d$ .

To prove the assertion in general case, let us consider the polynomial

$$G(x, y_1, \dots, y_k) = (x - f(y_1)) \dots (x - f(y_k)).$$

It does not change under substitutions of  $y_1, \dots, y_k$  and by the fundamental theorem on symmetric polynomials [1, p. 134] can be expressed in terms of  $x$  and elementary symmetric polynomials  $\sigma_1, \dots, \sigma_k$  defined by the equality

$$(x - y_1) \dots (x - y_k) = x^k - \sigma_1 x^{k-1} + \sigma_2 x^{k-2} - \dots + (-1)^k \sigma_k.$$

Since  $(x - \alpha_1) \dots (x - \alpha_k) = \mu_\alpha(x) \in K[x]$ , we have  $G(x, \alpha_1, \dots, \alpha_k) \in K[x]$ . The further argument is similar.  $\square$

In equality (15), equate the sums of roots (with multiplicities) in

$$d\sigma(f(r)) = f(r) + f(r\varepsilon) + \dots + f(r\varepsilon^{k-1}).$$

Calculate the right part for  $f(x) = c_0 + c_1x + \dots + c_{k-1}x^{k-1}$ :

$$\begin{aligned} f(r) &= c_0 + c_1r + \dots + c_{k-1}r^{k-1}, \\ f(r\varepsilon) &= c_0 + c_1r\varepsilon + \dots + c_{k-1}r^{k-1}\varepsilon^{k-1}, \\ &\dots \\ f(r\varepsilon^{k-1}) &= c_0 + c_1r\varepsilon^{k-1} + \dots + c_{k-1}r^{k-1}\varepsilon^{(k-1)^2}. \end{aligned}$$

Add the numbers in each column. Since  $\varepsilon^k = 1$ , then

$$1 + \varepsilon^j + \varepsilon^{2j} + \dots + \varepsilon^{(k-1)j} = \frac{1 - \varepsilon^{kj}}{1 - \varepsilon^j} = 0, \quad j = 1, \dots, k-1.$$

Hence  $f(r) + f(r\varepsilon) + \dots + f(r\varepsilon^{k-1}) = kc_0$ , so

$$\sigma(c_0 + c_1r + \dots + c_{k-1}r^{k-1}) = \frac{k}{d} \cdot c_0. \quad (16)$$

Finally we arrive to a contradiction in (12). Let  $A_j$  be the first nonzero coefficient in the sequence  $A_0, \dots, A_{k-1}$ . Divide the equality (12) by  $r_{n-1}^j$ :

$$\frac{r_n^l}{r_{n-1}^j} = A_j + A_{j+1}r_{n-1} + \dots + A_{k-1}r_{n-1}^{k-j-1}. \quad (17)$$

Suppose  $K = \mathbb{Q}(r_1, \dots, r_{n-2})$ ,  $R = r_n^l/r_{n-1}^j$ . Then  $R \notin K$ , otherwise  $R = A_j$  and  $A_{j+1} = \dots = A_{k-1} = 0$  due to linear independence of  $1, r_{n-1}, \dots, r_{n-1}^{k-1}$  over  $K$  (remind that at least two of numbers  $A_j, \dots, A_{k-1}$  are nonzero). Furthermore  $R^k = p_n^l/p_{n-1}^j \in \mathbb{Q}$ , hence  $\sigma(R) = 0$  by Lemma 4. But the value of  $\sigma$  corresponding to the right part of (17) is by (16) proportional to  $A_j$  (which plays the role of  $c_0$ ) and hence is nonzero. This contradiction proves Theorem 2.

In fact we have proved more: each number from the field  $\mathbb{Q}(r_1, \dots, r_n)$  is a linear combination of  $k^n$  numbers

$$r_1^{l_1} \dots r_n^{l_n} \quad (0 \leq l_1, \dots, l_n < k)$$

with uniquely determined rational coefficients. In terms of vectors, these numbers form a basis of the field  $\mathbb{Q}(r_1, \dots, r_n)$  over  $\mathbb{Q}$ . This representation is obtained by removal of the irrationality in the denominator, and uniqueness of the coefficients is equivalent to linear independence of the system.

### A short proof with use of trace

If you have a bit more information about algebraic numbers or know the foundations of linear algebra then you can give a short proof of Theorem 1 (without reduction to Theorem 2). The base for this argument is some value proportional to the sum of conjugates. Moreover it has the remarkable feature of linearity which minimizes the technical aspect.

A function  $f: L \rightarrow \mathbb{C}$  where  $L$  is a subfield in  $\mathbb{C}$  is called linear (more precisely,  $\mathbb{Q}$ -linear) if  $f(ax + by) = af(x) + bf(y)$  for all  $x, y \in L$  and  $a, b \in \mathbb{Q}$ . Suppose  $L = \mathbb{Q}(\sqrt[k]{Q_1}, \dots, \sqrt[k]{Q_N})$ . In §4 we will show that there exists a linear function  $\text{tr}: L \rightarrow \mathbb{C}$  called the trace, such that

$$\text{for every } \alpha \in L \text{ there exists } d \in \mathbb{N} \text{ such that } \text{tr}(\alpha) = d\sigma(\alpha) \quad (18)$$

( $\sigma(\alpha)$  is defined in (13)). Suppose that  $a_1\sqrt[k]{Q_1} + \dots + a_N\sqrt[k]{Q_N} = 0$  where not all  $a_1, \dots, a_N \in \mathbb{Q}$  are zeroes. Assume that  $a_N \neq 0$ . Surprisingly we will separate not a radical but a coefficient. Divide both parts by  $\sqrt[k]{Q_N}$  and denote  $R_i = \sqrt[k]{Q_i}/\sqrt[k]{Q_N}$ ,  $i = 1, \dots, N-1$ :

$$-a_N = a_1R_1 + \dots + a_{N-1}R_{N-1}. \quad (19)$$

Since  $R_i^{k_i k_N} \in \mathbb{Q}$  and by condition  $R_i \notin \mathbb{Q}$ , we have  $\sigma(R_i) = 0$  by Lemma 4, hence  $\text{tr}(R_i) = 0$  by (18). By linearity, the trace of the right part of (19) equals 0. On the other hand,  $\sigma(-a_N) = -a_N \neq 0$ , and by (18) we have  $\text{tr}(-a_N) \neq 0$ . This contradiction completes the proof of Theorem 1.

### §4. Appendix: regarding trace

We shall construct the function named trace  $\text{tr}: L \rightarrow L$  for any extension  $L \supseteq \mathbb{Q}$  generated by a finite set of algebraic numbers, in particular for  $L = \mathbb{Q}(\sqrt[k]{Q_1}, \dots, \sqrt[k]{Q_N})$ . We will perform this in two ways. The first way is closer to the argument in §3 and enriches it by translation to the language of Galois theory. After that we will give the basic definition of the trace, which explains its name, by the way. This way requires basic information from linear algebra:

- the basis and dimension of an extension, the tower theorem [4, §5];
- matrix operations, the inverse matrix [1, p. 41–44, 73];
- the matrix of a linear operator in a basis, its transformation under change of the basis [1, p. 234–236].

## I approach (in spirit of Galois theory)

We need the following well-known fact [4, theorem 2]: *the set  $\mathbb{A}$  of algebraic (over  $\mathbb{Q}$ ) numbers is a field.* Thus  $L \subseteq \mathbb{A}$  because  $L$  is generated by algebraic numbers over  $\mathbb{Q}$ .

Let us call the map  $\varphi: L \rightarrow \mathbb{C}$  an *inclusion* if  $\varphi(a+b) = \varphi(a) + \varphi(b)$ ,  $\varphi(ab) = \varphi(a)\varphi(b)$  for all  $a, b \in L$  and  $\varphi(c) = c$  for all  $c \in \mathbb{Q}$ . In particular,  $\varphi$  is linear:  $\varphi(ca) = \varphi(c)\varphi(a) = c\varphi(a)$  for  $c \in \mathbb{Q}$  and  $a \in L$ . In the sequel we show that there exists only a finite number of inclusions  $\varphi_1, \dots, \varphi_n$  of  $L$ . Put

$$\text{tr}(\alpha) = \sum_{j=1}^n \varphi_j(\alpha). \quad (20)$$

**PROBLEM 13.** Without further reading: a) prove that all inclusions  $\mathbb{Q}(i) \rightarrow \mathbb{C}$  are of the form  $a + bi \mapsto a \pm bi$  ( $a, b \in \mathbb{Q}$ ); b) describe all inclusions  $\mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right) \rightarrow \mathbb{C}$ . Find  $\text{tr}(1+i)$  for each case.

The inclusions discover a new approach to conjugates described above in terms of roots of irreducible polynomials. Suppose  $\alpha \in L$  and

$$\mu_\alpha(x) = x^m - c_{m-1}x^{m-1} - \dots - c_1x - c_0. \quad (21)$$

Apply any inclusion  $\varphi: L \rightarrow \mathbb{C}$  to both parts of the equality  $\mu_\alpha(\alpha) = 0$ :

$$\varphi(\mu_\alpha(\alpha)) = \varphi(\alpha)^m - c_{m-1}\varphi(\alpha)^{m-1} - \dots - c_1\varphi(\alpha) - c_0 = \mu_\alpha(\varphi(\alpha)) = \varphi(0) = 0.$$

We see that  $\varphi(\alpha)$  is conjugate to  $\alpha$ . Conversely suppose that  $\alpha_j$  is some conjugate for  $\alpha \in L$ . Does there exist an inclusion  $L \rightarrow \mathbb{C}$  such that  $\alpha$  maps to  $\alpha_j$ ? This inclusion must be determined in  $\mathbb{Q}(\alpha)$  by the rule  $f(\alpha) \mapsto f(\alpha_j)$ , where  $f \in \mathbb{Q}[x]$  (by Theorem 3 each number from  $\mathbb{Q}(\alpha)$  has this form). On the other hand, this rule is correct (does not depend on the choice of  $f$ ) and determines an inclusion  $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$  since for all  $f, g \in \mathbb{Q}[x]$  we have

$$\begin{aligned} f(\alpha) = g(\alpha) &\Leftrightarrow f(x) - g(x) \mid \mu_\alpha(x) \Leftrightarrow f(\alpha_j) = g(\alpha_j), \\ f(\alpha) + g(\alpha) &= (f + g)(\alpha), \quad f(\alpha)g(\alpha) = (fg)(\alpha). \end{aligned}$$

By the way it is not evident that this inclusion extends from  $\mathbb{Q}(\alpha)$  to  $L$  but at any rate we are already able to describe the inclusions of *simple* extensions of  $\mathbb{Q}$  (that is, extensions generated by a single number).

**Theorem 3.** Let  $\theta_1 = \theta, \dots, \theta_n$  be the conjugates of  $\theta \in \mathbb{A}$ . Then the inclusions  $\mathbb{Q}(\theta) \rightarrow \mathbb{C}$  are

$$\varphi_j: f(\theta) \mapsto f(\theta_j) \quad (f \in \mathbb{Q}[x]), \quad j = 1, \dots, n.$$

Luckily an extension generated by a finite set of algebraic numbers is generated by a single number as well (this number is called a *primitive element of the extension*).

**Example 12.** Let us show that  $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ . Inclusion  $\supseteq$  is evident. Conversely

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) \ni \frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{3} - \sqrt{2} \implies \mathbb{Q}(\sqrt{2} + \sqrt{3}) \ni \frac{\sqrt{3} + \sqrt{2}}{2} \pm \frac{\sqrt{3} - \sqrt{2}}{2} = \sqrt{3}, \sqrt{2}.$$

**Theorem 4** (on the primitive element). *There exists  $\theta \in L$  such that  $L = \mathbb{Q}(\theta)$ .*

*Proof.* It suffices to find  $\theta = \alpha + c\beta \in L$  for given  $\alpha, \beta \in L$ , such that  $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$  (we proceed by induction in the number of generators). Let  $\alpha = \alpha_1, \dots, \alpha_m$  and  $\beta = \beta_1, \dots, \beta_n$  be the conjugates of  $\alpha$  and  $\beta$ . The common roots of  $\mu_\beta(x)$  and  $\mu_\alpha(\theta - cx)$  are  $\beta_j$  such that  $\theta - c\beta_j = \alpha_i$  for some  $i$ . Choose  $c$  so that  $\alpha + c\beta \neq \alpha_i + c\beta_j$  for  $(i, j) \neq (1, 1)$ . Then  $\beta$  is the only root of the above polynomials, and since  $\mu_\beta(x)$  has no multiple roots (see the remark after (13)) we have

$$(\mu_\beta(x), \mu_\alpha(\theta - cx)) = x - \beta \in \mathbb{Q}(\theta)[x].$$

Thus,  $\beta \in \mathbb{Q}(\theta)$ , and so  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ . □

In practice it occurs simpler to use several generators but of simpler nature.

**PROBLEM 14.** Describe all inclusions of the fields  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ,  $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ ,  $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ .

Let us prove that the function (20) has the required features. The linearity of the trace follows from the linearity of inclusions. Let us prove (18). Suppose  $\alpha \in L$ . By Theorem 4  $\alpha = f(\theta)$ , where  $f \in \mathbb{Q}[x]$ . Furthermore  $\varphi_j(\alpha) = \varphi_j(f(\theta)) = f(\varphi_j(\theta))$  which equals  $f(\theta_j)$  by Theorem 3. Thus

$$\prod_{j=1}^n (x - \varphi_j(\alpha)) = \prod_{j=1}^n (x - f(\theta_j)) \stackrel{\text{Th.5}}{=} \mu_{f(\theta)}(x)^d = \mu_\alpha(x)^d, \quad d \in \mathbb{N}. \quad (22)$$

Equate the sums of roots (with multiplicities) of polynomials in the left and right sides to get (18).

## II approach (linear algebra only)

The trace  $\text{tr } A$  of a square matrix  $A = (a_{ij})$  is the sum of its diagonal elements,  $\text{tr } A = \sum_i a_{ii}$ . A straightforward checking shows that  $\text{tr}(AB) = \text{tr}(BA)$  for matrices  $A$  and  $B$  of the same size. This implies that the trace of the matrix of an operator is independent of the choice of a basis:  $\text{tr}(C^{-1}AC) = \text{tr}(C^{-1}CA) = \text{tr}(A)$ . It is called the trace of the operator.

From [4, Theorems 8 and 9] it follows that the extensions generated by a finite number of algebraic elements are just the finite extensions, that is, the extensions of finite dimension. (By the way, this is one more way to understand why  $\mathbb{A}$  is a field.) The degree of a finite extension  $L \supseteq K$  is denoted  $[L : K]$ . So let  $L \supseteq \mathbb{Q}$  be any finite extension,  $L \subset \mathbb{C}$ . Suppose  $\alpha \in L \subset \mathbb{C}$ . The trace of a linear operator  $L \rightarrow L$ ,  $x \mapsto \alpha x$ , is called the trace of the number  $\alpha$  and is denoted  $\text{tr}_{\mathbb{Q}}^L(\alpha)$ , or  $\text{tr}(\alpha)$  if the extension  $L \supseteq \mathbb{Q}$  is fixed.

**Example 13.** The matrix of multiplication by  $\sqrt[3]{2}$  in the basis  $1, \sqrt[3]{2}, \sqrt[3]{4}$  of the extension  $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$  is of the form  $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$  because  $1 \mapsto \sqrt[3]{2} \mapsto \sqrt[3]{4} \mapsto 2$ . Hence  $\text{tr}(\sqrt[3]{2}) = \text{tr } A = 0$ .

Clearly  $\text{tr}(\alpha)$  depends of  $\alpha$  linearly. We will specify the sense of the factor  $d$  in (18) and prove the formula

$$\boxed{\text{tr}(\alpha) = [L : \mathbb{Q}(\alpha)]\sigma(\alpha), \quad \alpha \in L.} \quad (23)$$

For this, let us choose a suitable basis in  $L/\mathbb{Q}$ . We retain the notation (21). Then  $1, \alpha, \dots, \alpha^{m-1}$  form a basis in  $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$ . Take any basis  $e_1, \dots, e_d$  in the extension  $L \supseteq \mathbb{Q}(\alpha)$ . By [4, Tower theorem 9]

$$\underbrace{e_1, e_1\alpha, \dots, e_1\alpha^{m-1}}_{\text{1st block}}, \dots, \underbrace{e_d, e_d\alpha, \dots, e_d\alpha^{m-1}}_{\text{dth block}}$$

form a basis in  $L \supseteq \mathbb{Q}$ . Under multiplication by  $\alpha$  the vectors of  $i$ th block transform according to the rule

$$e_i \mapsto e_i\alpha \mapsto e_i\alpha^2 \mapsto \dots \mapsto e_i\alpha^{m-1} \mapsto e_i\alpha^m = e_i(c_0 + c_1\alpha + \dots + c_{m-1}\alpha^{m-1}).$$

Hence in this basis the matrix of multiplication by  $\alpha$  is block diagonal with  $d$  identical blocks

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & c_0 \\ 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & c_{m-2} \\ 0 & 0 & 0 & \dots & 1 & c_{m-1} \end{pmatrix}$$

and its trace equals  $dc_{m-1}$ . Since  $d = [L : \mathbb{Q}(\alpha)]$  and  $c_{m-1} = \sigma(\alpha)$ , the formula (23) is proven. Observe that it also follows from (22):

$$d = \frac{n}{\deg \mu_\alpha(x)} = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = [L : \mathbb{Q}(\alpha)].$$

Thus two above definitions of the trace are equivalent.

In conclusion observe that  $\mu_\alpha(x)$  is the minimal polynomial for the operator of multiplication by  $\alpha$ , and  $\mu_\alpha(x)^d$  is its characteristic polynomial.

## References

- [1] E. B. Vinberg. A course of algebra (in Russian). M.: MCCME. 2019.
- [2] L. Kamnev. Irrationality of the sum of radicals (in Russian). Kvant, 1972, #2.
- [3] A. Kanunnikov. Algebra and geometry of complex numbers (in Russian). Kvant, 2017, #5, 6.
- [4] A. L. Kanunnikov. Algebraic numbers as vectors (in Russian). // Matematicheskoye prosveshcheniye. Ser. 3. Iss. 26. M.: MCCME. 2020. P. 91–122.
- [5] V. Oleynikov. Irrationality and irreducibility (in Russian). // Kvant, 1986, #10.
- [6] V. A. Ufnarovsky. Mathematical aquarium (in Russian). M.: MCCME. 2010.
- [7] I. Richards. An Application of Galois Theory to Elementary Arithmetic. Advances in Mathematics 13, p. 268–273. 1974.

## Solutions of the problems

**1.** All three sums of radicals are irrational because all radicals and their ratios in each sum are irrational by Lemma 1. For the radical  $\sqrt[17]{2021!}$  in the last sum it suffices to observe that the prime  $p = 2011$  appears in the decomposition of  $2021!$  with exponent 1.

**2.** a) One tuple is obtained from another using multiplication by some radical, for instance,

$$(\sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}) = \sqrt{5}(1, \sqrt{2}, \sqrt{3}, \sqrt{6}).$$

b) To draw a hypercube, first draw a 3-dimensional cube placing a square inside another square and connecting the corresponding vertices (fig. 1a). (This is top view of a cube made of jelly and deformed falling on the table.) Now we draw similarly a cube inside another cube and connect the corresponding vertices to obtain a hypercube. The radicals on the inner cube are already indicated at fig. 2b. Multiply these by  $\sqrt{7}$  to obtain the radicals for the corresponding vertices of the outer cube.

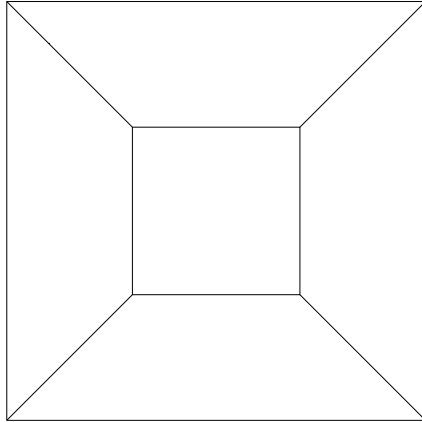


Fig. 1a

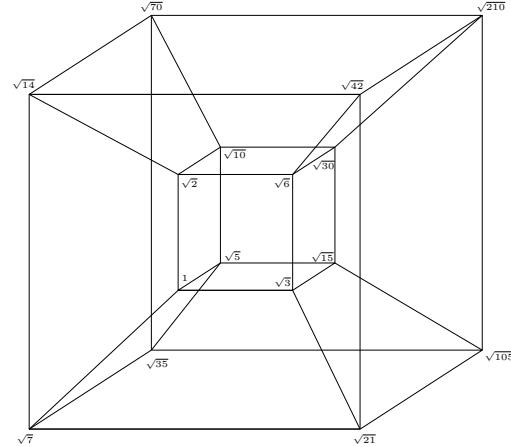


Fig. 1b

**3.**  $1 \Rightarrow 2$ . Apply Theorem 1 to  $\{Q_1, \dots, Q_N\} = \{r_1^{l_1} \dots r_n^{l_n} \mid 0 \leq l_1, \dots, l_n < k\}$  and  $k_1 = \dots = k_N = k$ . The condition  $\sqrt[k]{Q_i/Q_j} \notin \mathbb{Q}$  for  $i \neq j$  holds by Lemma 1.

$2 \Rightarrow 1$ . Let  $p_1, \dots, p_n$  be prime divisors of the numerators and denominators in the irredundant representation of  $Q_1, \dots, Q_N$  and  $k = k_1 \dots k_N$ . Then  $\sqrt[k]{Q_i} = \sqrt[k]{Q_i^{k/k_i}}$  is proportional with a rational coefficient to a number of the form  $\sqrt[k]{p_1^{l_1} \dots p_n^{l_n}}$ , where  $0 \leq l_1, \dots, l_n < k$ .

**4.** a) For zero we can take any nonzero coefficient, and for proportional numbers  $kx$  and  $lx$  ( $0 \neq k, l \in K$ ) we can take the coefficients  $l$  and  $-k$  respectively. Take the zero coefficients for the other elements of the system to get a zero linear combination with not only zero coefficients.

b) Suppose the system  $x_1, \dots, x_m, x_{m+1}, \dots, x_n$  is linearly independent over  $K$  and  $a_1x_1 + \dots + a_mx_m = 0$ . Then  $a_1x_1 + \dots + a_mx_m + 0x_{m+1} + \dots + 0x_n = 0$  implies  $a_1 = \dots = a_m = 0$ .

c) If  $x \in K$  then put  $a = x$  and  $b = -1$  in  $a \cdot 1 + b \cdot x = 0$  to obtain that 1 and  $x$  are linearly dependent over  $K$ . Conversely, if  $x \notin K$  then  $a \cdot 1 + b \cdot x = 0$  with  $a, b \in K$  implies  $b = 0$  (otherwise  $x = -a/b \in K$ ) and hence  $a = 0$ .

d) If  $a_1x_1 + \dots + a_nx_n = b_1x_1 + \dots + b_nx_n$  with  $a_1, b_1, \dots, a_n, b_n \in K$  then  $(a_1 - b_1)x_1 + \dots + (a_n - b_n)x_n = 0$ . Linear independence of  $x_1, \dots, x_n$  is equivalent to the equalities  $a_1 - b_1 = \dots = a_n - b_n = 0$ .

**5.** Suppose the theorem is proven for  $n - 1$  primes, and  $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})$ . By induction, each number in this field is uniquely expressed as a sum of  $2^{n-1}$  summands of the form  $a\sqrt{p_1}^{l_1} \dots \sqrt{p_{n-1}}^{l_{n-1}}$ ,  $a \in \mathbb{Q}$ ,  $l_i = 0, 1$ . The number  $\sqrt{p_n}$  is equal to a sum of numbers of this form but not equal to any of them by Lemma 1. Thus the sum contains at least two summands, so some radical among  $\sqrt{p_1}, \dots, \sqrt{p_{n-1}}$  appears in some summand and does not appear in another summand. Let this radical be  $\sqrt{p_{n-1}}$ . Then  $\sqrt{p_n} = A + B\sqrt{p_{n-1}}$  where  $A, B \in \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-2}}) = K$  with  $AB \neq 0$ . Square this equality:  $p_n = A^2 + B^2p_{n-1} + 2AB\sqrt{p_{n-1}}$  to get  $AB = 0$ , a contradiction.

**6.** The core of the matter is the definition of a conjugate. In *each specific* field  $K(\sqrt{d})$  conjugation is defined by the formula  $f_d(a + b + \sqrt{d}) = a - b\sqrt{d}$  ( $a, b \in K$ ). This is correct:  $a, b$  are uniquely determined since  $\sqrt{d} \notin K$ . But we may not equate conjugate related to distinct fields: if  $\alpha = a + b\sqrt{d} = a' + b'\sqrt{d'}$  then why  $f_d(\alpha) = a - b\sqrt{d}$  must equal  $f_{d'}(\alpha) = a - b\sqrt{d'}$ ?

The definition in question may be understood so that if  $\alpha$  is represented as  $a + b\sqrt{d}$  with  $a, b, d \in K$ ,  $\sqrt{d} \notin K$ , then let the conjugate to  $\alpha$  be equal to  $a - b\sqrt{d}$ . But then the implication

$$a + b\sqrt{d} = a' + b'\sqrt{d'} \implies a - b\sqrt{d} = a' - b'\sqrt{d'}$$

is nothing but verification of correctness of this definition!

The solution is to define conjugates in an invariant way not related to a specific expression in the form of a quadratic irrationality. Namely, let  $\alpha \notin K$  be a root of a polynomial of degree 2 over  $K$ . Then define the conjugate for  $\alpha$  as the second root of this polynomial. Correctness of this definition reduces to obvious verification of uniqueness of this polynomial up to a number factor. Indeed, if  $x^2 + px + q$  and  $x^2 + p'x + q'$  are two polynomials with a root  $\alpha$  over  $K$  then their difference  $(p - p')x + q - q' \in K$  also has the root  $\alpha$  whence  $p = p'$  (otherwise  $\alpha = \frac{q' - q}{p - p'} \in K$ ) and moreover  $q = q'$ . In fact the conjugates in general situation are defined just in this way.

**7.** The idea is to pass to conjugate numbers:  $(a - b\sqrt{2})^2 + (c - d\sqrt{2})^2 = 7 - 5\sqrt{2} < 0$ , a contradiction. The conceptual motivation of this transition is in verifying that the conjugation  $f(a + b\sqrt{2}) = a - b\sqrt{2}$  ( $a, b \in \mathbb{Q}$ ) is an inclusion (see definition at p. 9).

**8.** Sum up the given number and its conjugate:  $(6 + \sqrt{35})^{1000} + (6 - \sqrt{35})^{1000}$ . This sum is integer (by the formula for the Newton binomial). On the other hand, the conjugate is very small:

$$(6 - \sqrt{35})^{1000} = \frac{1}{(6 + \sqrt{35})^{1000}} < \frac{1}{10^{1000}}.$$

Hence the first 1000 digits of the original number are 9.

**9.** Consider  $2^{99}$  polynomials  $1 + \varepsilon_2x_2 + \dots + \varepsilon_{100}x_{100}$ , where  $\varepsilon_i \in \{\pm 1\}$ . Their product is a polynomial even in each variable, so it has the form  $f(x_2^2, \dots, x_{100}^2)$ , where  $f$  is a polynomial with integer coefficients. In particular, for  $x_2 = \sqrt{2}, \dots, x_{100} = \sqrt{100}$  we obtain an integer which we will denote by  $d$ . Now repeat the argument for the opposite by sign polynomials  $-1 + \varepsilon_2x_2 + \dots + \varepsilon_{100}x_{100}$  to obtain the same integer  $d$  (because the number of polynomials is even). Thus the product in question is equal to  $d^2$ .

$$\text{10. a)} \frac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}} = \frac{1}{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{(1+\sqrt{2})^2-3(\sqrt{2}-1)^2} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{8\sqrt{2}-6} = \frac{(1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3})(4\sqrt{2}+3)}{46}.$$

$$\text{b) Answer: } \frac{1}{7}(3\sqrt[4]{27} + 8\sqrt[4]{9} + 5\sqrt[4]{3} + 8).$$

**11.**  $m = k^5$ ,  $n = (2021 - k)^5$ ,  $k = 1, \dots, 2020$ . The solution is similar to Example 7.

**12.** Divide both parts by  $\sqrt[3]{2}$ :  $C\sqrt[6]{3/4} = a + b\sqrt[6]{2}$ . Now the contradiction is obtained similarly to Example 7.

**13.** We will prove a general statement.

**Lemma 6.** Let  $K$  be a subfield in  $\mathbb{C}$ ,  $r \in \mathbb{C} \setminus K$ ,  $r^2 \in K$ . Then all the inclusion  $K(r) \rightarrow \mathbb{C}$  over  $K$  (that is, identical on  $K$ ) are of the form  $a + br \mapsto a \pm br$ .

*Proof.* Clearly  $K(r) = \{a + br \mid a, b \in K\}$  and each inclusion  $\varphi: K(r) \rightarrow \mathbb{C}$  over  $K$  is determined by its value at  $r$ . Moreover  $\varphi(r)^2 = \varphi(r^2) = r^2$ , whence  $\varphi(r) = \pm r$ . For the plus sign we get an identical inclusion, and for the minus sign we get an analogue of the complex conjugation ( $K = \mathbb{R}$ ,  $r = i$ ):  $\varphi(a + br) = a - br$ . This is an inclusion over  $K$ : the properties  $\varphi(x + y) = \varphi(x) + \varphi(y)$  and  $\varphi(k) = k$  for  $k \in K$  are obvious. Furthermore

$$\varphi((a + br)(c + dr)) = \varphi(ac + bdr^2 + (ad + bc)r) = ac + bdr^2 - (ad + bc)r = (a - br)(c - dr) = \varphi(a + br)\varphi(c - dr)$$

for all  $a, b, c, d \in K$ . □

a) Apply Lemma 6 for  $K = \mathbb{Q}$  and  $r = i$ ;  $\text{tr}(1+i) = (1+i) + (1-i) = 2$ .

b) Denote  $\varepsilon = \frac{1+i}{\sqrt{2}}$ . Since  $\varepsilon^2 = i$ , we have  $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\varepsilon, i) = \mathbb{Q}(\sqrt{2}, i)$ . For any inclusion of the field  $\mathbb{Q}(\sqrt{2}, i)$  we have  $\sqrt{2} \mapsto \pm\sqrt{2}$  and  $i \mapsto \pm i$ . All combinations of signs are given by 4 inclusions: identical  $\varphi_{++}$ , inclusions from Lemma 6:

$$\varphi_{+-}: a + bi \mapsto a - bi, \quad a, b \in \mathbb{Q}(\sqrt{2})$$

$$\varphi_{-+}: a' + b'\sqrt{2} \mapsto a' - b'\sqrt{2}, \quad a', b' \in \mathbb{Q}(i),$$

and their composition  $\varphi_{--} = \varphi_{+-} \circ \varphi_{-+}$ . Hence  $\text{tr}(1+i) = (\varphi_{++} + \varphi_{+-} + \varphi_{-+} + \varphi_{--})(1+i) = 4$ .

Observe that the images of  $\varepsilon$  under all inclusions form the set of conjugates  $\left\{ \frac{1 \pm i}{\pm \sqrt{2}} \right\} = \{\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7\}$  that are the roots of  $\mu_\varepsilon(x) = x^4 + 1$ . These are the primitive roots of degree 8 from 1 (fig. 2).

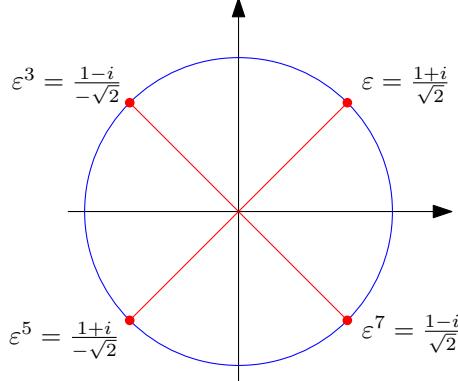


Fig. 2

**14.** Similarly to the solution of Problem 13b) we obtain 4 inclusions of the field  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  such that  $\sqrt{2} \mapsto \pm\sqrt{2}$  and  $\sqrt{3} \mapsto \pm\sqrt{3}$ . Each of these extends to an inclusion of the field  $K(\sqrt{5})$  in two ways:  $\sqrt{5} \mapsto \pm\sqrt{5}$  (similarly by Lemma 6 take three inclusions that change the sign of a radical, and form all possible  $2^3$  combinations of them).

Now let us describe the inclusions of  $L = \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$ . Put  $r = \sqrt[12]{2}$ . Then  $\sqrt[4]{2} = r^3$ ,  $\sqrt[6]{2} = r^2$  and  $L = \mathbb{Q}(r^3, r^2) = \mathbb{Q}(r)$ . By Example 5 we have  $\mu_r(x) = x^6 - 2$ , so by Theorem 3 all inclusions  $\varphi_0, \dots, \varphi_5$  of the field  $\mathbb{Q}(r)$  are defined by the conditions  $\varphi_j: r \mapsto r\varepsilon^j$ , where  $\varepsilon = \frac{1+i\sqrt{3}}{2} \in \sqrt[6]{1}$ .

# Определители в теории графов

Проект представляют О. Бурсиан, К. Кохась, В. Ретинский, Б. Френкин

26.01.2021

## 1 Предварительные сведения

**Графы.** Неформально говоря, *граф* — это множество точек (вершин), соединённых отрезками (ребрами). Формальное определение: задать граф  $G$  — значит задать множество *вершин*  $V(G)$  и множество *ребер*  $E(G)$ , состоящее из некоторых пар  $(v_1v_2)$  элементов из  $V$ . Граф называется *неориентированным*, если не учитывается порядок элементов в паре, т.е. пары  $(v_1v_2)$  и  $(v_2v_1)$  не различаются. В противном случае граф называется *ориентированным*, или сокращённо *орграфом*. В дальнейшем считаем, что множество  $V(G) = \{v_1, v_2, \dots, v_n\}$  *конечно*, тогда и множество  $E(G)$  конечно.

Если  $(v_1v_2) \in E(G)$ , то мы говорим, что *ребро*  $v_1v_2$  *соединяет* вершины  $v_1$  и  $v_2$ . Говорят также, что это ребро *инцидентно* вершинам  $v_1$  и  $v_2$ , а эти вершины *инцидентны* ребру  $v_1v_2$ . При этом вершины  $v_1$  и  $v_2$  называются *смежными*, а в противном случае *несмежными*. Если любые две вершины смежны, то граф называется *полным*.

*Степень* вершины графа — количество рёбер, инцидентных данной вершине. Степень вершины  $v$  обозначается  $\deg v$ . *Исходящая* и *входящая* степень вершины — соответственно, количество рёбер, исходящих и входящих в данную вершину.

*Квадратная числовая матрица*  $A$  порядка  $n$  — это таблица размера  $n \times n$ , в клетках которой стоят вещественные числа; число, стоящее на пересечении  $i$ -й строки и  $j$ -го столбца, обозначается  $a_{ij}$ . *Матрица смежности* неориентированного графа  $G$  — это  $n \times n$ -матрица  $A = (a_{ij})$ , в которой  $a_{ij} = 1$ , если вершины  $v_i$  и  $v_j$  смежны, и  $a_{ij} = 0$  в противном случае. Такая матрица обязательно симметрична (относительно *главной диагонали*, ведущей из левого верхнего угла в правый нижний).

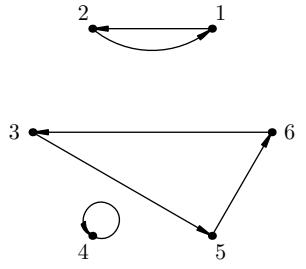
*Матрица смежности* ориентированного графа  $G$  — это  $n \times n$ -матрица  $A = (a_{ij})$ , в которой  $a_{ij} = 1$ , если в графе  $G$  есть ребро, ведущее из  $v_i$  в  $v_j$ , и  $a_{ij} = 0$  в противном случае. Такая матрица уже не обязательно симметрична.

*Путь* в графе — это последовательность  $v_{i_1}v_{i_2}, \dots, v_{i_{k-1}}v_{i_k}$  рёбер графа ( $k \geq 1$ ), где первая вершина каждого следующего ребра совпадает со второй вершиной предыдущего. Множество из одного ребра также считается путём. Если  $v_{i_k} = v_{i_1}$ , т.е. путь замкнут, то он называется *циклом*. Граф называется *связным*, если между любыми его вершинами имеется путь или вершина только одна. Граф называется *деревом*, если он связан и в нём нет циклов. Нетрудно видеть, что в этом и только этом случае между любыми двумя вершинами существует ровно один путь.

**Перестановки и их чётность.** *Перестановкой* множества  $\{1, \dots, n\}$  называется отображение этого множества в себя, при котором различные элементы переходят в различные и в каждый элемент переходит какой-то элемент — возможно, он сам. Если  $\pi$  — некоторая перестановка, то  $\pi(i)$  обозначает тот элемент, в который переходит элемент  $i$  под действием этой перестановки.

Ориентированный граф, в котором исходящая и входящая степень каждой вершины равна 1, будем называть *одновалентным*, в таком графе могут быть *петли* (ребра, у которых начало совпадает с концом). Каждая перестановка  $\pi$  определяет одновалентный граф на множестве вершин  $\{1, 2, \dots, n\}$ : этот граф содержит ориентированное ребро  $ij$  в том и только том случае, если  $\pi(i) = j$ . На рисунке приведен пример для  $n = 6$ :  $\pi(1) = 2, \pi(2) = 1, \pi(3) = 5, \pi(4) = 4, \pi(5) = 6, \pi(6) = 3$ .

*Произведение перестановок*  $\sigma$  и  $\tau$  — это перестановка, состоящая в последовательном выполнении перестановок  $\sigma$  и  $\tau$ . *Транспозиция* — это перестановка, которая меняет местами два элемента, а остальные оставляет на месте. Нетрудно видеть, что любая перестановка является произведением транспозиций. Одна и та же перестановка не может являться произведением и чётного, и нечётного количества транспозиций. Если перестановка является произведением чётного количества транспозиций, то она называется *чётной*, а в противном случае *нечётной*. Знак перестановки  $\pi$  обозначается  $\text{sgn}(\pi)$ . Если перестановка задана одновалентным графом, ее знак равен  $(-1)^m$ , где  $m$  — количество чётных (т.е. состоящих из чётного количества элементов) циклов в графе.



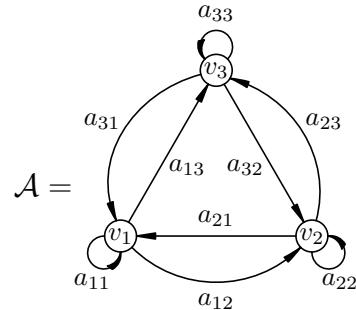
**Определитель матрицы.** Каждой квадратной матрице  $A = (a_{ij})$  сопоставим вещественное число, которое называется её *определителем* и равно сумме произведений:

$$\det A = \sum_{\pi} \text{sgn}(\pi) a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \dots \cdot a_{n,\pi(n)}, \quad (1)$$

где  $\pi$  пробегает всевозможные перестановки множества  $\{1, \dots, n\}$ . Таким образом, сумма содержит  $n!$  слагаемых. Если  $\det A = 0$ , то матрица  $A$  называется *вырожденной*, а в противном случае *невырожденной*.

Для каждой матрицы  $A$  рассмотрим полный орграф  $\mathcal{A}$  на  $n$  вершинах (с петлями), в котором каждому ребру  $v_i v_j$  сопоставлено вещественное число  $a_{ij}$ , которое называется *весом* этого ребра.

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$



Далее мы будем рассматривать только такие одновалентные подграфы орграфа  $\mathcal{A}$ , которые содержат все его вершины. Каждая перестановка  $\pi$  из суммы (1) задает одновалентный подграф в графе  $\mathcal{A}$  (и наоборот: каждый одновалентный подграф определяет перестановку). Каждому одновалентному подграфу поставим в соответствие число, равное произведению весов всех его ребер; если подграф содержит нечётное количество циклов с чётным числом вершин, дополнительно умножим это число на  $-1$ . Результат будем называть *весом* подграфа. Таким образом, вес одновалентного подграфа, соответствующего перестановке  $\pi$ , в точности равен слагаемому из суммы (1), и мы можем принять альтернативное определение.

*Определителем* матрицы  $A$  называется сумма весов всех одновалентных подграфов графа  $\mathcal{A}$ .

Для графа  $\mathcal{A}$  из нашего примера все одновалентные подграфы и их веса изображены на рис. 1. Таким образом,

$$\det A = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31}.$$

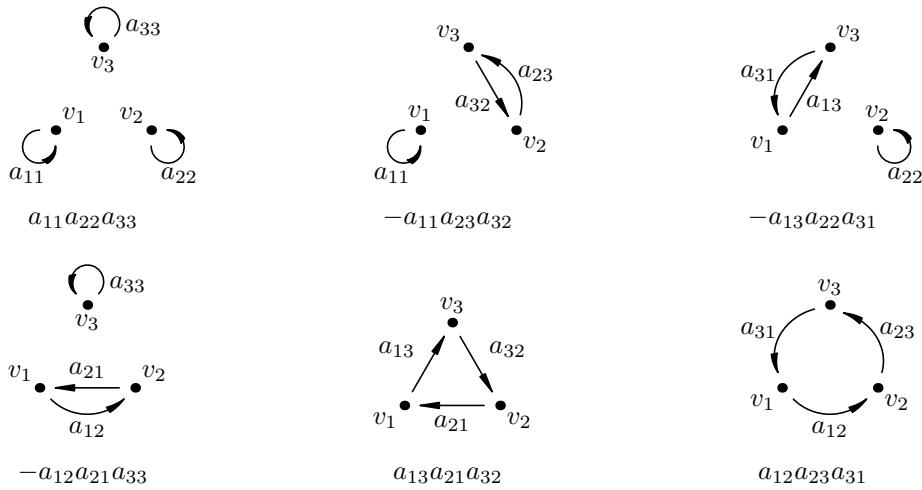


Рис. 1. Одновалентные подграфы графа  $\mathcal{A}$  и их веса

## 2 Свойства определителей

**2.1.** Пользуясь комбинаторным определением, докажите следующие свойства определителя.

- a) Если в некоторой строке матрицы  $A$  каждый элемент умножить на вещественное число  $c$ , то в результате определитель тоже умножится на  $c$ .
- b) Если в матрице поменять местами две строки, определитель сменит знак.
- c) Пусть в  $k$ -м столбце матрицы  $A$  на диагонали стоит 1, а остальные элементы  $k$ -го столбца равны нулю. И пусть  $\tilde{A}$  — матрица, получающаяся из  $A$  вычеркиванием  $k$ -й строки и  $k$ -го столбца. Тогда  $\det A = \det \tilde{A}$ .
- d) Данна матрица  $A = (a_{ij})$  и матрицы  $A^{(1)}$  и  $A^{(2)}$ , у которых все элементы такие же, как в матрице  $A$ , за исключением  $j$ -й строки, а для элементов  $j$ -й строки выполняется правило

$$a_{ij} = a_{ij}^{(1)} + a_{ij}^{(2)}.$$

Тогда  $\det A = \det A^{(1)} + \det A^{(2)}$ .

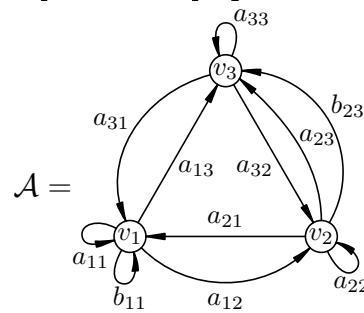
е) Обозначим через  $A_{ij}$  матрицу, которая получается вычеркиванием  $i$ -й строки и  $j$ -го столбца из матрицы  $A$ . Тогда верна формула разложения по строке

$$\det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}.$$

В связи с задачей 2.1 d) отметим следующий «лайфхак».

**2.2.** Пусть дана матрица  $A = (a_{ij})$ , в которой некоторые матричные элементы записаны в виде сумм, как в примере ниже. Построим орграф  $\mathcal{A}$ , в котором каждому слагаемому отвечает одно ребро. В отличие от стандартного случая в таком графе могут появиться кратные ребра и кратные петли (с разными весами). Определитель матрицы  $A$  по-прежнему равен сумме весов всех одновалентных подграфов построенного графа  $\mathcal{A}$ .

$$A = \begin{pmatrix} a_{11} + b_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} + b_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$



**2.3.** Пусть сумма элементов каждой строки матрицы  $A$  равна 0, а именно: в каждой диагональной клетке матрицы  $A$  стоит число, равное сумме остальных элементов той же строки со знаком минус.

a) Докажите, что  $\det A = 0$ .

b) Докажите, что  $\det A_{ij_1} = (-1)^{j_2-j_1} \det A_{ij_2}$  для каждого  $i$  и любых  $j_1, j_2$  (обозначение из задачи 2.1 е).

**2.4.** Пусть граф  $G$ , построенный по матрице  $A$ , содержит подграф  $H$  с 8 вершинами, изображённый на рис. 2 слева, причем в подграфе могут быть рёбра, инцидентные светлым вершинам, не показанные на рисунке, но все чёрные вершины имеют степень 3, т. е. все их ребра указаны. Заменим этот подграф на подграф  $H'$ , изображенный на рис. 2 справа, где новые веса задаются формулами

$$x' = \frac{y}{wz - xy}, \quad y' = \frac{x}{wz - xy}, \quad z' = \frac{w}{xy - wz}, \quad w' = \frac{z}{xy - wz}. \quad (2)$$

Пусть  $A'$  — матрица, соответствующая новому графу. Тогда

$$\det A = (xy - wz)^2 \det A'. \quad (3)$$

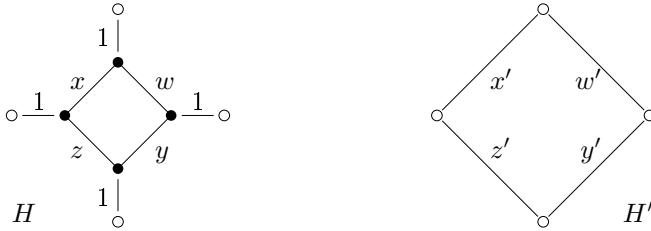


Рис. 2. Перестраиваем фрагмент графа.

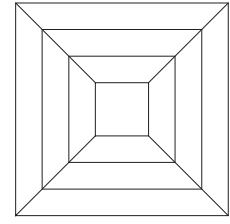


Рис. 3. Граф  $C_4 \times P_{m-1}$ .

**2.5.** Пусть  $G$  — граф, изображенный на рис. 3 (всего  $m - 1$  концентрических квадратов),  $A$  — матрица смежности этого графа. Докажите, что

$$\det A = \begin{cases} m^2, & \text{если } m \text{ нечётно,} \\ 0, & \text{если } m \text{ чётно.} \end{cases}$$

### 3 Определители клетчатых фигур

Пусть  $F$  — ограниченная клетчатая фигура на клетчатой плоскости,  $G_F$  — граф, двойственный фигуре  $F$ , т. е. граф, в котором вершины соответствуют клеткам фигуры, а рёбра соединяют вершины, соответствующие соседним по стороне клеткам. Удобно представлять себе граф  $G_F$  и его подграфы как ориентированные, полагая, что между двумя соседними клетками проведено два ребра с противоположными ориентациями. Обозначим через  $A_F$  матрицу смежности графа  $G_F$ . Замощениями будем называть разбиения фигуры  $F$  на домино. Ребро одновалентного подграфа в  $G_F$  будем называть *восходящим*, если оно вертикально и направлено вверх, и *нисходящим*, если оно вертикально и направлено вниз. (Напомним, что рассматриваются только такие одновалентные подграфы, которые содержат все вершины графа.) Фигура  $F$  называется *односвязной*, если она «без дыр» — более формально, если ее двойственный граф и двойственный граф её дополнения тоже связан.

**3.1.** Докажите, что количество одновалентных подграфов графа  $G_F$  равно квадрату количества замощений фигуры  $F$ .

**3.2.** Пусть  $P$  — односвязный клетчатый многоугольник, на границе которого  $a$  точек с чётной ординатой и  $b$  точек с нечётной, а внутри —  $d$  целочисленных точек. Тогда сумма длин вертикальных сторон многоугольника  $P$  сравнима с  $a - b + 2d + 2$  по модулю 4.

**3.3.** Пусть  $F$  — односвязная клетчатая фигура чётной площади. Тогда в её графе  $G_F$  либо чётность количества восходящих рёбер каждого одновалентного графа совпадает с чётностью количества циклов в нём, либо для каждого одновалентного подграфа эти чётности противоположны.

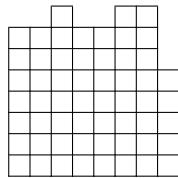


Рис. 4. Правильная 8-деталь

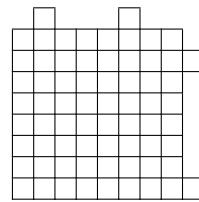


Рис. 5. Неправильная 9-деталь

Обозначим через  $c_k$  количество замощений фигуры  $F$ , в которых ровно  $k$  вертикальных домино. Многочлен  $f_F(x) = \sum_{k=0}^{+\infty} c_k \cdot x^k$  назовём *вертикальным многочленом* фигуры  $F$ . Пару замощений назовём *хорошой*, если количество вертикальных домино в них отличается ровно на 2. *Знаком фигуры*  $F$  будем называть число  $\operatorname{sgn} F = (-1)^h$ , где  $h$  — количество горизонтальных домино в любом замощении фигуры.

**3.4.** Докажите, что определение знака корректно для односвязных фигур.

**3.5.** Для каждой односвязной клетчатой фигуры  $F$

$$\begin{aligned}\det A_F &= \operatorname{sgn} F \cdot \sum_{\pi} (-1)^{m(\pi)}, \\ &= \operatorname{sgn} F \cdot f_F^2(\mathbf{i}),\end{aligned}$$

где суммирование происходит по всем одновалентным подграфам графа  $G_F$ ,  $m(\pi)$  — количество восходящих рёбер в перестановке  $\pi$ ,  $\mathbf{i} = \sqrt{-1}$ .

**3.6.** Пусть  $F$  — произвольная односвязная клетчатая фигура площади  $2s(F)$ . Если все замощения фигуры  $F$  разбиваются на хорошие пары, то  $\det A_F = 0$ . Если все замощения, кроме одного, разбиваются на хорошие пары, то  $\det A_F = (-1)^{s(F)}$ .

Будем называть *n-деталью* квадрат  $n \times n$ , у которого, возможно, вырезаны некоторые клетки, прилегающие к верхней или правой стороне. Пронумеруем строки *n-детали* числами от 1 до  $n$  снизу вверх, а столбцы — слева направо. Клетку будем обозначать парой номеров её строки и столбца. Будем называть *n-деталью правильной* (рис. 4), если из пары клеток  $(n, k)$  и  $(k, n)$  при  $k < n$  вырезана ровно одна, а также вырезана клетка  $(n, n)$ . Остальные детали будем называть *неправильными* (рис. 5).

**3.7.** Пусть  $F$  — произвольная правильная *n-деталь*. Тогда  $\det A_F = (-1)^{n(n-1)/2}$ . Если же  $F$  — неправильная *n-деталь*, то  $\det A_F = 0$ .

**3.8.** Для произвольного прямоугольника  $n \times m$

$$\det A_{n \times m} = \begin{cases} 0, & \text{если } (n+1, m+1) \neq 1; \\ (-1)^{\frac{n \cdot m}{2}}, & \text{если } (n+1, m+1) = 1; \end{cases}$$

где  $(n, m)$  — наибольший общий делитель  $n$  и  $m$ .

## 4 Остовные деревья

Пусть  $G$  — произвольный (неориентированный) связный граф. *Остовное дерево* графа  $G$  — это дерево, множество вершин которого то же, что у  $G$ , а множество рёбер содержится в множестве рёбер графа  $G$ .

Наша цель — зная строение связного графа  $G$ , найти количество его остовых деревьев. Для этого нам потребуется *матрица Лапласа* графа  $G$  — это  $n \times n$ -матрица  $L = (\ell_{ij})$ , в

которой

$$\ell_{ij} = \begin{cases} \deg v_i & \text{при } i = j; \\ -1, & \text{если } i \neq j \text{ и вершины } v_i \text{ и } v_j \text{ смежны;} \\ 0 & \text{в остальных случаях.} \end{cases} \quad (4)$$

По утверждению задачи 2.3а выполнено равенство  $\det L = 0$ . Обозначим через  $L^-$  матрицу, которая получается вычёркиванием из матрицы Лапласа последней строки и последнего столбца.

Справедлива матричная теорема о деревьях: *количество оственных деревьев связного графа равно  $\det L^-$ .*

Хорошей стартовой точкой для доказательства этой теоремы служит лайфхак из задачи 2.2 или следующая конструкция.

Представим определитель матрицы  $L^-$  как сумму произведений её элементов, при этом каждый диагональный элемент матрицы представим как сумму единиц или минус единиц и раскроем скобки. Полученное выражение назовём *сверхразложением* определителя. Каждому слагаемому сверхразложения поставим в соответствие следующий орграф с вершинами  $v_1, v_2, \dots, v_n$  и со знаками «+» и «-» на рёбрах (рис. 6). Обведём множители этого слагаемого (это единицы и минус единицы, по одной в каждой строке и каждом столбце). Если на пересечении строки  $i$  и столбца  $j$  обведена минус единица, то из  $v_i$  в  $v_j$  проводится *отрицательное* ребро (со знаком минус). Если в диагональном элементе  $a_{ii}$  обведена  $k$ -я единица, то проведём из вершины  $v_i$  *положительное* ребро (со знаком плюс) к  $k$ -му наименьшему соседу вершины  $V_i$  (это вершина  $v_j$ , смежная с  $v_i$  и такая, что имеется ровно  $k - 1$  вершин с номерами меньше  $j$ , смежных с  $v_i$ ). Как нетрудно видеть, каждый из полученных орграфов возникает из ровно одного слагаемого в сверхразложении. Теперь можно определить *знак орграфа* в целом: это знак соответствующего слагаемого в сверхразложении.

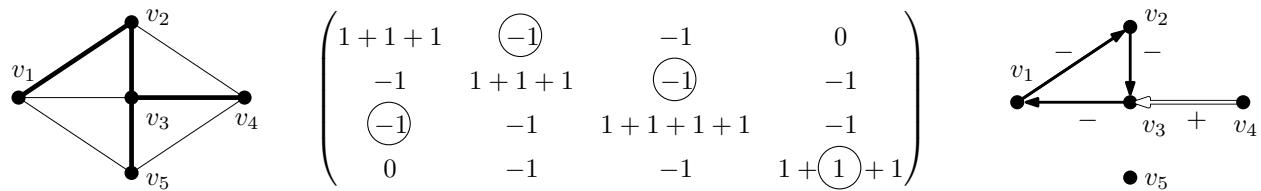


Рис. 6. Слева нарисован граф  $G$  и одно из его оственных деревьев. В центре показана матрица  $L^-$  графа  $G$ . Числа, обведенные кружками, дают одно из слагаемых сверхразложения, знак этого слагаемого равен  $(-1)^m \operatorname{sgn}(\pi)$ , где  $m$  — число выбранных минус единиц,  $\operatorname{sgn}(\pi)$  — знак перестановки, задающей это слагаемое, в нашем случае  $\pi = (2314)$ , а её знак — «+». Справа нарисован орграф, соответствующий этому слагаемому.

**4.1.** Докажите матричную теорему о деревьях.

**4.2.** Обозначим через  $E_{i,j}$  матрицу размера  $n \times n$ , в которой на пересечении  $i$ -й строки и  $j$ -го столбца стоит 1, а в остальных клетках — нули (такие матрицы называются матричными единицами). Докажите, что количество оственных деревьев графа  $G$  равно

a)  $\det(L + E_{i,i})$  для любого  $i$ ,      b)  $\det(L + E_{i,j})$  для любых  $i, j$ .

**4.3.** Пусть по-прежнему  $L$  — матрица Лапласа графа  $G$ . Зафиксируем набор вершин  $v_1, v_2, \dots, v_k$  графа  $G$  ( $k < n$ ) и вычёркнем из матрицы  $L$  столбцы и строки, соответствующие зафиксированным вершинам. Полученную  $(n - k) \times (n - k)$  матрицу обозначим через  $L_k^-$ . Подграф графа  $G$ , состоящий из  $k$  деревьев без общих вершин и рёбер с корнями  $v_1, v_2, \dots, v_k$ , содержащий все вершины графа  $G$ , назовем *остовным лесом*, посаженным в вершины  $v_1, v_2, \dots, v_k$ . При этом может оказаться, что некоторые из деревьев оственного леса состоят всего лишь из одной вершины.

Докажите, что определитель матрицы  $L_k^-$  равен количеству оственных лесов, посаженных в вершины  $v_1, v_2, \dots, v_k$ .

*Корневым ориентированным деревом* с корнем  $v$  назовем подграф орграфа  $G$ , содержащий все вершины  $G$ , в котором для каждой вершины существует единственный путь в  $v$ .

**4.4.** Пусть  $G$  — орграф без петель. Его матрица Лапласа  $L^-$  определяется формулой (4) с поправкой на то, что при  $i = j$  берется исходящая степень вершины  $v_i$ , а при  $i \neq j$  полагаем  $\ell_{ij} = -1$  лишь в случае, когда имеется ребро из вершины  $v_i$  в  $v_j$ . Докажите вариант матричной теоремы о деревьях для ориентированных графов:  $\det L^-$  равен числу корневых ориентированных деревьев с корнем  $v_n$ .

**4.5.** В орграфе без петель входящая степень каждой вершины равна исходящей. Докажите, что число ориентированных корневых деревьев с данным корнем не зависит от корня.

**4.6.** Используя матричную теорему о деревьях, докажите *формулу Кэли*: число деревьев на  $n$  пронумерованных вершинах равняется  $n^{n-2}$ .

Граф  $G$  называется *двудольным*, если множество его вершин состоит из двух непересекающихся подмножеств (*долей*), внутри которых нет рёбер.

**4.7.** Докажите, что число остовных деревьев полного двудольного графа  $K_{k,m}$  равняется  $k^{\ell-1}\ell^{k-1}$ .

**4.8.** В графе  $G$  чётное число вершин, а также степени всех вершин чётны. Докажите, что число остовных деревьев графа  $G$  чётно.

## 5 Определители и существование совершенных паросочетаний

В этом разделе мы работаем с (неориентированными) двудольными графами. Пусть  $n = 2m$ , мы будем рассматривать только двудольные графы, доли которых содержат по  $m$  (т. е. по о в и у) вершин. *Двудольной матрицей смежности* двудольного графа  $G$  называют  $m \times m$  матрицу  $B = (b_{ij})$ , в которой  $b_{ij} = 1$ , если  $i$ -я вершина первой доли соединена ребром с  $j$ -й вершиной второй доли, и  $b_{ij} = 0$  в противном случае. Если заменить в двудольной матрице смежности графа  $G$  каждый элемент  $b_{ij}$ , равный 1, на переменную  $x_{ij}$ , то полученную матрицу  $\tilde{B}$  назовём *переменной двудольной матрицей смежности* графа  $G$ .

*Совершенным паросочетанием* в графе  $G$  называется такое подмножество  $M \subseteq E(G)$  множества его рёбер, что каждая вершина графа принадлежит ровно одному ребру из  $M$ .

**5.1.** Докажите, что если доли произвольного двудольного графа  $G$  содержат поровну вершин, то существование совершенного паросочетания в графе  $G$  равносильно тому, что  $\det \tilde{B}$  не равен тождественно нулю (как многочлен).

Как проверить невырожденность двудольной матрицы смежности  $A$  за разумное время? Для этого может пригодиться следующая теорема.

**5.2. Теорема Шварца – Зиппеля.** Пусть  $d$  — натуральное число,  $S$  — множество из  $s$  вещественных чисел,  $p(x_1, \dots, x_m)$  — многочлен степени  $d$  от  $m$  переменных с вещественными коэффициентами. Тогда количество наборов  $(r_1, \dots, r_m)$ , где  $r_1, \dots, r_m \in S$  и  $p(r_1, \dots, r_m) = 0$ , не превосходит  $ds^{m-1}$ .

**5.3.** Пусть дан двудольный граф  $G$ , доли которого содержат по  $m$  вершин. Используя теорему Шварца – Зиппеля, постройте алгоритм для проверки существования совершенного паросочетания, который ошибается не более чем в половине случаев.

Многократно применяя этот алгоритм, можно сделать вероятность ошибки сколь угодно малой.

## 6 Подсчёт совершенных паросочетаний в планарном двудольном графе

Граф называется *планарным*, если его можно изобразить на плоскости без самопересечений. Это означает, что его вершины можно изобразить точками плоскости, а инцидентные им рёбра — линиями с концами в этих точках, причём внутренние точки этих линий не принадлежат другим таким линиям. Будем называть *областью* любую часть плоскости, граница которой состоит из образов рёбер, а внутренность (остальные точки области) не принадлежат образам рёбер. Для любого изображения связного планарного графа выполнена *формула Эйлера*

$$v - e + f = 2,$$

где  $v$  — количество вершин,  $e$  — количество рёбер,  $f$  — количество областей.

Если в выражении (1) для определителя матрицы  $A$  взять все слагаемые с плюсом, то получим *перманент* матрицы  $A$ , который обозначается  $\text{per}(A)$ .

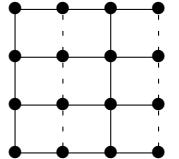
**6.1.** Докажите, что количество совершенных паросочетаний в двудольном графе равно перманенту двудольной матрицы смежности.

Вычисление перманента значительно более трудоёмко, чем вычисление определителя. Возникает вопрос: нельзя ли свести вычисление перманента двудольной матрицы смежности к вычислению определителя, поменяв знаки некоторых её элементов?

Пусть  $G$  — планарный двудольный граф. На рёбрах графа  $G$  расставим знаки «+» и «-». В его двудольной матрице смежности  $B$  заменим 1 на  $-1$ , если соответствующее ребро имеет знак минус. Расстановку знаков на рёбрах обозначим  $\sigma$ , а полученную матрицу  $B^\sigma$ . *Кастелейнова расстановка знаков* — это такая расстановка знаков  $\sigma$ , что

$$|\det B^\sigma| = \text{per}(B).$$

**6.2.** На рисунке изображен граф с 16 вершинами. Сплошные линии обозначают ребра со знаком «плюс», пунктирные — со знаком «минус». Докажите, что эта расстановка знаков кастелейнова.



Пусть  $C$  — цикл длины  $2\ell$  в двудольном графе,  $\sigma$  — расстановка знаков на рёбрах,  $n_C$  — количество отрицательных рёбер в  $C$ . Назовём цикл  $C$  *правильно помеченным* относительно  $\sigma$ , если числа  $n_C$  и  $\ell$  имеют разную чётность. Цикл  $C$  *удачно размещён*, если при удалении из  $G$  всех его вершин и смежных с ними рёбер получится граф, имеющий совершенное паросочетание. Граф называется *двусвязным*, если он связан и каждое ребро лежит хотя бы в одном цикле.

**6.3.** Пусть каждый удачно размещённый цикл правильно помечен относительно расстановки знаков  $\sigma$ . Тогда  $\sigma$  является кастелейновой. (Планарность графа не предполагается.)

**6.4.** Пусть  $G$  — планарный двудольный двусвязный граф. Зафиксируем его изображение на плоскости. Пусть  $\sigma$  — расстановка знаков на  $G$ , причём граничный цикл каждой ограниченной области на чертеже правильно помечен. Тогда расстановка знаков  $\sigma$  кастелейнова.

**6.5.** Докажите, что всякий планарный двусвязный двудольный граф имеет кастелейнову расстановку знаков.

**6.6. а)** Пусть в ориентированном графе  $G$  отмечено  $n$  вершин, имеющих только исходящие ребра (эти вершины — «входы» в граф, с них можно начать движение по графу) и  $n$  вершин, имеющих только входящие ребра («выходы»). Обозначим через  $a_{i,j}$  число способов пройти от  $i$ -го входа к  $j$ -му выходу. Докажите, что перманент матрицы  $(a_{i,j})$  равен количеству наборов, каждый из которых состоит из  $n$  путей, где каждый путь ведёт от входа к выходу, причем у любых двух путей не совпадают ни начальные, ни конечные вершины.

**б)** Пусть дополнительно известно, что граф плоский, причем все входы расположены левее всех выходов, а при движении по рёбрам вы всегда смещаетесь вправо. Докажите,

что определитель матрицы  $(a_{i,j})$  равен количеству наборов, каждый из которых состоит из  $n$  непересекающихся путей, где  $i$ -й путь ведет от  $i$ -го входа к  $i$ -му же выходу.

**6.7. а)** В левом нижнем углу доски  $n \times n$  стоит хромой король, умеющий ходить только в трёх направлениях: вправо, вверх и по диагонали вправо-вверх. Обозначим через  $A_n$  количество всех его маршрутов, ведущих в противоположный угол доски, а через  $B_n$  — количество таких маршрутов, не заходящих в левый столбец и верхнюю строку (кроме начальной и конечной позиции). Докажите, что  $B_n = 2A_{n-1}$ .

**б)** Рассмотрим матрицу  $A^{(n)} = (A_{i,j})_{1 \leq i,j \leq n}$ , где  $A_{i,j}$  — количество маршрутов хромого короля на доске  $i \times j$ , ведущих из левого нижнего угла в правый верхний. Найдите  $\det A^{(n)}$ .

**6.8.** Обозначим через  $C_n$  ( $n = 0, 1, 2, \dots$ ) количество способов пройти с левой нижней клетки доски  $(n+1) \times (n+1)$  в правую верхнюю клетку, не поднимаясь выше диагонали, если каждым ходом разрешается переходить на одну клетку вправо или на одну клетку вверх. Например  $C_2 = 2$  (проверьте!). Числа  $C_n$  называются *числами Каталана*, они могут быть вычислены по формуле  $C_n = \frac{1}{n+1} \binom{2n}{n}$ .

Пусть  $H$  — матрица  $(n+1) \times (n+1)$ , где  $h_{i,j} = C_{i+j}$  (мы считаем, что строки и столбцы матрицы нумеруются от 0 до  $n$ ). Найдите  $\det H$ .

## 7 Задачи о деревьях

**7.1.** Пусть  $G$  — дерево на  $n$  вершинах. Докажите, что тогда

$$\det A_G = \begin{cases} (-1)^{\frac{n}{2}}, & \text{если в графе } G \text{ существует совершенное паросочетание;} \\ 0 & \text{в остальных случаях.} \end{cases}$$

*Характеристическим многочленом* графа  $G$  называется определитель матрицы  $\tilde{A}_G = (\tilde{a}_{ij})$ , где

$$\tilde{a}_{ij} = \begin{cases} x & \text{при } i = j; \\ -1, & \text{если вершины } v_i \text{ и } v_j \text{ смежны;} \\ 0 & \text{иначе.} \end{cases}$$

Таким образом, характеристический многочлен является многочленом от переменной  $x$  и обозначается через  $\chi_G(x)$ .

Обозначим через  $m_k$  количество способов выбрать  $k$  ребер графа  $G$  так, чтобы никакие два ребра не были инцидентны одной и той же вершине. *Паросочетательным многочленом* графа  $G$  назовем

$$m_G(x) = \sum_{k=0}^{\left[\frac{n}{2}\right]} (-1)^k m_k x^{n-2k}.$$

**7.2.** Пусть  $G$  — дерево. Докажите, что  $\chi_G(x) = m_G(x)$ .



# Решения

**2.1.** а) Это очевидно. Умножению  $k$ -й строки матрицы  $A$  на число  $c$  соответствует умножению на  $c$  весов всех рёбер, исходящих из вершины  $v_k$ . Каждый одновалентный подграф содержит ровно одно такое ребро, значит, его вес тоже умножится на  $c$ .

б) Если в одновалентном графе имеется ребро, ведущее из вершины  $v_k$  в вершину  $v_i$ , будем называть вершину  $v_i$  последователем вершины  $v_k$ . Перемена местами  $j$ -й и  $k$ -й строк матрицы  $A$  задает следующее преобразование одновалентных подграфов: ребро, выходящее из вершины  $v_k$ , перенаправляется и ведет теперь не к последователю  $v_k$ , а к последователю  $v_j$ , а взамен ребро, выходящее из вершины  $v_j$  перенаправляется к последователю  $v_k$ . Если вершины  $v_k$  и  $v_j$  находились в разных циклах длины  $\ell_k$  и  $\ell_j$ , то в результате операции они окажутся в одном цикле длины  $\ell_k + \ell_j$ . Если же вершины находились в одном цикле, он распадётся на две части с сохранением суммарной длины. Проверить! В обоих случаях количество чётных циклов изменится на 1.

Каждый одновалентный подграф графа  $\mathcal{A}$  должен содержать петлю с вершиной  $v_k$ , тем самым, рёбра, ведущие в вершину  $v_k$  (из остальных вершин графа) не могут принадлежать ни одному одновалентному подграфу. Поэтому существует естественная биекция между одновалентными подграфами с ненулевым весом графа  $\mathcal{A}$  и одновалентными подграфами с ненулевым весом графа  $\tilde{\mathcal{A}}$ , состоящая в отбрасывании петли вершины  $v_k$ . Так как сама петля имеет единичный вес, эта биекция к тому же сохраняет вес подграфа.

с) Каждый одновалентный подграф содержит одно ребро, соответствующее какому-то элементу  $a_{ij}$  из  $j$ -й строки. Вес такого подграфа равен произведению числа  $a_{ij}$  и произведения весов оставшихся рёбер (и еще, возможно,  $-1$ ). Заменяя вес этого ребра на  $a_{ij}^{(1)}$  или  $a_{ij}^{(2)}$ , мы получим одновалентные подграфы из разложений определителей  $\det A^{(1)}$  и  $\det A^{(2)}$  и сумма весов этих подграфов равна весу первого подграфа.

д) Представим  $i$ -ю строку матрицы  $A$  в виде суммы  $n$  строк:

$$(a_{i1}, 0, \dots, 0) + (0, a_{i2}, 0, \dots, 0) + \dots + (0, 0, \dots, a_{in}).$$

В силу утверждения предыдущего пункта, достаточно проверить для каждого  $j$ , что если  $i$ -я строка матрицы  $A$  равна  $(0, \dots, 0, a_{ij}, 0, \dots, 0)$ , то  $\det A = (-1)^{j+i} a_{ij} \det A_{ij}$ .

Частный случай этого утверждения для  $j = i$  фактически разобран в пункте с). Пусть теперь для определенности  $i < j$ . Последовательно переставим в матрице  $A$   $i$ -ю строку с  $(i+1)$ -й, потом  $(i+1)$ -ю строку с  $(i+2)$ -й и т. д.,  $(j-1)$ -ю строку с  $j$ -й. В результате  $i$ -я строка матрицы  $A$  опустится на  $j$ -е место и мы получим матрицу  $B$ , у которой  $j$ -я строка имеет вид  $(0, \dots, 0, a_{ij}, 0, \dots, 0)$  — ненулевой элемент  $a_{ij}$  стоит на  $j$ -м месте, т. е. на диагонали. При этом  $B_{jj} = A_{ij}$ ,  $\det B = (-1)^{j-i} \det A = (-1)^{j+i} \det A$ , а тогда по свойству с)

$$\det A = (-1)^{j+i} \det B = (-1)^{j+i} a_{ij} \det B_{jj} = (-1)^{j+i} a_{ij} \det A_{ij},$$

что и требуется.

Как видим, рассуждение получилось не «чисто комбинаторное». Для оправдания разберем случай  $j = i+1$  на комбинаторном языке. Ограничимся рассмотрением частного случая  $n = 6, i = 3, j = 4$ . Мы хотим проверить равенство

$$\det \left( \begin{array}{cc|cc|cc} a & b & c & d & e & f \\ g & h & k & \ell & m & n \\ \hline 0 & 0 & 0 & a_{i+1} & 0 & 0 \\ o & p & q & r & s & t \\ \hline u & v & w & x & w & z \\ \alpha & \beta & \gamma & \delta & \epsilon & \phi \end{array} \right) = -a_{i+1} \cdot \det \left( \begin{array}{cc|cc|cc} a & b & c & e & f \\ g & h & k & m & n \\ \hline o & p & q & s & t \\ u & v & w & w & z \\ \hline \alpha & \beta & \gamma & \epsilon & \phi \end{array} \right)$$

Рассмотрим произвольный орграф, соответствующий матрице в левой части равенства, изменим его следующим образом: удалим все рёбра, входящие в вершину  $v_{i+1}$ , ребро  $v_i v_{i+1}$  стянем — образуется новая вершина  $v$ , рёбра, ранее выходившие из вершины  $v_{i+1}$  теперь

будут выходить из вершины  $v$ , а ребра, ранее входившие в  $v_i$ , будут входить в вершину  $v$ . Мы получим орграф, соответствующий матрице из правой части. Посмотрим, как описанная трансформация сказывается на одновалентных подграфах. Поскольку каждый одновалентный подграф исходного графа содержит ребро  $v_iv_{i+1}$  (так как это единственное ребро, выходящее из  $v_i$ ), он не содержит никакого другого ребра, входящего в  $v_{i+1}$ . Поэтому в результате трансформации из подграфа не будет удалено ни одного ребра, кроме стянутого ребра  $v_iv_{i+1}$ , вес которого учтен в виде отдельного сомножителя  $a_{ii+1}$  в правой части. При стягивании один из циклов одновалентного подграфа изменит свою чётность, поэтому изменится знак подграфа. С другой стороны, для каждого одновалентного подграфа для правой матрицы нетрудно установить, из какого (однозначно определённого) одновалентного подграфа левой матрицы он получен.

**2.2.** Пусть какой-то элемент матрицы  $A$ , например диагональный элемент на месте  $(1, 1)$ , записан в виде суммы, скажем,  $a_{11} + b_{11}$ . Заменим в орграфе  $\mathcal{A}$  две петли при вершине  $v_1$  с весами  $a_{11}$  и  $b_{11}$  на одну петлю с весом  $a_{11} + b_{11}$ . Полученный граф обозначим  $\tilde{\mathcal{A}}$ . Каждому одновалентному подграфу  $H$  орграфа  $\tilde{\mathcal{A}}$ , содержащему петлю при вершине  $v_1$ , соответствуют два одновалентных подграфа в  $\mathcal{A}$  — один с петлей при вершине  $v_1$  с весом  $a_{11}$ , а другой — с весом  $b_{11}$ . Очевидно, суммарный вес этих подграфов равен весу  $H$ . Если же одновалентный подграф орграфа  $\tilde{\mathcal{A}}$  не содержит петли при вершине  $v_1$ , то в графе  $\mathcal{A}$  найдется изоморфный ему подграф.

Суммируя по всем одновалентным подграфам, мы приходим к выводу, что при объединении двух петель в одну или, что то же самое, при замене формальной суммы  $a_{11} + b_{11}$  на ее значение, определитель матрицы не меняется. Аналогично обстоят дела с другими матричными элементами, записанными в виде формальных сумм.

**2.3. a)** [6] Рассмотрим матрицу

$$A = \begin{pmatrix} a_{12} + a_{13} + a_{14} & -a_{12} & -a_{13} & -a_{14} \\ -a_{21} & a_{21} + a_{23} + a_{24} & -a_{23} & -a_{24} \\ -a_{31} & -a_{32} & a_{31} + a_{32} + a_{34} & -a_{34} \\ -a_{41} & -a_{42} & -a_{43} & a_{41} + a_{42} + a_{43} \end{pmatrix}$$

Такую форму записи матриц с нулевой суммой строк — когда вне диагонали стоят элементы со знаком минус, а на диагонали их суммы со знаком плюс — будем считать стандартной. Дальнейшие рассуждения мы будем проводить, опираясь на этот пример, но читатель без труда восстановит детали общего доказательства.

Согласно утверждению предыдущей задачи для вычисления  $\det A$  следует перебирать одновалентные подграфы в графе  $\mathcal{A}$ , изображенном на рис. 7 слева. Но мы сейчас опишем конструкцию, которая сведет этот перебор к перебору подграфов в графе  $\mathcal{A}_1$ , получающемуся из  $\mathcal{A}$  удалением всех петель и знаков у весов рёбер (рис. 7 справа).

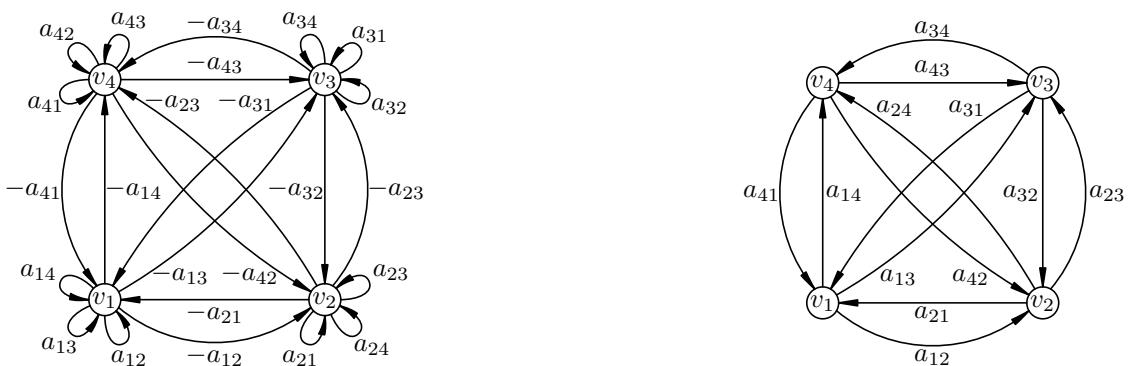


Рис. 7. Графы  $\mathcal{A}$  и  $\mathcal{A}_1$

Поскольку в графе  $\mathcal{A}$  повторяются метки, некоторые подграфы могут иметь одинаковый вес (см. рис. 8, a; не будем пока обращать внимание на знак веса). Метки на рёбрах графа  $\mathcal{A}$  — это числа  $\pm a_{ij}$ , причем индексы  $i$  и  $j$  у каждой метки различны. Очевидно, что ребро,

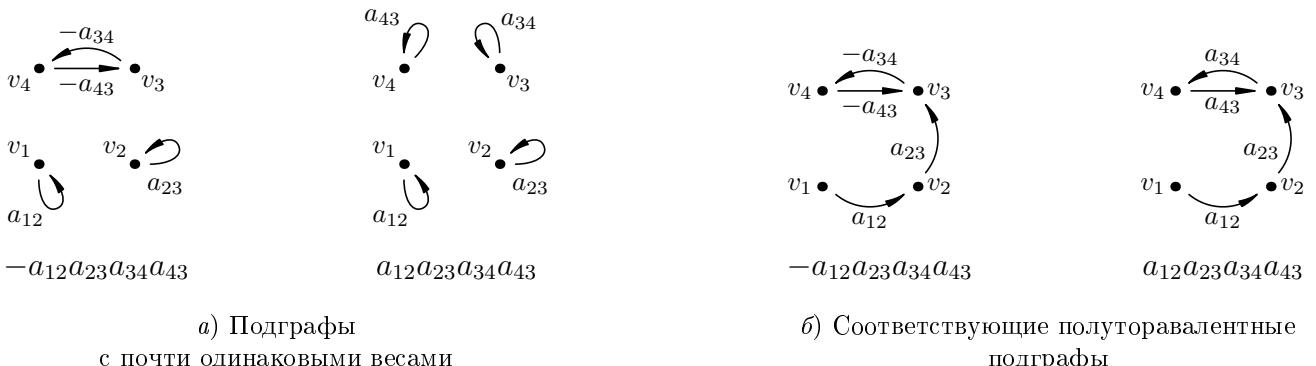


Рис. 8. Новое правило рисования подграфов

выходящее из вершины  $v_i$ , помечено меткой, у которой первый индекс равен  $i$ . Отсюда следует, что метки всех рёбер любого одновалентного подграфа графа  $\mathcal{A}$  попарно различны. Введем тогда *новое правило для изображения одновалентных подграфов* графа  $\mathcal{A}$ . Выпишем все метки рёбер одновалентного подграфа и нарисуем подграф заново (на том же множестве вершин), а именно: для каждой метки  $\pm a_{ij}$  нарисуем ребро, идущее из вершины  $v_i$  в  $v_j$ , помеченное этой самой меткой  $\pm a_{ij}$  (см. рис. 8, б). Нарисованный по новому правилу граф, очевидно, не имеет петель. Фактически это подграф графа  $\mathcal{A}_1$ , отличие только в том, что веса рёбер у нашего подграфа могут иметь лишний знак минус. Чуть позже мы устраним это отличие.

Полученные подграфы сами по себе уже не являются одновалентными. От одновалентных графов в них осталось лишь свойство, состоящее в том, что из каждой вершины выходит одно ребро. Входящих же рёбер у вершины может быть несколько или ни одного. Назовем такие графы *полупоравалентными*.

Очевидно, всякий полупоравалентный граф содержит хотя бы один цикл (двигайтесь по стрелкам — когда-нибудь вы придетете в вершину, где уже были раньше), а если он содержит несколько циклов, то эти циклы не имеют общих вершин. Кроме циклов он может содержать несколько деревьев, посаженных в вершины циклов.

Как видно из рис. 8, б, одинаковые полупоравалентные графы могут иметь разную разметку рёбер. Метка ребра  $v_i \rightarrow v_j$  полупоравалентного графа может быть равна  $+a_{ij}$  или  $-a_{ij}$ , однако если этот граф получен по описанному правилу из одновалентного, расстановка знаков не вполне хаотична. А именно: полупоравалентный граф в том и только том случае получается из одновалентного, если:

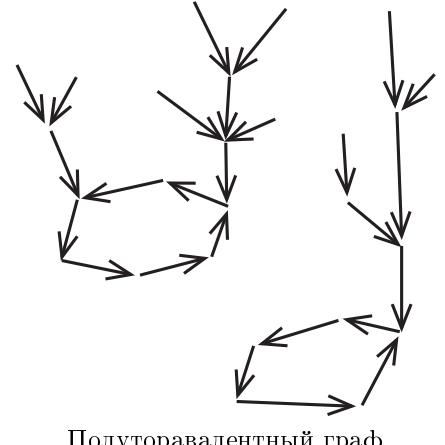
1) в каждом его цикле выполнено свойство: либо все метки рёбер цикла имеют вид  $+a_{ij}$  (такой цикл будем называть *положительным*, в одновалентном графе ему соответствовал набор петель), либо все они имеют вид  $-a_{ij}$  (такой цикл будем называть *отрицательным*, в одновалентном графе ему соответствовал этот же цикл);

2) рёбра, не входящие ни в какой цикл, имеют метки вида  $+a_{ij}$ .

Графы, обладающие этим свойством разметки рёбер, будем называть *допустимыми*.

Правило вычисления веса полупоравалентного графа такое же, как и у одновалентного: вес равен произведению весов рёбер, взятым со знаком минус, если в графе нечётное количество отрицательных чётных циклов. Мы учитываем только отрицательные чётные циклы, поскольку положительным циклам полупоравалентного графа соответствует набор петель в одновалентном графе, а петли на знак веса не влияют.

Работая с полупоравалентными графиками, удобно метки рёбер изображать вообще без знака, но при этом дополнительно помнить о знаке каждого цикла. В этом случае вес полупоравалентного графа равен произведению весов всех его рёбер, умноженному на  $(-1)^c$ , где  $c$  — количество отрицательных чётных циклов.



**Утверждение.** Определитель матрицы  $A$  равен сумме весов всех допустимых полуторавалентных подграфов в графе  $\mathcal{A}_1$ .

Собственно, доказывать тут нечего. Допустимые полуторавалентные подграфы графа  $\mathcal{A}_1$  находятся во взаимно однозначном соответствии с одновалентными подграфами графа  $\mathcal{A}$ , причем это соответствие сохраняет вес подграфа.

Вернёмся к решению задачи. Теперь совсем нетрудно проверить, что  $\det A = 0$ . Действительно, рассмотрим какой угодно допустимый полуторавалентный подграф и поменяем знак у цикла, проходящего через вершину с наименьшим номером. Мы получим другой допустимый подграф. Повторное применение этой операции приведет к исходному подграфу. Таким образом, с помощью этой операции множество всех допустимых полуторавалентных подграфов разбивается на пары. Но сумма весов графов одной пары равна нулю: если пара построена с помощью смены знака чётного цикла, то количества отрицательных циклов в графах этой пары имеют разную чётность, а набор весов рёбер одинаков; если же пара построена с помощью смены знака нечётного цикла, то при смене знака сменился знак произведения меток этого цикла.

b) Чтобы не связываться с линейной алгеброй, докажем утверждение задачи, обобщив матричную теорему о деревьях на случай взвешенных ориентированных графов. Пусть дан полный орграф  $\mathcal{A}_1$  на  $n$  вершинах без петель, в котором между любыми двумя вершинами  $v_i$  и  $v_j$  ( $i \neq j$ ) имеется как ребро  $v_i v_j$  с весом  $a_{ij}$ , так и ребро  $v_j v_i$  с весом  $a_{ji}$  (рис. 7 справа). Матрица  $A$  из условия задачи есть матрица Лапласа такого графа.

*Корневым ориентированным остовным деревом с корнем  $v_i$*  назовем такой ациклический граф на множестве вершин  $\{v_1, v_2, \dots, v_n\}$ , в котором исходящая степень вершины  $v_i$  равна 0, а любой другой вершины — 1, иными словами для любой вершины существует единственный путь из неё в  $v_i$ . Вес корневого ориентированного остовного дерева равен произведению весов его рёбер.

Утверждение задачи сразу следует из теоремы: число  $(-1)^{i+j} \det A_{ij}$  равно сумме весов всех корневых ориентированных остовных деревьев с корнем  $v_i$ .

Докажем эту теорему. Достаточно рассмотреть случай  $i = n$ , остальные случаи аналогичны. Пусть  $\tilde{A} — n \times n$  матрица, у которой  $n$ -я строка равна  $(0, \dots, 0, 1, 0, \dots, 0)$  (единица на  $j$ -м месте), а остальные матричные элементы такие же, как в матрице  $A$ . Тогда из разложения  $\det \tilde{A}$  по  $n$ -й строке получаем

$$\det \tilde{A} = (-1)^{n+j} \cdot 1 \cdot \det A_{nj}. \quad (5)$$

Будем вычислять определитель  $\det A_{nj}$  с помощью техники полуторавалентных графов. Для примера опять ограничимся случаем  $n = 5$ , пусть  $j = 2$ :

$$A_{25} = \begin{pmatrix} a_{12} + a_{13} + a_{14} + a_{15} & -a_{13} & -a_{14} & -a_{15} \\ -a_{21} & -a_{23} & -a_{24} & -a_{25} \\ -a_{31} & a_{31} + a_{32} + a_{34} + a_{35} & -a_{34} & -a_{35} \\ -a_{41} & -a_{43} & a_{41} + a_{42} + a_{43} + a_{45} & -a_{45} \end{pmatrix}.$$

Удобно полагать, что строки матрицы  $A_{nj}$  пронумерованы от 1 до  $n - 1$ , а столбцы — от 1 до  $n$ , но с пропуском номера  $j$ .

Как и в предыдущем пункте, следует в каждой строке и каждом столбце выбрать по одному числу (если соответствующий матричный элемент записан как сумма, следует взять лишь одно из слагаемых), после чего построить рёбра графа  $\mathcal{A}_1$ , соответствующие выбранным числам. Если при этом ребро имеет вес с «лишним» знаком минус (например, если в матрице был выбран элемент  $-a_{13}$ ), будем называть такое ребро отрицательным. Получится граф на вершинах  $\{v_1, \dots, v_n\}$ , обладающий следующими свойствами (рис. 9).

- 1) Исходящая степень вершин  $v_1, \dots, v_{n-1}$  равна 1, исходящая степень вершины  $v_n$  равна 0.
- 2) Из вершины  $v_j$  выходит одно «отрицательное» ребро, а входить могут только «положительные» ребра.

3) Отрицательные ребра образуют несколько циклов и еще один «неполный цикл» — путь из  $v_j$  в  $v_n$  (этот путь становится циклом, если мы дополним его ребром  $v_nv_j$ , соответствующим элементу  $a_{nj}=1$  матрицы  $\tilde{A}$ ).

4) Положительные рёбра также могут образовывать несколько циклов и еще несколько ориентированных корневых деревьев, посаженных в какие-то из вершин циклов (включая неполный цикл).

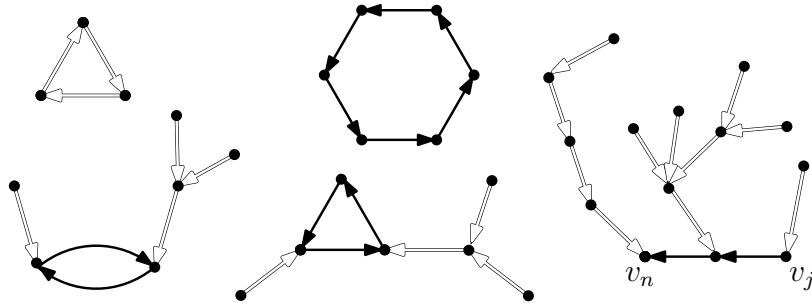


Рис. 9. Чёрным цветом обозначены «отрицательные» ребра, белым — «положительные»

Знак такого подграфа равен  $(-1)^{c+\ell}$ , где  $c$  — количество отрицательных чётных циклов,  $\ell$  — число рёбер в неполном цикле. Действительно, дополнив комплект выбранных матричных элементов, порождающих рассматриваемый подграф, элементом  $a_{nj} = 1$ , добавим к подграфу ребро  $v_nv_j$ . Получится полуторавалентный подграф, используемый в вычислении  $\det \tilde{A}$ . Неполный цикл превратится в обычный отрицательный цикл, его вклад в вычисление знака подграфа как раз и будет равен  $(-1)^\ell$ . При этом сам факт добавления к матричным элементам, выбранным на местах  $(1, \pi_1), (2, \pi_2), \dots, (n-1, \pi_{n-1})$  (здесь  $\pi$  — перестановка множества  $\{1, 2, \dots, j-1, j+1, \dots, n\}$ , нумерующего столбцы матрицы  $A_{nj}$ ), ещё одного множителя  $a_{nj}$  создаёт перестановку множества  $\{1, 2, \dots, n\}$ , в которой на  $n-j$  транспозиций больше, чем в  $\pi$ . Поправочный знак  $(-1)^{n-j} = (-1)^{n+j}$  относится ко всем рассматриваемым полуторавалентным подграфам, и именно его мы и видим в формуле (5).

Итак, вычисление определителя  $\det A_{ij}$  сводится к суммированию с надлежащими знаками весов всех полуторавалентных подграфов со свойствами 1)–4). Применяя инволюцию из предыдущего пункта (смена знака цикла, проходящего через вершину с наименьшим номером), мы сократим все подграфы, содержащие хотя бы один цикл. Рассмотрим любой несократившийся подграф, он представляет собой ориентированное дерево с корнем  $v_n$ . Пусть он содержит  $\ell$  отрицательных рёбер (это ребра «неполного цикла»), знак этого подграфа равен  $(-1)^\ell$ , и это же значение имеет произведение знаков «отрицательных» рёбер. Таким образом, итоговый вес этого подграфа — это произведение весов рёбер дерева.

Итак, подсчитываемый определитель есть сумма весов всех ориентированных деревьев с корнем  $v_n$ .

**2.4.** Мы взяли эту задачу в [2, лемма 2.1]. В приводимом рассуждении одновалентные подграфы называются *1-факторами*.

Разобьем все 1-факторы графов  $G$  и  $G'$  на группы, у которых одинаково устроено пересечение с подграфами  $H$  и  $H'$  соответственно. После этого предъявим взаимно однозначное соответствие между этими группами (а иногда даже между отдельными 1-факторами), сохраняющее суммарный вес.

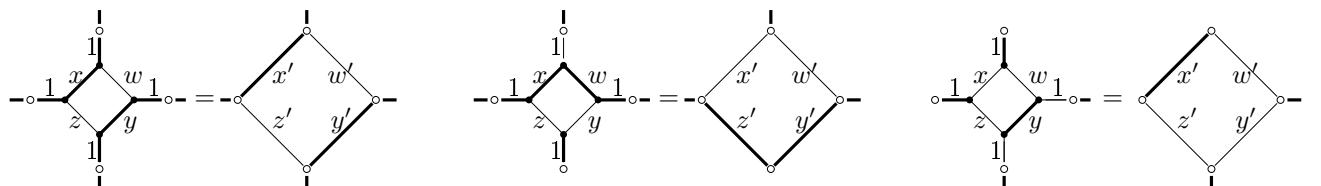


Рис. 10. Перестраиваем 1-факторы.

1) Каждому 1-фактору графа  $G$ , имеющему циклы, проходящие по рёбрам  $x$  и  $y$  в подграфе  $H$ , поставим в соответствие 1-фактор графа  $G'$ , в котором эти фрагменты циклов заменены на рёбра  $x'$ ,  $y'$  (рис. 10 слева). Указанные фрагменты циклов в подграфе  $H$  давали вклад  $xy$  в вес 1-фактора. После замены мы имеем вес  $x'y' = \frac{xy}{(wz-xy)^2}$ , а также множитель  $(wz-xy)^2$  в правой части равенства (3). В итоге вес не изменился. Аналогично поступим, если циклы проходят по рёбрам  $w$ ,  $z$ .

2) Каждому 1-фактору графа  $G$ , имеющему длинный цикл, проходящий по рёбрам  $x$ ,  $w$  в подграфе  $H$ , и цикл длины 2, проходящий по вертикальному ребру (рис. 10 в центре), поставим в соответствие 1-фактор графа  $G'$ , в котором 2-цикл отсутствует, а фрагмент длинного цикла заменен на пару рёбер  $z'$ ,  $y'$ . Аналогично поступим для конфигураций, содержащих 2-цикл, проходящий по ребру  $y$ , и два 2-цикла, примыкающих к ребру  $x$  (рис. 10 справа), а также для похожих конфигураций. Сохранение веса проверяется так же, как в предыдущем пункте.



Рис. 11. Перестраиваем группы 1-факторов.

3) Соберём в одну группу 1-факторы графа  $G$ , которые совпадают вне графа  $H$  и при этом содержат либо цикл, проходящий по рёбрам  $z$ ,  $y$ ,  $w$  (дающий вклад  $yzw$  в вес 1-фактора), либо 2-цикл по ребру  $y$  и длинный цикл, проходящий через  $x$  (и дающий вклад  $xy^2$ ). Следует иметь в виду, что эти две конфигурации имеют разные знаки, поскольку количества циклов в них отличаются на 1. Каждой группе сопоставим 1-фактор в  $G$ , который вне графа  $H$  устроен так же (и поэтому вклад внешней части один и тот же для всех упомянутых 1-факторов) и при этом содержит ребро  $x'$  (рис. 11 слева). Опять получаем равенство весов, поскольку  $yzw - xy^2 = (wz-xy)^2x'$ . Аналогично разбирается “двойственный” случай (рис. 11 справа).

4) Аналогично разбираются оставшиеся варианты (рис. 12). Отметим только, что правый цикл, показанный на рис. 12 сверху, и левый цикл на рис. 12 снизу должны рассматриваться с обеими возможными ориентациями, что удваивает их вклад. Равенство весов на рис. 12 обеспечивается тождествами

$$1 = (wz-xy)^2(x'^2y'^2 + w'^2z'^2 - 2x'y'w'z') \quad \text{и} \quad x^2y^2 + w^2z^2 - 2xywz = (wz-xy)^2.$$

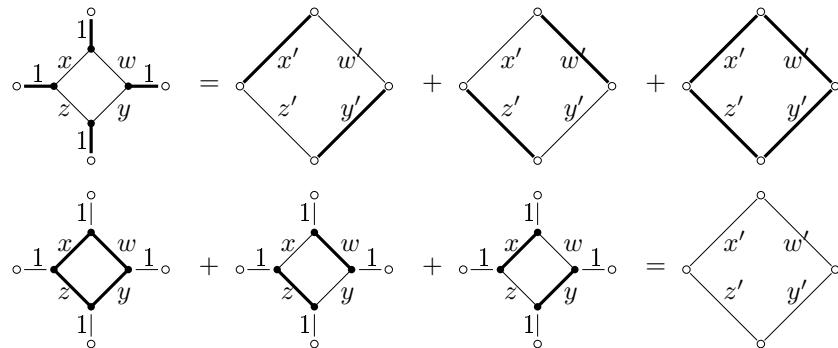


Рис. 12. Остальные отождествления.

## 2.5. Мы взяли эту задачу в [2, пример 2.2].

Пользуясь утверждением задачи 2.4, будем последовательно удалять 4-циклы на краю цилиндра (рис. 13). Чтобы избежать при вычислениях нулей в знаменателях, будем считать,

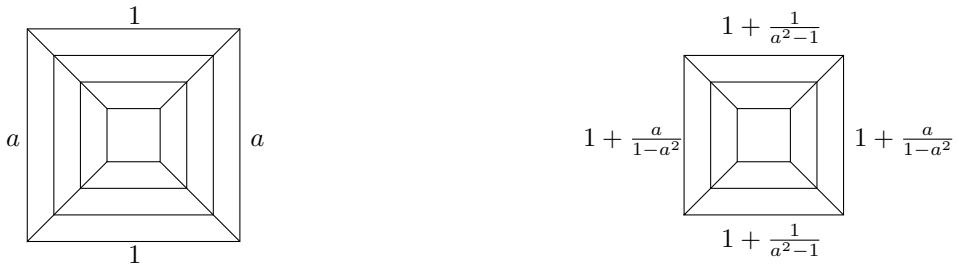


Рис. 13. Удаляем цикл на краю цилиндра.

что рёбра цикла  $H_0$  на краю цилиндра имеют веса  $x_0 = a$ ,  $z_0 = 1$ ,  $y_0 = a$ ,  $w_0 = 1$ , а все остальные рёбра в графе имеют вес 1. После применения одной операции крайний цикл исчезает, и теперь на краю появляется новый цикл  $H_1$ . Веса его рёбер равны сумме весов рёбер, которые еще до операции присутствовали в графе – а в графе было четыре ребра веса 1 – и новых рёбер, веса которых равны  $\frac{a}{1-a^2}$ ,  $\frac{1}{a^2-1}$ ,  $\frac{a}{1-a^2}$ ,  $\frac{1}{a^2-1}$  в силу формулы (2). Итак,

$$x_1 = 1 + \frac{a}{1-a^2}, \quad z_1 = 1 + \frac{1}{a^2-1}, \quad y_1 = 1 + \frac{a}{1-a^2}, \quad w_1 = 1 + \frac{1}{a^2-1}.$$

Теперь по индукции проверяется, что после  $2n$  повторений этой операции (индукция с шагом 2 удобна, поскольку формулы после чётного и нечётного числа операций немного отличаются) веса в крайнем цикле будут равны

$$x_{2n} = y_{2n} = \frac{na^2 + a}{2na + 1}, \quad z_{2n} = w_{2n} = \frac{1 + 2na - na^2}{2na + 1},$$

а произведение определителей всех убранных циклов равно

$$\det A(H_0) \det A(H_1) \dots \det A(H_{2n-1}) = (2na + 1)^2.$$

В результате если  $m$  чётно, скажем  $m - 1 = 2n + 1$ , то после  $2n$  операций от исходного графа останется лишь один 4-цикл с весами рёбер, указанными выше. Определитель матрицы такого цикла равен

$$(x_{2n}y_{2n} - z_{2n}w_{2n})^2 = \left( \frac{(2n+1)a + 1}{2na + 1} \right)^2 (a - b)^2,$$

и, значит, искомый определитель равен

$$\det A(H_0) \det A(H_1) \dots \det A(H_{2n}) (x_{2n}y_{2n} - z_{2n}w_{2n})^2 = ((2n+1)a + 1)^2 (a - b)^2.$$

При  $a = b = 1$  это выражение равно 0. Если же  $m$  нечётно, аналогично получаем, что определитель равен  $((m-1)a + 1)^2$ , и при  $a = b = 1$  это выражение равно  $m^2$ .

**3.1.** [1, теорема 2.1]. Покрасим клетки фигуры в шахматном порядке, и рёбра каждого одновалентного графа разобьём на две группы — рёбра, выходящие из чёрных вершин, и рёбра, выходящие из белых. Рёбра каждой группы задают паросочетание, которому, в свою очередь, соответствует замощение. Это соответствие является биекцией.

**3.2.** [1, лемма 2.3]. Индукция по площади. Если в двойственном графе есть висячая вершина, отрежем соответствующую клеточку. В противном случае отрежем подходящую угловую клетку.

Отметим, что если допускать вырожденные многоугольники, а именно — «двуугольники» (циклы из двух вершин и двух встречных рёбер), то утверждение задачи верно и для них.

**3.3.** [1, теорема 2.4]. Рассмотрим любой одновалентный подграф. Очевидно, что количество восходящих и нисходящих рёбер в нем одинаково, обозначим это количество через  $v$ .

Подграф представляет собой набор нескольких, скажем  $k$ , циклов, т.е. клетчатых многоугольников. Поскольку все циклы чётные и в совокупности содержат все клетки, а фигура односвязная, внутри каждого цикла содержится чётное число клеток. В силу этого, применив утверждение предыдущей задачи к каждому циклу, мы можем не учитывать слагаемое  $2d$ . Суммируя по всем циклам, получаем, что

$$A - B + 2 \cdot k \equiv_{\text{mod } 4} \text{сумма длин вертикальных сторон} = 2 \cdot v,$$

где  $A$  — суммарное количество точек с чётными ординатами,  $B$  — суммарное количество точек с нечётными ординатами на границах всех циклов. Так как одновалентный подграф содержит все целочисленные узлы фигуры, разность  $A - B$  чётна и не зависит от подграфа, положим  $A - B = 2 \cdot t$ . Тогда  $2 \cdot v \equiv 2 \cdot t + 2 \cdot k \pmod{4}$ , откуда  $v \equiv t + k \pmod{2}$ . Поскольку  $t$  не зависит от подграфа, утверждение доказано.

**3.4.** [1, лемма 2.5]. Задача тривиально решается с помощью раскраски «горизонтальная зебра», но мы приведем другое рассуждение.

Будем интерпретировать замощение как одновалентный подграф, где каждая доминошка определяет 2-цикл, тогда число циклов — это количество доминошек, число восходящих рёбер — это количество вертикальных доминошек. Отсюда

$$\begin{aligned} &\text{число циклов} + \text{число восходящих рёбер} = \\ &= \text{число домино} + \text{число вертик. домино} \equiv_{\text{mod } 2} \text{число гориз. домино}. \end{aligned} \quad (6)$$

Как мы знаем из предыдущей задачи, чётность суммы в левой части не зависит от одновалентного подграфа (и, в частности, от замощения), следовательно, чётность количества горизонтальных домино во всех замощениях фигуры одинакова. Значит, определение знака не зависит от замощения.

Отметим одно следствие из сделанных наблюдений. Если  $\text{sgn}F = 1$ , т.е. в правой части формулы (6) стоит чётное число, то в любом замощении (а тогда и в любом одновалентном подграфе в силу утверждения задачи 3.3) чётность количества восходящих рёбер совпадает с чётностью числа циклов, а если  $\text{sgn}F = -1$ , эти чётности противоположны. Иными словами, для любого одновалентного подграфа  $\pi$  в графе  $G_F$

$$(-1)^{\text{количество восходящих рёбер в } \pi} = \text{sgn}F \cdot (-1)^{\text{количество циклов в } \pi}. \quad (7)$$

Напомним, что график  $G_F$  двудольный, все циклы в нем чётные, поэтому заключаем, что верна формула

$$\det A_F = \text{sgn}F \cdot \sum_{\pi} (-1)^{\text{количество восходящих рёбер в } \pi}. \quad (8)$$

**3.5.** [1, теорема 2.7]. Обозначим через  $\gamma_k$  количество одновалентных подграфов графа  $G_F$ , имеющих  $k$  восходящих рёбер. Тогда

$$\det A_F = \text{sgn}F \cdot \sum_{\pi} (-1)^{\text{количество восходящих рёбер в } \pi} = \text{sgn}F \cdot \sum_{k=0}^{+\infty} \gamma_k \cdot (-1)^k. \quad (9)$$

Благодаря биекции из задачи 3.1 ясно, что коэффициент при  $x^k$  в выражении  $f_F(x)^2$  равен количеству одновалентных подграфов, у которых ровно  $k$  вертикальных рёбер. Количество восходящих рёбер в одновалентном подграфе равно половине числа вертикальных рёбер, откуда  $f_F(x)^2 = \sum_{k=0}^{+\infty} \gamma_k x^{2k}$ . Подставляя сюда  $x = \mathbf{i}$ , из формулы (9) получаем требуемое.

В частности, мы установили формулу

$$\det A_F = \text{sgn}F \cdot f_F(\mathbf{i})^2. \quad (10)$$

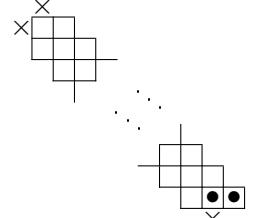
**3.6.** [1, теорема 2.8]. Будем вычислять  $\det A_F$  по формуле (10). Если хорошая пара содержит замощение с  $k$  вертикальными домино и замощение с  $k + 2$  вертикальными домино, то её

вклад в  $f_F(\mathbf{i})$  равен  $\mathbf{i}^k + \mathbf{i}^{k+2} = 0$ . Тем самым все хорошие пары вносят нулевой вклад в  $f_F(\mathbf{i})$ . Отсюда следует первое утверждение.

Если все замощения, кроме одного, разбиты на хорошие пары, обозначим через  $v$  и  $h$  количество вертикальных и горизонтальных домино в замощении, оставшемся без пары,  $h+v = s(F)$ . Тогда  $f_F(\mathbf{i}) = \mathbf{i}^v$  в силу предыдущего рассуждения,  $\text{sgn}F = (-1)^h$ , и следовательно,  $\det A_F = \text{sgn}F \cdot f_F^2(\mathbf{i}) = (-1)^{h+v} = (-1)^{s(F)}$ .

**3.7.** [1, теорема 2.11]. Выражение  $n(n-1)$  в доказываемой формуле — это площадь правильной детали. По утверждению задачи 3.6 достаточно проверить, что для каждой правильной детали все её замощения, кроме одного, разбиваются на хорошие пары, а для каждой неправильной — все замощения разбиваются на хорошие пары. И то, и другое проверяется индукцией по  $n$ . Для доказательства нам понадобится следующая лемма [4, лемма 2.1].

**Л е м м а** (о полуdiagонали). Пусть фигура  $F$  содержит фрагмент, состоящий из трёх диагональных рядов клеток, показанных на рисунке, причём клетки, помеченные крестиками, не принадлежат фигуре. Тогда множество замощений фигуры  $F$ , не содержащих доминошку, помеченную жирными кружочками, разбивается на хорошие пары.



**Д о к а з а т е л ь с т в о л е м м ы.** Рассмотрим средний из этих диагональных рядов. Докажем, что найдется квадрат  $2 \times 2$ , состоящий из двух доминошек замощения и содержащий две клетки этого диагонального ряда (переставляя доминошки в таком квадрате, мы легко разобьем множество разбиений на пары). Действительно, если такого квадрата не найдется, то, просматривая этот ряд клеток, начиная с верхнего левого угла, мы видим, что каждая очередная доминошка, накрывающая диагональную клетку, должна накрывать также либо клетку справа, либо клетку снизу. Дойдя до правого нижнего угла, получаем противоречие.

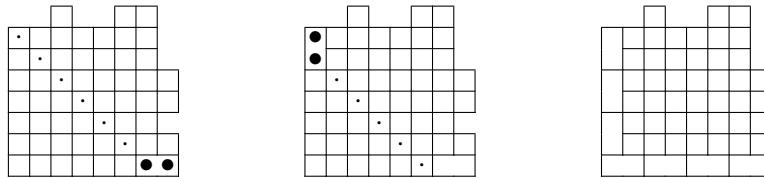


Рис. 14. Строим непарное замощение  $(n+1)$ -детали

Вернёмся к решению задачи.

1) Проверим индукцией по  $n$  (размеру детали), что все замощения каждой правильной детали, кроме одного, разбиваются на хорошие пары. База тривиальна.

Переход  $n \rightarrow n+1$ . Возьмем правильную  $(n+1)$ -деталь разобьем множество её замощений на хорошие пары. Для этого рассмотрим правый нижний и левый верхний углы  $(n+1)$ -детали. Какая-то из этих двух клеток лежит внутри квадрата со стороной  $n$ , пусть для определённости это левый верхний угол. Запустим вправо-вниз из этой клетки лемму о полуdiagонали. В силу этой леммы замощения, не содержащие доминошку, отмеченную на рис. 14 слева, разбиваются на хорошие пары. Рассмотрим замощения, содержащие эту доминошку. Запустим влево-вверх из клетки, прилегающей к ней слева, лемму о полуdiagонали (рис. 14, в центре). По этой лемме замощения, не содержащие отмеченную доминошку в левом верхнем углу, тоже разбиваются на хорошие пары. Рассмотрим оставшиеся замощения, они содержат и эту доминошку. Далее запустим лемму о диагонали вправо-вниз из клетки, прилегающей к этой доминошке снизу и т.д. В результате этих применений леммы о диагонали, неразбитыми на пары останутся лишь замощения, содержащие домино вдоль левой и нижней стороны нашей  $(n+1)$ -детали (рис. 14, справа). Эти замощения взаимно однозначно соответствуют замощениям оставшейся  $n$ -детали. Поэтому все они, кроме одного, разбиваются на хорошие пары.

2) Проверим индукцией по  $n$ , что замощения любой неправильной детали разбиваются на хорошие пары. База тривиальна.

Переход  $n - 1 \rightarrow n$ . Рассмотрим произвольную  $n$ -деталь. Обозначим некоторые клетки её квадрата  $n \times n$  как показано на рис. 15.

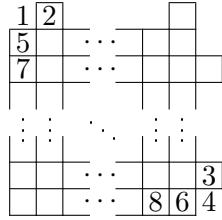


Рис. 15. Разметка клеток для неправильной детали

Рассмотрим случаи:

1) Клетки 1 и 4 не принадлежат детали. Тогда начнём строить диагональ из 5 в 6. По лемме о полудиагонали замощения разбиваются на пары (поскольку отмеченная доминошка не лежит в фигуре). Аналогично — если четыре клетки 1, 2, 3, 4 принадлежат детали.

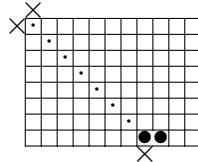
2) Клетка 1 принадлежит детали, а 4 не принадлежит. Или наоборот. Разберём первый вариант, второй аналогичен. Запустим рассуждение леммы о полудиагонали из 6 в 1. Как и в доказательстве предыдущего пункта теоремы, мы разобьём на пары все замощения, кроме тех, у которых расположение доминошек вдоль левого столбца и нижней строки фиксировано как на рис. 14 справа. Остальные замощения разбиваются на хорошие пары по индукционному предположению.

3) Клетки 1 и 4 принадлежат детали, а 2 и 3 — нет. Тогда любое замощение содержит доминошки 1 — 5 и 4 — 6. Вырежем их. По лемме о полудиагонали, запущенной из 7 в 8, замощения разбиваются на хорошие пары.

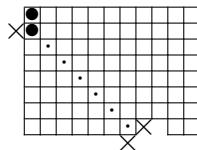
4) Клетки 1, 2, 4 принадлежат детали, а 3 — нет. Аналогично, когда 1, 3, 4 принадлежат, а 2 — нет. Очевидно, что в любом замощении присутствует домино 4 — 6. Вырежем его. Запустим лемму о полудиагонали из 8 в 7 и, действуя аналогично случаю 2, сведём вопрос к предположению индукции.

**3.8. [4, теорема 1.2].** Проверим, что количество разбиений прямоугольника  $m \times n$  на домино нечётно тогда и только тогда, когда числа  $m + 1$  и  $n + 1$  взаимно просты, причем в случае, когда количество разбиений чётно, все они разбиваются на хорошие пары, а если нечётно — все, кроме одного, разбиваются на хорошие пары. Тогда утверждение задачи будет следовать из задачи 3.6.

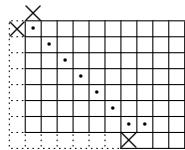
Индукция, реализующая алгоритм Евклида. Рассмотрим диагональный ряд клеток, выходящий из угла. По лемме о полудиагонали, достаточно ограничиться изучением чётности количества разбиений, содержащих отмеченную доминошку.



Теперь мы можем взять диагональный ряд клеток снизу от только что рассмотренного и, просматривая его снизу вверх, снова применить лемму о полудиагонали.



Продолжая опускать рассматриваемую диагональ, не изменяя чётности числа разбиений, мы сможем убрать все клетки первого столбца, а также все клетки нижней строки, лежащие левее отмеченной доминошки. После этого опять можно применить лемму о полудиагонали.



Продолжая дальше, мы уберем клетки второго столбца и второй строки (лежащие левее найденной доминошки). Действуя таким образом, мы уберем в конце концов из нашего прямоугольника  $m \times n$  прямоугольную часть размера  $(n+1) \times n$ . Осталась часть  $(m-n-1) \times n$ , которая удовлетворяет предположению индукции.

**4.1.** Пусть  $\mathcal{D}$  обозначает множество всех орграфов со знаками  $D$ , полученных из слагаемых сверхразложения (как описано перед условием задачи). Соответствующую перестановку обозначим  $\pi_D$ .

Разделим  $\mathcal{D}$  на три части следующим образом:

- $\mathcal{T}$ , орграфы  $D \in \mathcal{D}$  без направленных циклов;
  - $\mathcal{D}^+$ , орграфы  $D \in \mathcal{D}$  с  $\text{sgn}(D) = +1$  и хотя бы одним направленным циклом;
  - $\mathcal{D}^-$ , орграфы  $D \in \mathcal{D}$  с  $\text{sgn}(D) = -1$  и хотя бы одним направленным циклом.

Дальнейший план доказательства таков. Мы покажем, что все  $D \in \mathcal{T}$  — “ациклические объекты” — имеют положительный знак и взаимно однозначно соответствуют остовным деревьям графа  $G$ ; таким образом, их количество нам и нужно. Затем, построив подходящую биекцию, мы докажем, что  $|\mathcal{D}^+| = |\mathcal{D}^-|$ . Тогда

$$\det(L^-) = \sum_{D \in \mathcal{D}} \text{sgn}(D) = |\mathcal{T}| + |\mathcal{D}^+| - |\mathcal{D}^-| = |\mathcal{T}|$$

и теорема доказана.

Чтобы осуществить этот план, вначале перечислим несколько простых свойств орграфов из  $\mathcal{D}$ .

- (i) Если  $v_i v_j$  — направленное ребро в орграфе  $D$ , то  $v_i v_j$  — ребро графа  $G$ . (Очевидно.)
  - (ii) Из каждой вершины, кроме  $v_n$ , выходит ровно одно ребро, а из  $v_n$  ни одно ребро не выходит. (Очевидно.)
  - (iii) Все рёбра, входящие в  $v_n$ , положительны. (Поскольку отрицательные ребра, входящие в произвольную вершину  $v_j$ , соответствуют элементам  $j$ -го столбца матрицы  $L$ , а при построении матрицы  $L^-$  столбец с номером  $n$  был вычеркнут.)
  - (iv) В каждую вершину входит не более одного отрицательного ребра. (Поскольку два отрицательных входящих ребра  $v_j v_i$  и  $v_k v_i$  означали бы два обведённых элемента  $\ell_{ji}$  и  $\ell_{ki}$  в  $i$ -м столбце.)
  - (v) Если в вершину  $v_i$  входит отрицательное ребро, то исходящее ребро также отрицательно. (Действительно, отрицательное входящее ребро  $v_j v_i$  означает, что обведён недиагональный элемент  $\ell_{ji}$  и потому не может быть обведена единица в диагональном элементе  $\ell_{ii}$  — а это единственный способ получить положительное ребро, исходящее из  $v_i$ .)

Утверждение A. Перечисленные свойства характеризуют  $\mathcal{D}$ . Иными словами, если орграф  $D$  со знаками удовлетворяет условиям (i)–(v), то  $D \in \mathcal{D}$ .

Докажем это. Для данного  $D$  найдём обведённый элемент в каждой строке  $i$  ( $1 \leq i \leq n-1$ ) матрицы  $L^-$ . Рассмотрим единственное выходящее из него ребро  $v_i v_j$ . Если оно положительно, то обведём соответствующую единицу в элементе  $\ell_{ii}$ , а если отрицательно, то обведём  $\ell_{ij}$ . В одном столбце не может быть двух обведённых элементов, поскольку они

отвечаали бы ситуациям, исключённым в силу условий (iv) и (v). (Если обведены два недиагональных элемента, то нарушается условие (iv), а если обведена единица, отвечающая элементу  $\ell_{ii}$ , и недиагональный элемент  $\ell_{ij}$ , то в вершину  $i$  входит отрицательное ребро, а исходит из неё положительное, что противоречит условию (v).)

Теперь применим (i)–(v), чтобы описать структуру графа  $D$ .

Утверждение В. Каждый орграф  $D \in \mathcal{D}$  имеет следующую структуру (рис. 16).

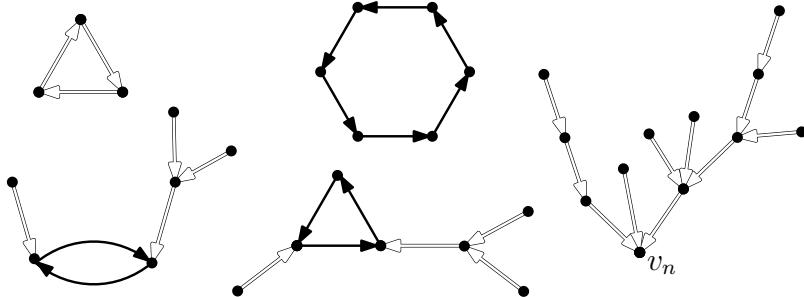


Рис. 16.

- (a) Множество вершин состоит из одного или более непересекающихся подмножеств  $V_1, V_2, \dots, V_k$ , отвечающих компонентам графа  $D$ , причём различные  $V_i$  не соединены рёбрами. Если подмножество  $V_1$  содержит вершину  $v_n$ , то подграф с множеством вершин  $V_1$  является деревом, все рёбра которого направлены в сторону  $v_n$ . Подграф с любым другим  $V_i$  в качестве множества вершин содержит ровно один направленный цикл длины не меньше 2 и для каждой его вершины — содержащее её дерево (возможно, пустое), рёбра которого направлены в сторону цикла.
- (b) Все рёбра, не принадлежащие направленным циклам, положительны, а в каждом направленном цикле либо все рёбра положительны, либо все рёбра отрицательны.
- (c) Обратно, любой орграф  $D$  с такой структурой, удовлетворяющий условию (i), принадлежит  $\mathcal{D}$ .

Действительно, пункт (a) непосредственно вытекает из условия (ii) (единственность исходящего ребра для каждой вершины, кроме  $v_n$ ): если добавить направленную петлю при вершине  $v_n$ , то у каждой вершины будет ровно одно исходящее ребро и мы получим так называемый *функциональный орграф*, для которого структура, описанная в п. (a), хорошо известна.

Перейдём к п. (b). Если начать путь по графу с отрицательного ребра, то в силу условия (v) нам встретятся только отрицательные рёбра. Значит, мы не сможем достичь вершины  $n$ , поскольку входящие в неё рёбра положительны, и с какого-то момента начнём двигаться по отрицательному циклу. При этом отрицательное ребро не может войти извне в такой цикл в силу (iv).

Что касается п. (c), то для графа  $D$  со структурой, описанной в пп. (a) и (b), условия (ii)–(v) очевидно выполнены и можно применить утверждение А. Тем самым утверждение В доказано.

Теперь совсем легко завершить первую часть нашего плана.

Все  $D \in \mathcal{T}$  имеют положительный знак. Они взаимно однозначно соответствуют остовным деревьям графа  $G$ .

Действительно, если  $D \in \mathcal{D}$  не содержит направленных циклов, то  $D$  является деревом с положительными рёбрами, направленными в сторону вершины  $v_n$ . При этом перестановка  $\pi_D$  тождественная, поскольку все обведённые элементы в слагаемом, отвечающем графу  $D$ , лежат на диагонали матрицы  $L^-$ . Значит,  $\text{sgn}(D) = +1$ , и если забыть об ориентациях рёбер, то получится остовное дерево графа  $G$ . Обратно, если дано остовное дерево графа  $G$ , то можно ориентировать его рёбра в сторону  $v_n$  и получить орграф  $D \in \mathcal{T}$ .

Осталось разобраться с “циклическими объектами”. Пусть  $D \in \mathcal{D}^+ \cup \mathcal{D}^-$ . Назовём *наименьшим циклом* направленный цикл, содержащий вершину с наименьшим номером (среди всех вершин в циклах). Пусть  $\bar{D}$  получается из  $D$  переменой знака всех рёбер в наименьшем цикле.

Очевидно,  $\bar{\bar{D}} = D$ , и при  $D \in \mathcal{D}$  будет и  $\bar{D} \in \mathcal{D}$ , как можно видеть из утверждения В. Осталось показать, что отображение, переводящее  $D$  в  $\bar{D}$ , является биекцией между  $\mathcal{D}^+$  и  $\mathcal{D}^-$ . Для этого докажем, что  $\text{sgn}(\bar{D}) = -\text{sgn}(D)$ .

Выполнено равенство  $\text{sgn}(D) = \text{sgn}(\pi_D)(-1)^m$ , где  $m$  — количество отрицательных рёбер в графе  $D$ , а  $\pi_D$  — ассоциированная перестановка.

Пусть  $i_1, i_2, \dots, i_s$  — вершины наименьшего цикла в  $D$ , занумерованные так, что направленные рёбра цикла имеют вид  $v_{i_1}v_{i_2}, v_{i_2}v_{i_3}, \dots, v_{i_{s-1}}v_{i_s}, v_{i_s}v_{i_1}$ .

В одном из графов  $D$  и  $\bar{D}$  наименьший цикл положителен, например в  $D$  (если он положителен в  $\bar{D}$ , рассуждение аналогично). Положительные рёбра отвечают диагональным элементам в  $L^-$ , поэтому  $i_j$  являются неподвижными точками перестановки  $\pi_D$ , т.е.  $\pi_D(i_j) = i_j$ ,  $j = 1, 2, \dots, s$ . В графе  $\bar{D}$  наименьший цикл отрицателен, так что

$$\pi_{\bar{D}}(i_1) = i_2, \dots, \pi_{\bar{D}}(i_{s-1}) = i_s, \pi_{\bar{D}}(i_s) = i_1,$$

т.е. вершины  $v_{i_1}, v_{i_2}, \dots, v_{i_s}$  образуют цикл перестановки  $\pi_{\bar{D}}$ .

Теперь легко проверить, что  $\pi_{\bar{D}}$  можно преобразовать в  $\pi_D$  посредством  $s - 1$  транспозиций, “уничтожающих” цикл  $(i_1, i_2, \dots, i_s)$ . Поскольку каждая транспозиция меняет знак перестановки, получаем  $\text{sgn}(\pi_{\bar{D}}) = (-1)^{s-1}\text{sgn}(\pi_D)$ , откуда

$$\text{sgn}(\bar{D}) = \text{sgn}(\pi_{\bar{D}})(-1)^{m+s} = (-1)^{s-1}\text{sgn}(\pi_D)(-1)^{m+s} = -\text{sgn}(D).$$

Этим завершается доказательство теоремы.

**4.2. а)** Рассмотрим граф  $\bar{G}$ , в котором  $V(\bar{G}) = V(G) \cup \{w\}$ ,  $E(\bar{G}) = E(G) \cup \{v_iw\}$ . Обозначим матрицу Лапласа графа  $\bar{G}$  через  $\bar{L}$ . Нетрудно понять, что  $\bar{L}^- = L + E_{i,i}$  (поэлементно). При этом количества оставных деревьев графов  $G$  и  $\bar{G}$  совпадают. Следовательно, по матричной теореме о деревьях, количество оставных деревьев графов  $G$  и  $\bar{G}$  равняется  $\det \bar{L}^- = \det(L + E_{i,i})$ , что и требовалось доказать.

**б)**  $\det(L + E_{i,j}) - \det(L + E_{i,i}) = \det M$ ;  $M = (m_{kn})$ , где

$$m_{kn} = \begin{cases} \ell_{kn} & \text{при } k \neq i; \\ -1, & \text{если } k = i \text{ и } n = j; \\ 1, & \text{если } k = i \text{ и } n = i; \\ 0 & \text{в остальных случаях.} \end{cases} \quad (11)$$

Заметим, что сумма элементов каждой строки матрицы  $M$  равна 0, и по задаче 2.3  $\det M = 0$ . Следовательно,  $\det(L + E_{i,j}) = \det(L + E_{i,i})$ , и из предыдущего пункта следует требуемое.

**4.3.** С легким переприподыvertом это утверждение сразу получается, если действовать аналогично решению задачи 2.3.а).

**4.4.** Это утверждение, к тому же в версии с весами, доказано в решении задачи 2.3.b).

**4.5.** Это задача по линейной алгебре. Изящное решение можно прочесть, например, в книжке Д. Карпова “Теория графов” (лежит в сети).

**4.6.** Для полного графа матрица  $L^-$  — это матрица  $(n-1) \times (n-1)$ , имеющая вид

$$L^- = \begin{pmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & n-1 \end{pmatrix}$$

Воспользуемся матричной теоремой о деревьях и подсчитаем её определитель.

$$\det \begin{pmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & n-1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & n-1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & n & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & n \end{pmatrix} = n^{n-2}.$$

Здесь в первом равенстве мы прибавили строчки с номерами от 2 до  $n-1$  к первой, от чего определитель не изменится. Во втором равенстве мы, наоборот, прибавили первую строчку ко всем остальным. Наконец, третье равенство следует из того, что среди одновалентных графов ненулевой вес имеет только граф, состоящий из  $n-1$  петли.

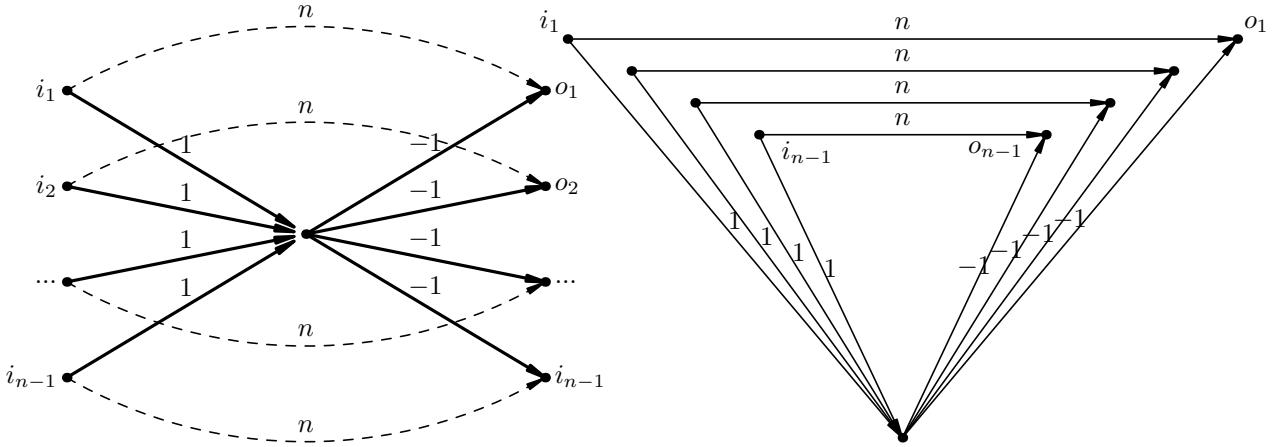


Рис. 17.

Дадим, однако, более комбинаторное рассуждение, воспользовавшись обобщением утверждения задачи 6.6 b).

*Весовая версия задачи 6.6 b).* Пусть дан граф, удовлетворяющий условию задачи 6.6 а). Пусть на каждом ребре графа написано действительное число, которое называется весом ребра. Весом пути называется произведение весов рёбер, входящих в этот путь, а весом набора из  $n$  путей называется произведение весов всех путей из набора, умноженное на  $(-1)^{|\pi|}$ , где  $\pi$  — перестановка, которую задает этот набор путей. Обозначим через  $a_{ij}$  сумму весов всех путей из  $i$ -го входа в  $j$ -й выход. Тогда определитель матрицы  $(a_{i,j})$  равняется сумме весов всех наборов из  $n$  непересекающихся путей.

Доказательство аналогично доказательству 6.6 b).

Итак, мы хотим найти определитель матрицы  $L^-$ . Посмотрим на граф на рис. 17, он имеет по  $n-1$  входов и выходов, а также одну промежуточную вершину. Заметим, что количество путей из  $i$ -го входа в  $j$ -й выход как раз равняется  $\ell_{ij}$ . Следовательно, по весовой версии задачи 6.6 b),  $\det L^-$  равен сумме весов наборов из  $n$  непересекающихся путей. При этом имеется один набор из  $n$  путей веса  $n^{n-1}$ , где  $i$ -й вход непосредственно соединен с  $i$ -м выходом, и  $n-1$  наборов веса  $-n^{n-2}$ . Таким образом, суммарный вес наборов из  $n$  непересекающихся путей равен

$$n^{n-1} - (n-1) \cdot n^{n-2} = n^{n-2}.$$

**4.7.** Воспользуемся матричной теоремой о деревьях. Здесь матрица Лапласа выглядит как

$$L = \left( \begin{array}{cccccc} k & \dots & 0 & -1 & \dots & -1 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & k & -1 & \dots & -1 \\ -1 & \dots & -1 & \ell & \dots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ -1 & \dots & -1 & 0 & \dots & \ell \end{array} \right) \left\{ \begin{array}{l} \ell \text{ строк} \\ k \text{ строк} \end{array} \right.$$

Мы найдем определитель матрицы  $M = L_{\ell,\ell+1}$  (обозначение из задачи 2.1 e). По задаче 2.3.b)  $\det L^- = -\det M$ .

$$M = \left( \begin{array}{ccccccc} k & \dots & 0 & 0 & -1 & \dots & -1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & k & 0 & -1 & \dots & -1 \\ -1 & \dots & -1 & -1 & 0 & \dots & 0 \\ -1 & \dots & -1 & -1 & \ell & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & \dots & -1 & -1 & 0 & \dots & \ell \end{array} \right) \quad \left. \begin{array}{l} \{\ell - 1 \text{ строк} \\ \} \\ \{\kappa - 1 \text{ строк} \end{array} \right.$$

Приведем два комбинаторных подсчёта определителя матрицы  $M$ .

Первый способ подсчёта определителя аналогичен подсчёту определителя в задаче 4.6. А именно, посмотрим на картинку рис. 18 слева. Нетрудно проверить, что сумма весов путей из  $i$ -го входа в  $j$ -й выход равна  $m_{ij}$ . Таким образом, по весовой версии задачи 6.6 b),  $\det M$  равен сумме весов наборов  $n$  непересекающихся путей. Нетрудно понять, что такой набор ровно один, и его вес равен  $-k^{\ell-1}\ell^{k-1}$ , что завершает подсчёт.

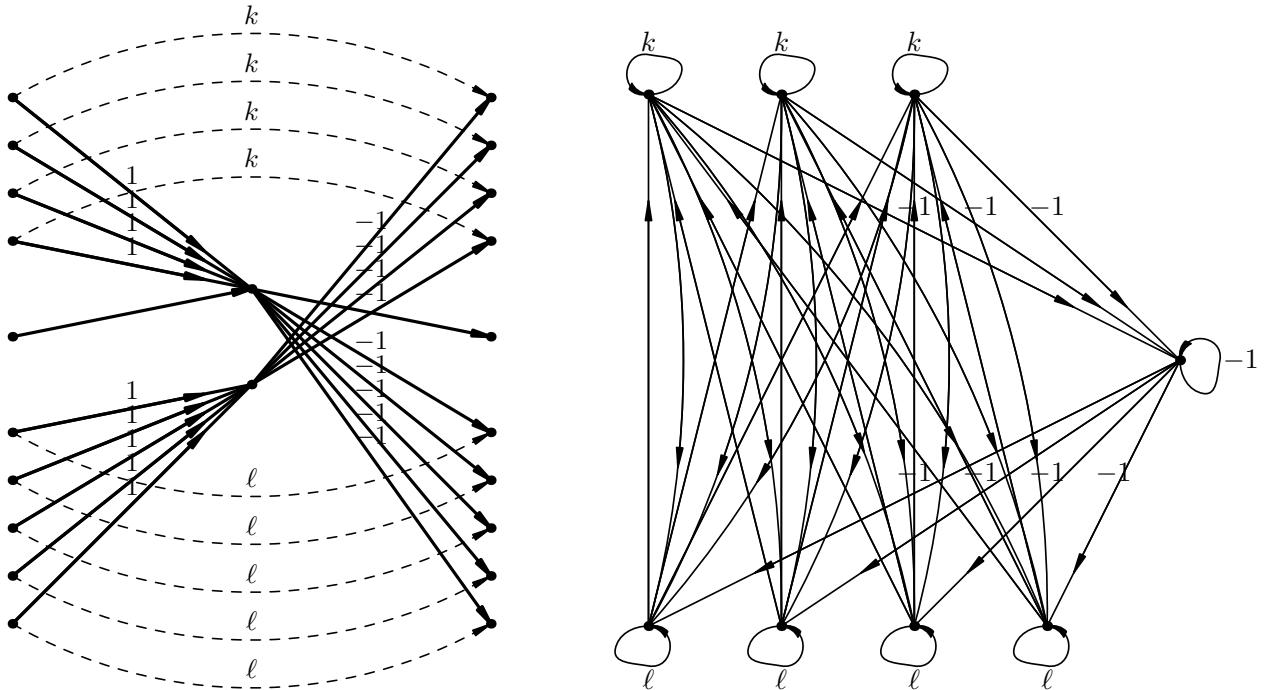
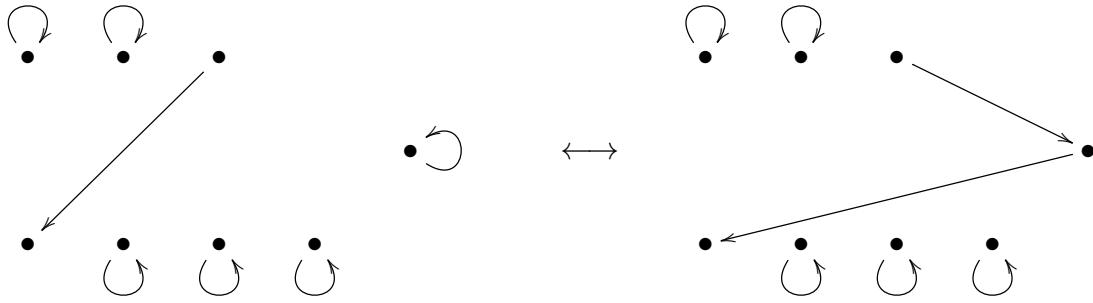


Рис. 18.

Второй способ подсчёта использует определение определителя через одновалентные графы. На рис. 18 справа изображен граф, одновалентные подграфы которого и пересчитывает  $\det M$ . В этом графе сверху изображены  $\ell - 1$  вершина первой доли, снизу  $k - 1$  вершина второй доли, а также одна особая вершина справа.

Во-первых, разобьем на пары одновалентные графы, которые содержат хотя бы 2 ребра, идущих из второй доли в первую. А именно, среди всех рёбер, идущих из второй доли в первую, выберем два, концы которых имеют наименьшие номера, и поменяем местами концы этих рёбер. Тогда перестановка сменит чётность. Нетрудно понять, что это соответствие биективно на заданном множестве, следовательно, все соответствующие графы сократятся.

Во-вторых, разобьем на пары одновалентные графы, содержащие ровно одно ребро, идущее из второй доли в первую. Раз имеется ровно одно ребро, выходящее из второй доли, то имеется и ровно одно ребро, входящее во вторую долю, либо двузвенный путь через особую вершину. Тогда в зависимости от того, откуда ведет это ребро, и выполним перестройку:



Итак, остались одновалентные графы, в которых во вторую долю не ведёт ни одного ребра. Нетрудно понять, что единственный граф, обладающий этим свойством, — граф, состоящий из всех петель. Вес этого графа, а следовательно и  $\det M$ , равен  $-k^{l-1}l^{k-1}$ .

**4.8.** Воспользуемся матричной теоремой о деревьях. Распишем  $\det L^-$  по комбинаторному определению через одновалентные графы. Если в одновалентном графе есть хотя бы одна петля, то соответствующий одновалентный граф имеет чётный вес. Иначе, так как число вершин в одновалентном графе нечётно, найдётся цикл длины хотя бы 3. Следовательно, если изменить направление всех стрелок, то получится другой одновалентный граф такого же веса. Итак, мы разбили некоторые одновалентные графы на пары равного веса, про остальные поняли, что они дают чётный вклад. Из этого мгновенно следует, что соответствующий определитель чётен.

**5.1.** Из формулы определителя следует, что если  $G$  не имеет совершенного паросочетания, то  $\det \tilde{B}$  — тождественный нуль.

Чтобы показать обратное, зафиксируем перестановку  $\pi$ , которая задаёт совершенное паросочетание, и дадим переменным в  $\det \tilde{B}$  следующие значения:  $x_{i,\pi(i)} := 1$  при  $i = 1, 2, \dots, n$ , а все остальные  $x_{ij}$  равны 0. Тогда  $\text{sgn}(\pi) \cdot x_{1,\pi(1)}x_{2,\pi(2)} \cdots x_{n,\pi(n)} = \pm 1$ .

Для каждой другой перестановки  $\sigma \neq \pi$  найдётся  $i$ , для которого  $\sigma(i) \neq \pi(i)$ , поэтому  $x_{i,\sigma(i)} = 0$ , так что все остальные слагаемые в разложении  $\det \tilde{B}$  равны 0. Таким образом, для данного выбора  $x_{ij}$  мы получаем  $\det \tilde{B} = \pm 1$ . Утверждение доказано.

**5.2.** Проведём индукцию по  $m$ . Случай одной переменной очевиден, так как по общеизвестной алгебраической теореме  $p(x_1)$  имеет не более  $d$  корней. (Это доказывается индукцией по  $d$ : если  $p(\alpha) = 0$ , то можно разделить  $p(x)$  на  $x - \alpha$ , понизив степень.)

Пусть  $m > 1$ . Предположим, что  $x_1$  появляется с ненулевым коэффициентом хотя бы в одном слагаемом из  $p(x_1, \dots, x_m)$  (в противном случае перенумеруем переменные). Запишем  $p(x_1, \dots, x_m)$  как многочлен от  $x_1$ , коэффициенты которого — многочлены от  $x_2, \dots, x_m$ :

$$p(x_1, x_2, \dots, x_m) = \sum_{i=0}^k x_1^i p_i(x_2, \dots, x_m),$$

где  $k$  — наибольший показатель при  $x_1$  в  $p(x_1, \dots, x_m)$ .

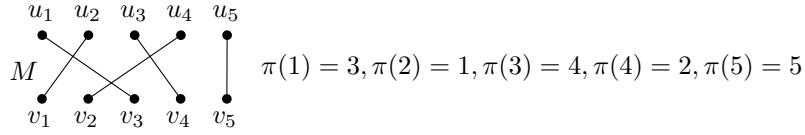
Наборы вида  $(r_1, \dots, r_m)$ , где  $p(r_1, \dots, r_m) = 0$ , мы разделим на два класса. Обозначим первый класс  $R_1$  и включим в него наборы, для которых  $p_k(r_2, \dots, r_m) = 0$ . Поскольку многочлен  $p_k(x_2, \dots, x_m)$  не равен тождественно нулю и имеет степень не выше  $d - k$ , количество вариантов для  $(r_2, \dots, r_m)$  по предположению индукции не превосходит  $(d - k)|S|^{m-2}$ , и потому  $|R_1| \leq (d - k)|S|^{m-1}$ .

Другой класс  $R_2$  состоит из остальных наборов, т. е. тех, для которых  $p(r_1, r_2, \dots, r_m) = 0$ , но  $p_k(r_2, \dots, r_m) \neq 0$ . Их мы подсчитаем так: значения переменных от  $r_2$  до  $r_m$  можно выбрать не более чем  $|S|^{m-1}$  способами, и если зафиксированы  $r_2, \dots, r_m$ , для которых  $p_k(r_2, \dots, r_m) \neq 0$ , то  $r_1$  должно быть корнем многочлена от одной переменной  $q(x_1) = p(x_1, r_2, \dots, r_m)$ . Этот многочлен имеет степень (ровно)  $k$ , поэтому у него не больше  $k$  корней. Значит, второй класс содержит не более  $k|S|^{m-1}$  наборов, и потому общее количество наборов не превосходит  $d|S|^{m-1}$ . На этом шаг индукции закончен, а с ним и доказательство теоремы Шварца — Зиппеля.

**5.3.** Предположим, что  $G$  имеет совершенное паросочетание и, значит,  $\det \tilde{B}$  — ненулевой многочлен степени  $n$ . Согласно теореме Шварца — Зиппеля, если вычислить  $\det \tilde{B}$  для значений переменных  $x_{ij}$ , независимо выбранных случайным образом из множества  $S := \{1, 2, \dots, 2n\}$ , то вероятность получить 0 не превосходит  $\frac{1}{2}$ .

Как обычно, вероятность неудачи можно понизить до  $2^{-k}$ , повторяя алгоритм  $k$  раз.

**6.1.** Пусть  $S_n$  обозначает множество всех перестановок множества  $\{1, 2, \dots, n\}$ . Каждое совершенное паросочетание  $M$  в графе  $G$  соответствует однозначно определённой перестановке  $\pi \in S_n$ , где  $\pi(i)$  — тот индекс  $j$ , для которого ребро  $u_i v_j$  лежит в  $M$ . Пример показан на рисунке.

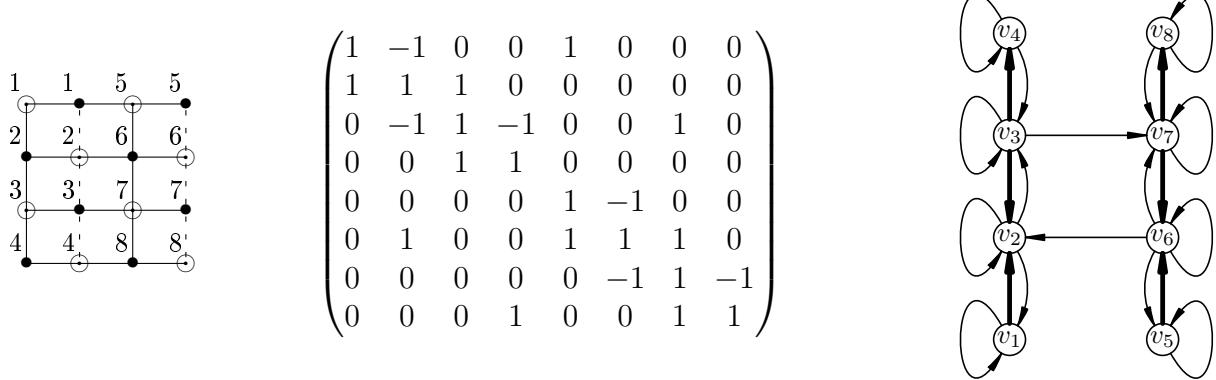


Обратно: когда в  $G$  существует совершенное паросочетание, соответствующее данной перестановке  $\pi \in S_n$ ? В точности тогда, когда  $b_{1,\pi(1)} = b_{2,\pi(2)} = \dots = b_{n,\pi(n)} = 1$ . Следовательно, количество совершенных паросочетаний в  $G$  равно

$$\sum_{\pi \in S_n} b_{1,\pi(1)} b_{2,\pi(2)} \dots b_{n,\pi(n)},$$

а это и есть перманент матрицы  $B$ .

**6.2.** Конечно, задача решается подсчётом определителя, но только не в нашем проекте! Пронумеруем вершины долей, выпишем двудольную матрицу смежности (чёрные вершины соответствуют столбцам, белые — строкам) и нарисуем граф, для которого эта матрица является обычной матрицей смежности:



Ребра, имеющие вес  $-1$ , нарисованы жирными стрелками. Осталось проверить, что любой чётный цикл любого одновалентного подграфа этого графа содержит нечётное число отрицательных рёбер (а нечётных циклов, кроме петель, здесь нет). Для этого графа это очевидно.

**6.3.** Пусть зафиксирована расстановка знаков  $\sigma$  из условия леммы, и пусть  $M$  — совершенное паросочетание в графе  $G$ , отвечающее перестановке  $\pi$ . В качестве его знака возьмём знак соответствующего слагаемого в  $\det(B^\sigma)$ ; в явном виде:

$$\operatorname{sgn}(M) := \operatorname{sgn}(\pi) b_{1,\pi(1)}^\sigma b_{2,\pi(2)}^\sigma \dots b_{n,\pi(n)}^\sigma = \operatorname{sgn}(\pi) \prod_{e \in M} \sigma(e).$$

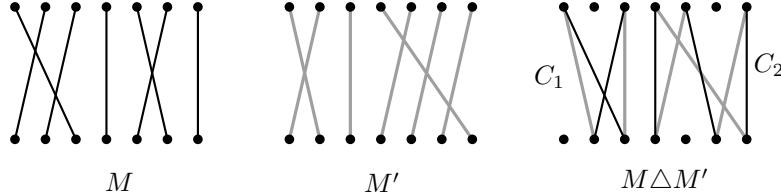
Легко видеть, что расстановка знаков  $\sigma$  будет кастелейновой тогда (и только тогда), когда все совершенные паросочетания в графе  $G$  имеют одинаковый знак.

Пусть  $M$  и  $M'$  — два совершенных паросочетания в графе  $G$ , а  $\pi$  и  $\pi'$  — соответствующие перестановки. Тогда

$$\begin{aligned}\operatorname{sgn}(M)\operatorname{sgn}(M') &= \operatorname{sgn}(\pi)\operatorname{sgn}(\pi')\left(\prod_{e \in M} \sigma(e)\right)\left(\prod_{e \in M'} \sigma(e)\right) \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\pi') \prod_{e \in M \Delta M'} \sigma(e),\end{aligned}$$

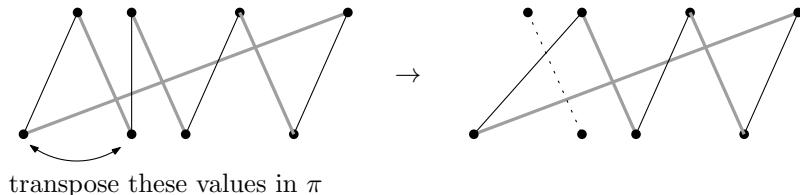
где  $\Delta$  обозначает симметрическую разность.

Симметрическая разность  $M \Delta M'$  является дизъюнктным объединением удачно размешённых циклов, как видно из рисунка.



Пусть  $C_1, C_2, \dots, C_k$  — эти циклы, причём длина  $C_i$  равна  $2\ell_i$ . Поскольку  $C_i$  удачно размешён, он согласно условию леммы правильно помечен, откуда  $\prod_{e \in C_i} \sigma(e) = (-1)^{\ell_i-1}$ . Таким образом,  $\prod_{e \in M \Delta M'} \sigma(e) = (-1)^t$ , где  $t = \ell_1 - 1 + \ell_2 - 1 + \dots + \ell_k - 1$ .

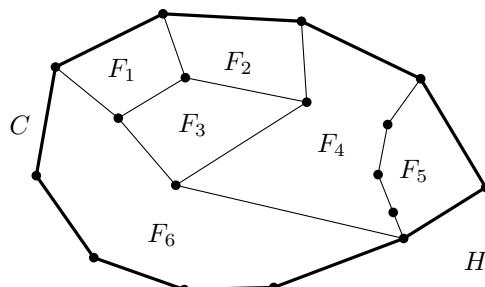
Осталось проверить, что  $\pi$  можно преобразовать в  $\pi'$  за  $t$  транспозиций (тогда в силу свойств знака перестановки  $\operatorname{sgn}(\pi) = (-1)^t \operatorname{sgn}(\pi')$ , откуда  $\operatorname{sgn}(M) = \operatorname{sgn}(M')$ , что и требуется). Это можно проделать по очереди для каждого цикла  $C_i$ . Как показано на рисунке для цикла длины  $2\ell_i = 8$ , применив к  $\pi$  подходящую транспозицию, можно “вычеркнуть” из цикла два ребра и перейти к циклу длины  $2\ell_i - 2$  (чёрные рёбра принадлежат множеству  $M$ , серые — множеству  $M'$ , а пунктирное ребро на правом рисунке принадлежит теперь обоим множествам).



Выполнив  $\ell_i - 1$  таких шагов, мы вычертим  $C_i$  и можем перейти к следующему циклу. В итоге хватит  $t$  шагов.

**6.4.** Пусть  $C$  — удачно размешённый цикл в графе  $G$ ; согласно задаче 6.3 нужно доказать, что он правильно помечен.

Пусть длина цикла  $C$  равна  $2\ell$ ;  $F_1, \dots, F_k$  — внутренние области, расположенные внутри  $C$ ;  $C_i$  ( $i = 1, \dots, k$ ) — граничный цикл области  $F_i$ , имеющий длину  $2\ell_i$ ;  $H$  — подграф в  $G$ , полученный удалением всех вершин и рёбер, начерченных вне  $C$ ; иначе говоря,  $H$  — объединение всех  $C_i$ .



Нужно понять, как чётность числа  $\ell$  связана с чётностями  $\ell_i$ . Количество вершин в  $H$  равно  $r + 2\ell$ , где  $r$  — количество вершин, лежащих внутри  $C$ . Каждое ребро в  $H$  принадлежит ровно двум циклам из  $C, C_1, \dots, C_k$ , так что количество рёбер в  $H$  равно  $\ell + \ell_1 + \dots + \ell_k$ . Наконец, изображение графа  $H$  содержит  $k + 1$  областей:  $F_1, \dots, F_k$  и одну внешнюю.

Применим теперь формулу Эйлера, согласно которой на любом изображении связного планарного графа количество вершин плюс количество областей равно количеству рёбер плюс 2. Значит,

$$r + 2\ell + k + 1 = \ell + \ell_1 + \dots + \ell_k + 2. \quad (12)$$

Теперь используем условие, что  $C$  удачно размещён. Поскольку граф, полученный удалением из  $G$  этого цикла и всех смежных с  $C$  рёбер, обладает совершенным паросочетанием, количество  $r$  вершин внутри  $C$  должно быть чётным. Поэтому из (12) вытекает

$$\ell - 1 \equiv \ell_1 + \dots + \ell_k - k \pmod{2}. \quad (13)$$

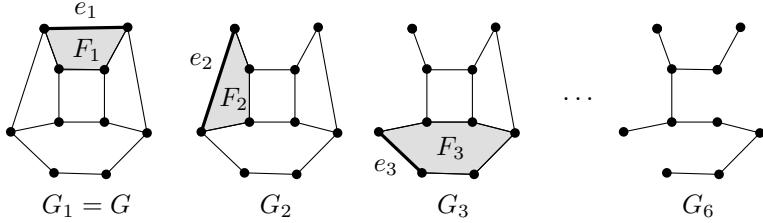
Пусть  $n_C$  — количество отрицательных рёбер в  $C$ , и аналогично определим  $n_{C_i}$ . Сумма  $n_C + n_{C_1} + \dots + n_{C_k}$  чётна, поскольку в ней включены по два раза все отрицательные рёбра, т.е.

$$n_C \equiv n_{C_1} + \dots + n_{C_k} \pmod{2}. \quad (14)$$

Наконец,  $n_{C_i} \equiv \ell_i - 1 \pmod{2}$ , поскольку циклы  $C_i$  правильно помечены. Соединив это с (13) и (14), получаем  $n_C \equiv \ell - 1 \pmod{2}$ . Значит,  $C$  правильно помечен, что и требовалось.

**6.5.** Пусть дан связный двусвязный планарный двудольный граф  $G$ . Зафиксируем некоторое его изображение на плоскости. Мы хотим построить расстановку знаков как в задаче 6.4, т.е. чтобы граница каждой внутренней области была правильно помечена.

Сначала займёмся удалением рёбер из  $G$ , как показано на рисунке.



Положим  $G_1 := G$ , и пусть  $G_{i+1}$  получается из  $G_i$  удалением ребра  $e_i$ , отделяющего внутреннюю область  $F_i$  от внешней (неограниченной) области (в данном изображении). Процесс останавливается на некотором  $G_k$ , не имеющем такого ребра. Изображение  $G_k$  тогда имеет лишь внешнюю область.

Теперь на рёбрах графа  $G_k$  произвольно расставим знаки. Продолжим эту расстановку на все рёбра графа  $G$  обратным ходом, расставляя знаки на рёбрах  $e_{k-1}, e_{k-2}, \dots, e_1$  в таком порядке. Каждое  $e_i$  содержится в границе ровно одной внутренней области  $F_i$  в изображении графа  $G_i$ , поэтому можно выбрать  $\sigma(e_i)$  так, чтобы граница области  $F_i$  была правильно помечена. Теорема доказана.

**6.6.** Мы взяли эту задачу в [7].

a) Утверждение очевидно. Выбрав перестановку  $\pi$ , мы для каждого входа  $i$  определяем, к какому выходу  $\pi(i)$  должен идти маршрут, при этом число способов выбрать маршрут равно  $a_{i\pi_i}$ . Тогда произведение  $a_{1\pi_1}a_{2\pi_2}\dots a_{n\pi_n}$  равно количеству способов выбрать набор. Суммируя по всем  $\pi$ , получаем общее число наборов.

b) Как и в рассуждении в п. а), произведение  $a_{1\pi_1}a_{2\pi_2}\dots a_{n\pi_n}$  равно количеству способов выбрать набор маршрутов. Наборы непересекающихся маршрутов учитываются лишь в произведении, заданном тождественной перестановкой, и в сумме, задающей определитель, это произведение засчитывается со знаком плюс. Остаётся проверить, что наборы пересекающихся маршрутов можно разбить на пары, засчитываемые с разными знаками, — тогда все они в этой сумме сократятся.

Припишем каждому пути номер, равный номеру входа, в котором он начинается. Для каждого набора из  $n$  пересекающихся путей, заданного перестановкой  $\pi$ , обозначим через  $i$  наименьший из номеров путей, которые пересекаются с другими путями. Обозначим через  $O$  первую точку пересечения  $i$ -го пути с каким-то другим путём, пусть это будет  $j$ -й путь.

Поменяем местами фрагменты  $i$ -го и  $j$ -го путей после точки  $O$ , полученный набор путей поставим в пару рассматриваемому набору. Перестановка, которая описывает полученный набор, отличается от исходной транспозицией  $(\pi_i, \pi_j)$  и поэтому имеет противоположный знак.

В приведенном рассуждении мы не использовали, что граф плоский, нам было существенно лишь, что он неперестаночны, т.е. в наборе из  $n$  непересекающихся путей у каждого пути номер выхода необходим равен номеру входа.

**6.7. а)** Мы взяли эту задачу в [3]. Пусть  $A_{mn}$  — количество путей хромого короля из угла прямоугольника  $m \times n$  в противоположный угол. Тогда

$$A_{n-1,n-1} = 2A_{n-2,n-1} + A_{n-2,n-2}$$

(чтобы убедиться в этом, рассмотрите три возможности первого хода короля). Аналогично,

$$B_n = A_{n-2,n-2} + A_{n-1,n-1} + 2A_{n-1,n-2}$$

(рассмотрим четыре варианта комбинации первого и последнего ходов). Подставляя первое равенство во второе, получаем требуемое.

Приведем рассуждение, дающее биективное доказательство требуемого равенства, родственное написанному выше формальному доказательству.

Величина  $B_n$  — это количество путей, ведущих из клетки  $a$  доски  $n \times n$  в клетку  $b$  и не заходящих в клетки, отмеченные крестиками, и в клетку  $c$ . Число  $2A_{n-1}$  — это количество путей, ведущих из клетки  $p$  в клетку  $e$ , плюс количество путей, ведущих из клетки  $q$  в клетку  $b$ . Взаимно однозначное соответствие между множествами таких путей устроено следующим образом. Рассмотрим произвольный путь хромого короля из  $p$  в  $e$ . Дополняя его шагами  $a-p$  и  $e-b$ , получаем путь из  $a$  в  $b$ , не заходящий в запрещенные клетки. При этом первый шаг в полученном пути — горизонтальный, а последний шаг — вертикальный. Теперь рассмотрим произвольный путь хромого короля из  $q$  в  $b$ . Если он не проходит через клетку  $c$ , дополним его шагом  $a-q$ . Получится путь из  $a$  в  $b$ , не заходящий в запрещённые клетки, в котором первый шаг — диагональный, а последний шаг — диагональный или вертикальный. Если же этот путь проходит через клетку  $c$ , удалим из него шаг  $c-b$ , опустим полученный в результате путь  $q-c$  на одну клетку вниз (получится путь из  $p$  в  $d$ ) и достроим этот путь шагами  $a-p$ ,  $d-b$  до пути из  $a$  в  $b$ . В полученном пути первый шаг — горизонтальный, а последний — диагональный. То, что построенное соответствие является взаимно однозначным, очевидно.

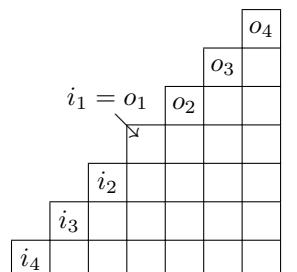
**б)** Мы взяли это утверждение в [5, лемма 5.1]. Рассмотрим матрицу  $B^{(n)} = (B_{i,j})_{1 \leq i,j \leq n}$ , где  $B_{i,j}$  — количество маршрутов хромого короля на доске  $i \times j$ , ведущих из левого нижнего угла в правый верхний, не заходящих в левую вертикаль и в верхнюю горизонталь (кроме начальной и конечной позиции). Аналогично утверждению предыдущего пункта доказывает-

ся, что  $B^{(n)} = 2A^{(n)}$ . По утверждению задачи 6.6, определители  $\det A^{(n)}$  и  $\det B^{(n)}$  подсчитывают одно и то же количество наборов маршрутов. Таким образом,  $\det A^{(n)} = 2^n \det A^{(n-1)}$ , откуда  $\det A^{(n)} = 2^{n(n+1)/2}$ .

**6.8.** Ответ: 1. Мы взяли эту задачу в [7]. Рассмотрим входы и выходы, указанные на рисунке. Количество путей от входов к выходам — это как раз числа Каталана. Тогда  $\det H$  вычисляет количество наборов непересекающихся маршрутов от входов к выходам. Очевидно, что такой набор маршрутов единственен.

**7.1.** Распишем  $\det A_G$  по комбинаторному определению через одновалентные графы. Так как в  $G$  нет циклов, то одновалентный граф входит с ненулевым весом только если в одновалентном графе все циклы длины 2, что соответствует совершенному паросочетанию  $G$ .

×	×	×	×	×	$c$	$b$
×					$d$	$e$
×						
×						
×						
×	$q$					
$a$	$p$					



Из того, что в дереве существует не более одного совершенного паросочетания, и следует требуемое утверждение.

**7.2.** Распишем  $\det \tilde{A}_G$  по комбинаторному определению через одновалентные графы. Так как в  $G$  нет циклов, то одновалентный граф входит с ненулевым весом только если в одновалентном графе нет циклов длины 3 и больше. Тогда одновалентные графы, состоящие из  $k$  кратных рёбер и  $n - 2k$  петель, войдут с весом  $(-1)^k x^{n-2k}$ . Теперь видно, что многочлены  $\chi G(x)$  и  $m_G(x)$  перечисляют одни и те же комбинаторные объекты с соответствующими весами, так что эти многочлены совпадают.

## Список литературы

- [1] Аксенов В. Е., Кохась К. П. Разбиения на домино и определители // Записки научн. семин. ПОМИ. 2013. Т 421. С. 5–18.
- [2] Аксенов В. Е., Кохась К. П. Удаление чипов. Urban Renewal revisited // Записки научн. семин. ПОМИ. 2015. Т 432. С. 5–29.
- [3] Иванов С. В., Кохась К. П., Храбров А. И. и др. Петербургские олимпиады школьников по математике. Задача 05.58. СПб: Невский диалект, 2007.
- [4] Кохась К. П. Разбиения на домино // Мат. просвещение. Третья серия. 2005. Вып. 9. С. 143–163.
- [5] Кохась К. П. Разбиения ацтекских диамантов и квадратов на домино // Записки научн. семин. ПОМИ. 2008. Т 360. С. 180–230.
- [6] Кохась К. П. Дележ денег в тайном обществе. В сб. Берлов С.Л., Петров Ф.В., Смирнов А.В. и др. Задачи Санкт-Петербургской олимпиады школьников по математике. СПб: Невский Диалект; БХВ-Петербург, 2011. С. 81–103.
- [7] Benjamin A. T., Cameron N. T. Counting on determinants // American Mathematical Monthly. 2005. Vol. 112. № 6. P. 481–492.
- [8] Brualdi R.A., Cvetković D. A combinatorial approach to matrix theory and its applications. Taylor & Francis Group. 2009. P. 63–96.
- [9] Matoušek J. Thirty-three Miniatures. Mathematical and Algorithmic Applications of Linear Algebra. Providence: AMS. 2010. P. 77–83, 107–111.

# Determinants in graph theory

Presented by O. Bursian, B. Frenkin, K. Kokhas, V. Retinsky

26.01.2021

## 1 Preliminaries

**Graphs.** Informally speaking, a *graph* is a set of points (vertices, or nodes) connected with linear segments (edges). The formal definition is as follows: a graph  $G$  is determined iff we have chosen the set of its *vertices*  $V(G)$  and the set of its *edges*  $E(G)$  which consists of some pairs  $(v_1v_2)$  of elements from  $V$ . A graph is called *undirected* if the order of elements in a pair is ignored, that is, pairs  $(v_1v_2)$  and  $(v_2v_1)$  are considered as the same pair. Otherwise the graph is called *directed* or briefly *a digraph*. In the sequel we assume that the set  $V(G) = \{v_1, v_2, \dots, v_n\}$  is *finite*, so that the set  $E(G)$  is finite as well.

For  $(v_1v_2) \in E(G)$  we say that *the edge*  $v_1v_2$  *connects the vertices*  $v_1$  and  $v_2$ . Also we say that this edge is *incident* to the vertices  $v_1$  and  $v_2$  and these vertices are *incident* to the edge  $v_1v_2$ . Then the vertices  $v_1$  and  $v_2$  are called *adjacent*, otherwise *non-adjacent*. If any two vertices are adjacent then the graph is called *complete*.

*The valency, or degree, of a vertex* of a graph is the number of edges incident to this vertex. The valency of a vertex  $v$  is denoted  $\deg v$ . *The exit valency* and *the entry valency*, respectively, is the number of edges which exit or enter the given vertex.

A *square matrix*  $A$  of *order*  $n$  is a table  $n \times n$  whose cells contain reals: the number at the intersection of  $i$ th row and  $j$ th column is denoted  $a_{ij}$ . *The adjacency matrix* of a non-directed graph  $G$  is the  $n \times n$  matrix  $A = (a_{ij})$  such that  $a_{ij} = 1$  if  $v_i$  and  $v_j$  are adjacent, and  $a_{ij} = 0$  otherwise. This matrix is necessarily symmetric (relative to the *main diagonal* that connects the upper left and lower right corners).

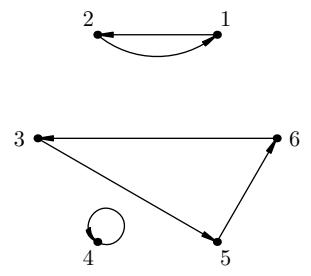
The adjacency matrix of a directed graph  $G$  is the  $n \times n$  matrix such that  $a_{ij} = 1$  if  $G$  contains an edge from  $v_i$  to  $v_j$ , and  $a_{ij} = 0$  otherwise. This matrix is not necessarily symmetric.

*A path* in a graph is a sequence  $v_{i_1}v_{i_2}, \dots, v_{i_{k-1}}v_{i_k}$  of its edges ( $k \geq 1$ ), where the first vertex of the next edge coincides with the second vertex of the preceding one. A set consisting of a single edge is also considered as a path. If  $v_{i_k} = v_{i_1}$ , so that the path is closed then it is called *a cycle*. A graph is called *connected* if there exists a path between any of its vertices or the graph has a single vertex. A graph is called *a tree* if it is connected and contains no cycles. It is easily seen that then and only then any two of its vertices are connected by a single path.

**Permutations and their parity.** A *permutation* of the set  $\{1, \dots, n\}$  is a mapping of this set into itself such that distinct elements map to distinct ones and each element is the image of some element (maybe the same one). If  $\pi$  is a permutation then  $\pi(i)$  denotes the element obtained from  $i$  under action of this permutation.

A directed graph such that the exit and the entry valency of each vertex equals 1 will be called *univalent*. It may contain *loops* (edges such that both their endpoints coincide). Each permutation  $\pi$  determines a univalent graph on the set of vertices  $\{1, 2, \dots, n\}$ : this graph contains some directed edge  $ij$  iff  $\pi(i) = j$ . The figure illustrates the case  $n = 6$ :  $\pi(1) = 2$ ,  $\pi(2) = 1$ ,  $\pi(3) = 5$ ,  $\pi(4) = 4$ ,  $\pi(5) = 6$ ,  $\pi(6) = 3$ .

*The product of permutations*  $\sigma$  and  $\tau$  is the permutation realized by consecutive execution of  $\sigma$  and  $\tau$ . *Transposition* is a permutation which interchanges two elements and fixes all the others.



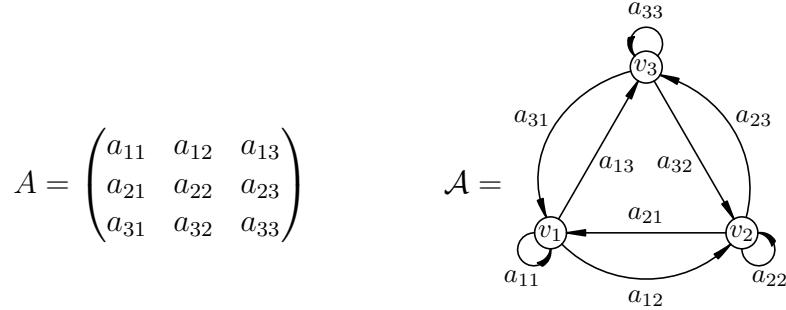
It is not difficult to see that any permutation is a product of transpositions. No permutation can be represented as a product of both even and odd number of transpositions. If a permutation is a product of even number of transpositions then it is called *even*, otherwise *odd* permutation. The sign of a transposition is  $+1$  for an even permutation and  $-1$  for an odd one. The sign of a permutation  $\pi$  is denoted  $\text{sgn}(\pi)$ . If a permutation corresponds to a univalent graph then its sign equals  $(-1)^m$ , where  $m$  is the number of even (including an even number of edges) cycles in the graph.

**The determinant of a matrix.** To each square matrix  $A = (a_{ij})$  there corresponds a real number which is called its *determinant* and is equal to the sum of products

$$\det A = \sum_{\pi} \text{sgn}(\pi) a_{1,\pi(1)} \cdot a_{2,\pi(2)} \cdot \dots \cdot a_{n,\pi(n)}, \quad (1)$$

where  $\pi$  runs over all permutations of  $\{1, \dots, n\}$ , so the sum contains  $n!$  summands. If  $\det A = 0$  then the matrix  $A$  is called *degenerate*, otherwise *non-degenerate*.

For every matrix  $A$  consider a complete digraph  $\mathcal{A}$  on  $n$  vertices (with loops), such that to each edge  $v_i v_j$  there corresponds real  $a_{ij}$  called *the weight* of this edge.



In the sequel, we consider only the univalent subgraphs of  $\mathcal{A}$  that contain all its vertices.

Each permutation  $\pi$  in the sum (1) determines a univalent subgraph in  $\mathcal{A}$  (and conversely, each univalent subgraph determines a permutation). For each univalent subgraph consider the product of weights of all its edges; if the subgraph contains an odd number of cycles with even number of vertices then multiply this product by  $-1$ . The result will be called *the weight* of the subgraph. Thus the weight of the univalent subgraph corresponding to a permutation  $\pi$  is equal to a summand of (1), and so we may accept the alternative definition.

The determinant of a matrix  $A$  is the sum of weights of all univalent subgraphs in  $\mathcal{A}$ .

For the graph  $\mathcal{A}$  from our example, all univalent subgraphs and their weights are shown at fig. 1. Thus

$$\det A = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31}.$$

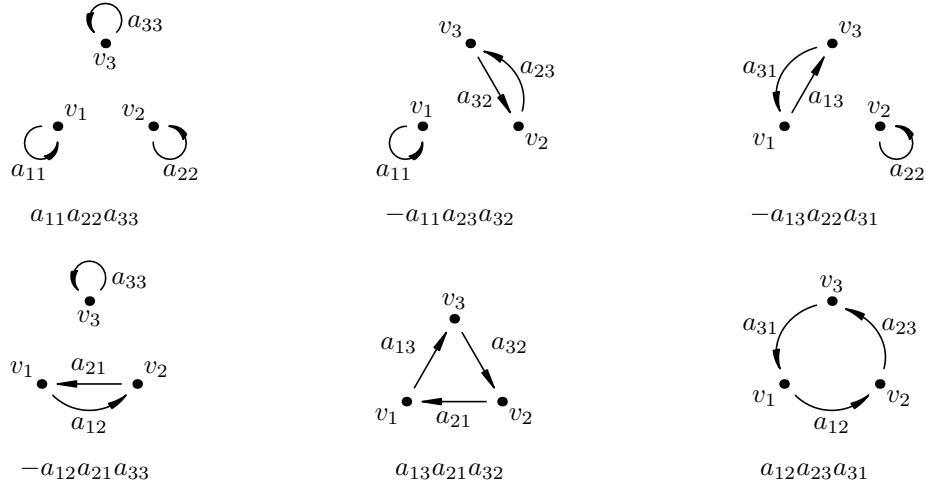


Рис. 1. Univalent subgraphs of the graph  $\mathcal{A}$  and their weights

## 2 Properties of determinants

**2.1.** Using the combinatorial definition of the determinant, prove its following properties.

a) If each element of some row of a matrix  $A$  is multiplied by a real  $c$  then the determinant is multiplied by  $c$  as well.

b) If two rows of a matrix are interchanged then the determinant changes its sign.

c) Suppose in the  $k$ th column of a matrix  $A$  the diagonal element is 1 and the other elements are 0. Let  $\tilde{A}$  be the matrix obtained from  $A$  by deletion of the  $k$ th row and the  $k$ th column. Then  $\det A = \det \tilde{A}$ .

d) Given a matrix  $A = (a_{ij})$  and matrices  $A^{(1)}$  and  $A^{(2)}$  identical to  $A$  except the  $j$ th row, and for the elements of the  $j$ th row we have

$$a_{ij} = a_{ij}^{(1)} + a_{ij}^{(2)}.$$

Then  $\det A = \det A^{(1)} + \det A^{(2)}$ .

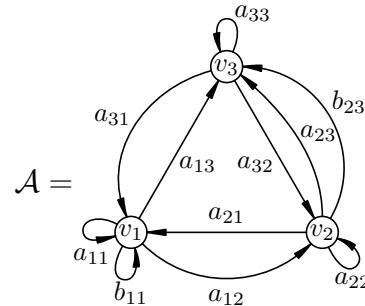
e) Let  $A_{ij}$  be the matrix obtained from the matrix  $A$  by deletion of the  $i$ th row and the  $j$ th column. Then we have the following formula for development along the  $i$ th row:

$$\det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det A_{ij}.$$

Regarding Problem 2.1 d), let us mention the following lifehack.

**2.2.** Given a matrix  $A = (a_{ij})$  such that some matrix elements are represented as sums, see the example below. Consider the digraph  $\mathcal{A}$  containing a single edge for each summand. Unlike the standard case, this graph may contain multiple edges and multiple loops (with different weights). Then the determinant of  $A$  is still equal to the sum of weights of all univalent subgraphs in the constructed graph  $\mathcal{A}$ .

$$A = \begin{pmatrix} a_{11} + b_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} + b_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$



**2.3.** Suppose that the sum of elements in each row of a matrix  $A$  equals 0: specifically, each diagonal cell of  $A$  contains the number equal to the minus sum of the remaining elements of the same row.

a) Prove that  $\det A = 0$ .

b) Prove that for each  $i$  and any  $j_1, j_2$  we have  $\det A_{ij_1} = (-1)^{j_2-j_1} \det A_{ij_2}$  (notation from 2.1 e).

**2.4.** Suppose that the graph  $G$  corresponding to the matrix  $A$  contains a subgraph  $H$  on 8 vertices, shown at fig. 2 at the left. Furthermore the graph may contain edges incident to white vertices and not shown at the figure, however the black vertices have valency 3, so all their edges are shown. Replace this subgraph with the subgraph  $H'$  shown at fig. 2 at the right, where the new weights are of the form

$$x' = \frac{y}{wz - xy}, \quad y' = \frac{x}{wz - xy}, \quad z' = \frac{w}{xy - wz}, \quad w' = \frac{z}{xy - wz}. \quad (2)$$

Let  $A'$  be the matrix corresponding to the new graph. Then

$$\det A = (xy - wz)^2 \det A'. \quad (3)$$

**2.5.** Suppose that  $G$  is the graph shown at fig. 3 (consisting of  $m - 1$  «concentric» squares),  $A$  is the adjacency matrix of this graph. Prove that

$$\det A = \begin{cases} m^2 & \text{for } m \text{ odd,} \\ 0 & \text{for } m \text{ even.} \end{cases}$$

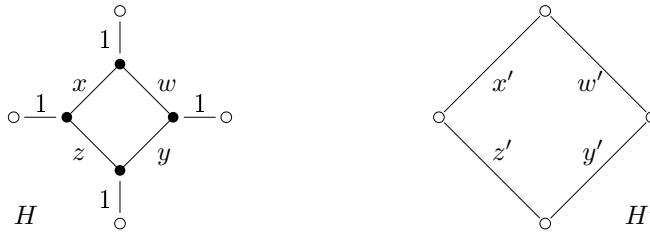


Рис. 2. Restructuring of a subgraph.

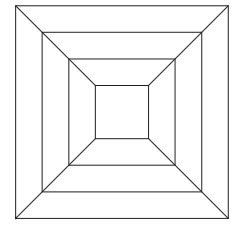


Рис. 3. Graph  $C_4 \times P_{m-1}$ .

### 3 Determinants of checkered figures

Suppose  $F$  is a bounded checkered figure on the checkered plane,  $G_F$  is the graph dual to  $F$ . This means that the vertices of  $G$  correspond to the cells of  $F$ , and the edges connect the cells adjacent by side. It is suitable to consider  $G_F$  and its subgraphs as directed, assuming that two adjacent cells are connected by two edges with opposite directions. Let  $A_F$  denote the adjacency matrix of  $G_F$ . *Tilings* mean dissections of  $F$  into dominoes. A vertical edge of a univalent subgraph in  $G_F$  will be called *ascending* if it is directed up, and *descending* if it is directed down. (Remind that we consider only univalent subgraphs that contain all vertices of the graph.) The figure  $F$  is called simple connected if it is «without holes», or more formally, if its dual graph is connected and the dual graph of its complement is connected too.

**3.1.** Prove that the number of univalent subgraphs of  $G_F$  equals the square of the number of tilings of  $F$ .

**3.2.** Let  $P$  be a simple connected checkered polygon such that its border contains  $a$  points with even  $y$ -coordinate and  $b$  points with odd  $y$ -coordinate, and there are  $d$  points with integer coordinates inside it. Then the sum of lengths of vertical sides of  $P$  is equivalent to  $a - b + 2d + 2$  modulo 4.

**3.3.** Let  $F$  be a simple connected checkered figure with even area. Then either for each univalent subgraph of  $G_F$  the number of ascending edges and the number of cycles have the same parity or for each univalent subgraph of  $G_F$  these parities are opposite.

The sign of a figure  $F$  will mean the number  $\text{sgn } F = (-1)^h$ , where  $h$  is the number of horizontal dominoes in some tiling of the figure. Let  $c_k$  denote the number of tilings of  $F$ , containing just  $k$  vertical dominoes. The polynomial  $f_F(x) = \sum_{k=0}^{+\infty} c_k \cdot x^k$  will be called the *vertical polynomial* of  $F$ . A pair of tilings will be called *good* if the numbers of vertical dominoes in these differ just by 2.

**3.4.** Prove that the definition of the sign of a figure is correct.

**3.5.** For each simple connected checkered figure  $F$

$$\det A_F = \text{sgn } F \cdot \sum_{\pi} (-1)^{\text{the number of ascending edges in } \pi}.$$

$$\det A_F = \text{sgn } F \cdot f_F^2(\mathbf{i}).$$

In the first formula summation is spread over all univalent subgraphs of  $G_F$ , in the second formula  $\mathbf{i} = \sqrt{-1}$ .

**3.6.** Let  $F$  be an arbitrary simple connected checkered figure with area  $2s(F)$ . If all tilings of  $F$  can be split into good pairs then  $\det A_F = 0$ . If all tilings except one can be dissected into good pairs then  $\det A_F = (-1)^{s(F)}$ .

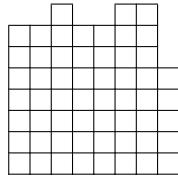


Рис. 4. A regular 8-stamp

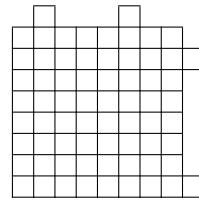


Рис. 5. An irregular 9-stamp

Let an *n-stamp* mean a square  $n \times n$  maybe with removal of some cells adjoining to the upper or right side. Enumerate the row of an *n-stamp* by numbers from 1 to  $n$  upwards, and the columns from left to right. A cell will be denoted by the pair consisting of the numbers of its row and column. Call an *n-stamp* *regular* (fig. 4) if in any pair of cells  $(n, i)$  and  $(i, n)$  with  $i < n$  just one was removed and the cell  $(n, n)$  was removed as well. The other stamps will be called *irregular* (fig. 5).

**3.7.** Let  $F$  be any regular  $n$ -stamp. Then  $\det A_F = (-1)^{n(n-1)/2}$ . And if  $F$  is an irregular  $n$ -stamp then  $\det A_F = 0$ .

**3.8.** For an arbitrary  $n \times m$  rectangle

$$\det A_{n \times m} = \begin{cases} 0, & \text{if } (n+1, m+1) \neq 1; \\ (-1)^{\frac{n \cdot m}{2}}, & \text{if } (n+1, m+1) = 1; \end{cases}$$

where  $(n, m)$  is the greatest common divisor of  $n$  and  $m$ .

## 4 Spanning trees

Let  $G$  be an arbitrary (non-directed) connected graph. A *spanning tree* of  $G$  is a tree whose set of vertices is the same as for  $G$ , and the set of edges is included in the set of edges of  $G$ .

Our goal is to determine the number of spanning trees of a given connected graph if we know its structure. For this, we require the *Laplacian matrix* of  $G$ : this is the  $n \times n$  matrix  $L = (\ell_{ij})$  such that

$$\ell_{ij} = \begin{cases} \deg v_i & \text{for } i = j; \\ -1 & \text{for } i \neq j \text{ and adjacent vertices } v_i \text{ and } v_j; \\ 0 & \text{otherwise.} \end{cases} \quad (4)$$

By assertion of Problem 2.3 a we have  $\det L = 0$ . Let  $L^-$  denote the matrix obtained from the Laplacian matrix by removing the last row and the last column.

We have the *Matrix-tree theorem*: *the number of spanning trees of a connected graph equals  $\det L^-$* .

A suitable starting point to prove this theorem is the lifehack from Problem 2.2 or the following construction.

Let us express the determinant of  $L^-$  as the sum of products of its elements, representing each diagonal element as a sum of units or minus units, and expanding brackets. The resulting expression will be called the *superexpansion* of the determinant. To each summand in the superexpansion we associate the following digraph having the vertices  $1, 2, \dots, n$  and signs «+», «-» at the edges (fig. 6). Circle the factors of this summand (these are units and minus units, one in each row and in each column). If a minus one is circled at the meet of row  $i$  and column  $j$  then we draw a *negative* edge (with the minus sign) from  $v_i$  to  $v_j$ . If in a diagonal element  $a_{ii}$  we circle the  $k$ th unit then we draw a *positive* edge (with the plus sign) from  $v_i$  to the  $k$ th smallest neighbor of  $V_i$  (it is the vertex  $v_j$  adjacent to  $v_i$  and such that there are just  $k-1$  vertices adjacent to  $v_i$  and having numbers smaller than  $j$ ). Clearly each of the resulting digraphs arises from a single summand of the superexpansion. Now we may define *the sign of the digraph* as a whole, meaning the sign of the corresponding summand in the superexpansion.

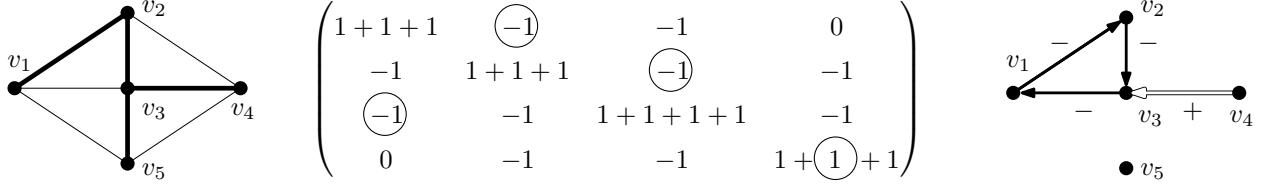


Рис. 6. Left part: the graph  $G$  and one of its spanning trees. Central part: the matrix  $L^-$  for  $G$ . The circled numbers form one of summands in the superexpansion. The sign of the summand is  $(-1)^m \text{sgn}(\pi)$ , where  $m$  is the number of chosen minus units,  $\text{sgn}(\pi)$  is the sign of the associated permutation, in our case  $\pi = (2314)$  and its sign is «+». Right part: the digraph associated with this summand.

#### 4.1. Prove the Matrix-tree theorem.

**4.2.** Let  $E_{i,j}$  denote the  $n \times n$  matrix such that the cell in the  $i$ th row and  $j$ th column contains 1 and the others contain zeroes (such matrices are called matrix units). Prove that the number of spanning trees of  $G$  equals

- a)  $\det(L + E_{i,i})$  for each  $i$ ,
- b)  $\det(L + E_{i,j})$  for each  $i, j$ .

**4.3.** Let  $L$  again denote the Laplacian matrix of a graph  $G$ . Fix a set of vertices  $v_1, v_2, \dots, v_k$  of  $G$  ( $k < n$ ) and remove the corresponding rows and columns from  $L$ . Denote the resulting  $(n-k) \times (n-k)$  matrix by  $L_k^-$ . The subgraph of  $G$  that contains all vertices of  $G$  and consists of  $k$  trees without common vertices or edges, containing, respectively, vertices  $v_1, v_2, \dots, v_k$  will be called the *spanning forest* based on  $v_1, v_2, \dots, v_k$ . Some trees of the spanning forest may consist of a single vertex.

Prove that the determinant of the matrix  $L_k^-$  is equal to the number of spanning forests based on  $v_1, v_2, \dots, v_k$ .

**4.4.** Let  $G$  be a digraph without loops. Its Laplacian matrix  $L^-$  is defined by the formula (4) with the only modification: for  $i = j$  take the exit valency of  $v_i$ , and for  $i \neq j$  put  $\ell_{ij} = -1$  only if there is an edge from  $v_i$  to  $v_j$ . A *rooted directed spanning tree* with the root  $v$  is the subgraph of a digraph  $G$ , such that it contains all vertices of  $G$  and for each vertex there is a unique path to  $v$ . Prove the following version of the Matrix-tree theorem for digraphs:  $\det L^-$  equals the number of rooted directed spanning trees with the root  $v_n$ .

**4.5.** In a digraph without loops, the entry valency of any vertex equals its exit valency. Prove that the number of rooted directed spanning trees with a given root does not depend on the root.

**4.6.** Using the Matrix-tree theorem, prove the *Cayley formula*: the number of trees on  $n$  enumerated vertices equals  $n^{n-2}$ .

A graph  $G$  is called *bipartite* if its set of vertices consists of two disjoint *color classes* such that no two vertices of the same class are adjacent.

**4.7.** Prove that the number of spanning trees of a complete bipartite graph  $K_{k,m}$  equals  $k^{\ell-1} \ell^{k-1}$ .

**4.8.** A graph  $G$  has an even number of vertices, and the valency of each vertex is even. Prove that the number of spanning trees of  $G$  is even.

## 5 Determinants and existence of perfect matchings

In this section we work with (non-directed) bipartite graphs. In this section we assume  $n = 2m$  and we consider only bipartite graphs such that both classes contain the same number  $m$  of vertices. The *bipartite adjacency matrix* of a bipartite graph  $G$  is the  $m \times m$  matrix  $B = (b_{ij})$  such that  $b_{ij} = 1$  if the  $i$ th vertex of the first class is adjacent to the  $j$ th vertex of the second class, and  $b_{ij} = 0$  otherwise. If in this matrix each element  $b_{ij}$  equal to 1 is replaced by a variable  $x_{ij}$  then the resulting matrix  $\tilde{B}$  is called the *variable bipartite adjacency matrix* of  $G$ . A *perfect matching* in a graph  $G$  is a subset  $M \subseteq E(G)$  of the set of its edges, such that each vertex of  $G$  is incident to a single edge from  $M$ .

**5.1.** Prove that if the color classes of a bipartite graph  $G$  contain equal number of vertices then the existence of a perfect matching in  $G$  is equivalent to the fact that  $\det \tilde{B}$  is not the zero constant (as a polynomial).

How can we check, in a sensible time, that the bipartite adjacency matrix  $A$  is non-degenerate? For this, the following theorem is useful.

**5.2. The Schwartz–Zippel theorem.** Suppose  $d$  is a positive integer,  $S$  is a set of  $s$  reals,  $p(x_1, \dots, x_m)$  is a polynomial of degree  $d$  in  $m$  variables with real coefficients. Then the number of tuples  $(r_1, \dots, r_m)$ , where  $r_1, \dots, r_m \in S$  and  $p(r_1, \dots, r_m) = 0$ , does not exceed  $ds^{m-1}$ .

**5.3.** Given a bipartite graph  $G$  whose color classes consist of  $m$  vertices each. Using the Schwartz–Zippel theorem, construct an algorithm which checks existence of a perfect matching and fails in at most half of cases.

Repeated application of this algorithm enables us to make the probability of an error arbitrarily small.

## 6 Counting perfect matchings in a planar bipartite graph

A graph is called *planar* if it can be drawn in the plane without self-intersections. This means that its vertices can be represented by points of the plane, and the edges incident to them by curves with ends in these points so that internal points of these curves don't belong to other such curves. We call a *domain* any part of the plane such that its border consists of images of edges, and the internal (remaining) points don't belong to images of edges. For any such picture of a connected planar graph we have *Euler formula*

$$v - e + f = 2,$$

where  $v$  is the number of vertices,  $e$  is the number of edges,  $f$  is the number of domains.

If in the expression (1) for the determinant of a matrix  $A$  all summands are taken with the plus sign then we obtain *the permanent* of  $A$ , denoted by  $\text{per}(A)$ .

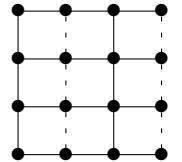
**6.1.** Prove that the number of perfect matchings in a bipartite graph equals the permanent of the bipartite adjacency matrix.

Calculation of the permanent requires much more work than that of the determinant. So the question arises whether it is possible to reduce the calculation of the permanent of a bipartite adjacency matrix to the calculation of its determinant changing signs of some elements of the matrix?

Let  $G$  be a planar bipartite graph. To its edges we attach signs «+» and «-». In the bipartite adjacency matrix  $B$  of this graph replace 1 by  $-1$  if the corresponding edge has minus sign. We denote this signing by  $\sigma$ , and the resulting matrix by  $B^\sigma$ . A *Kasteleyn signing* is a signing  $\sigma$  such that

$$|\det B^\sigma| = \text{per}(B).$$

**6.2.** The picture shows a graph on 16 vertices. The continuous lines represent edges with plus sign, and the dotted lines correspond to edges with minus sign. Prove that this signing is Kasteleyn one.



Suppose  $C$  is a cycle of length  $2\ell$  in a bipartite graph,  $\sigma$  is a signing of edges,  $n_C$  is the number of negative edges in  $C$ . The cycle  $C$  will be called *properly signed* with respect to  $\sigma$  if  $n_C$  and  $\ell$  are of opposite parity. The cycle  $C$  is *evenly placed* if the removal of all its vertices and adjacent to them edges from  $G$  results in a graph having a perfect matching. A graph is called *2-connected* if each its edge belongs to a cycle.

**6.3.** Suppose each evenly placed cycle is properly signed relative to a signing  $\sigma$ . Then  $\sigma$  is a Kasteleyn signing. (No planarity assumed.)

**6.4.** Let  $G$  be a planar bipartite 2-connected graph. Let us fix some planar drawing of  $G$ . Let  $\sigma$  be a signing of  $G$  such that the boundary cycle of every bounded domain in the drawing is properly signed. Then  $\sigma$  is a Kasteleyn signing.

**6.5.** Prove that any planar 2-connected bipartite graph has a Kasteleyn signing.

**6.6.** a) Suppose in a digraph  $G$  we have marked  $n$  vertices having only outgoing edges (these vertices are «inlets» from which we may start to move along edges of the graph) and  $n$  vertices having only incoming edges («outlets»). Let  $a_{i,j}$  be the number of ways to pass from the  $i$ th inlet to the  $j$ th outlet. Prove that the permanent of the matrix  $(a_{i,j})$  equals to the number of sets such that each set consists of  $n$  paths from an inlet to an outlet, and the beginning vertex and the ending vertex of any two paths do not coincide.

b) In addition suppose that the graph be planar, all inlets are located to the left from all outlets, and all edges in all paths are passed from the left to the right. Prove that the determinant of  $(a_{i,j})$  equals the number of sets such that each set consists of  $n$  non-intersecting paths where the  $i$ th path leads from the  $i$ th inlet to the  $i$ th outlet (with the same  $i$ ).



**6.7.** a) In the left lower corner of an  $n \times n$  board there is a lame king which may move only in three directions: to the right, up, and up to the right (along a diagonal). Denote by  $A_n$  the number of all its paths to the opposite corner of the board, and denote by  $B_n$  the number of these paths such that they are disjoint with the left column and the upper row (except the initial and final cells). Prove that  $B_n = 2A_{n-1}$ .

b) Consider the matrix  $A^{(n)} = (A_{i,j})_{1 \leq i,j \leq n}$ , where  $A_{i,j}$  is the number of paths of the lame king on the  $i \times j$  board, leading from the left lower to the right upper corner. Determine  $\det A^{(n)}$ .

**6.8.** Let  $H$  be the matrix  $(n+1) \times (n+1)$ , where  $h_{i,j} = C_{i+j} = \frac{1}{n+1} \binom{2n}{n}$  are Catalan numbers. Then  $\det H = 1$ .

## 7 Problems on trees

**7.1.** Let  $G$  be a tree with  $n$  vertices. Prove that

$$\det A_G = \begin{cases} (-1)^{\frac{n}{2}}, & \text{if } G \text{ has a perfect matching;} \\ 0 & \text{otherwise.} \end{cases}$$

The characteristic polynomial of a graph  $G$  is the determinant of the matrix  $\tilde{A}_G = (\tilde{a}_{ij})$ , where

$$\tilde{a}_{ij} = \begin{cases} x & \text{for } i = j; \\ -1, & \text{if the vertices } v_i \text{ and } v_j \text{ are adjacent;} \\ 0 & \text{otherwise.} \end{cases}$$

Thus the characteristic polynomial is a polynomial in  $x$  and is denoted by  $\chi_G(x)$ .

Let  $m_k$  be the number of ways to choose  $k$  edges of the graph  $G$  so that no two edges are incident to the same vertex. The matching polynomial of  $G$  is

$$m_G(x) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^k m_k x^{n-2k}.$$

**7.2.** Let  $G$  be a tree. Prove that  $\chi_G(x) = m_G(x)$ .

# Solutions

**2.1.** a) This is obvious. Multiplication of the  $k$ th row of a matrix  $A$  by a number  $c$  corresponds to multiplication of weights of all edges from  $v_k$  by  $c$ . Each univalent subgraph contains just one of these edges. Hence its weight is also multiplied by  $c$ .

b) If a univalent graph contains an edge from a vertex  $v_k$  to a vertex  $v_i$  then let us call  $v_i$  a successor of  $v_k$ . Interchange of the  $j$ th and  $k$ th rows of a matrix  $A$  determines the following transformation of univalent subgraphs: the edge from  $v_k$  leads now not to the successor of  $v_k$  but to the successor of  $v_j$ , and the edge from  $v_j$  leads now to the successor of  $v_k$ . If  $v_k$  and  $v_j$  were in distinct cycles of length  $\ell_k$  and  $\ell_j$  respectively then now they occur to be in the same cycle of length  $\ell_k + \ell_j$ . And if the vertices were in the same cycle then it decomposes into two parts with the same total length. In both cases the number of even cycles changes by 1.

c) Every univalent subgraph of  $\mathcal{A}$  must contain a loop at the vertex  $v_k$ , so the edges leading to  $v_k$  from the other vertices cannot belong to any univalent subgraph. Hence there exists a natural  $\tilde{\mathcal{A}}$  bijection between univalent subgraphs of  $\mathcal{A}$  with nonzero weight and univalent subgraphs of  $\tilde{\mathcal{A}}$  with nonzero weight: it removes the loop at  $v_k$ . Since the weight of the loop is 1, this bijection saves the weight of the subgraph as well.

d) Each univalent subgraph contains one edge which corresponds to some element  $a_{ij}$  of the  $j$ th row. The weight of this subgraph equals to the product of  $a_{ij}$  and the product of weights of the remaining edges (and maybe also  $-1$ ). Replacing the weight of this edge by  $a_{ij}^{(1)}$  or  $a_{ij}^{(2)}$  we obtain univalent subgraphs from the decompositions of  $\det A^{(1)}$  and  $\det A^{(2)}$ , and the sum of weights of these subgraphs equals the weight of the first subgraph.

e) Represent the  $i$ th row of the matrix  $A$  as the sum of  $n$  rows:

$$(a_{i1}, 0, \dots, 0) + (0, a_{i2}, 0, \dots, 0) + \dots + (0, 0, \dots, a_{in}).$$

By the assertion of the preceding part of the problem, it suffices to check for each  $j$  that if the  $i$ th row of  $A$  equals  $(0, \dots, 0, a_{ij}, 0, \dots, 0)$  then  $\det A = (-1)^{i+j} a_{ij} \det A_{ij}$ .

A particular case of this assertion for  $j = i$  was already considered in part c). For certainty suppose  $i < j$ . Let us consecutively interchange the  $i$ th row of  $A$  with the  $(i+1)$ th one, then the  $(i+1)$ th row with the  $(i+2)$ th one and so on, the  $(j-1)$ th row with the  $j$ th one. As the result, the  $i$ th row of  $A$  gets the  $j$ th position and we obtain a matrix  $B$  such that its  $j$ th row is of the form  $(0, \dots, 0, a_{ij}, 0, \dots, 0)$ : the nonzero element  $a_{ij}$  is at the  $j$ th position, that is, on the diagonal. Moreover  $B_{jj} = A_{ij}$ ,  $\det B = (-1)^{j-i} \det A = (-1)^{j+i} \det A$ , and then we have by c)

$$\det A = (-1)^{j+i} \det B = (-1)^{j+i} a_{ij} \det B_{jj} = (-1)^{j+i} a_{ij} \det A_{ij}$$

as required.

As we see, the argument is not “purely combinatorial”. To justify it, let us consider the case  $j = i+1$  in combinatorial language, for the particular case  $n = 6$ ,  $i = 3$ ,  $j = 4$ . We wish to check the equality

$$\det \left( \begin{array}{cc|cc|cc} a & b & c & d & e & f \\ g & h & k & \ell & m & n \\ \hline 0 & 0 & 0 & a_{i,i+1} & 0 & 0 \\ o & p & q & r & s & t \\ \hline u & v & w & x & w & z \\ \alpha & \beta & \gamma & \delta & \epsilon & \phi \end{array} \right) = -a_{i,i+1} \cdot \det \left( \begin{array}{cc|cc|cc} a & b & c & e & f \\ g & h & k & m & n \\ \hline o & p & q & s & t \\ u & v & w & w & z \\ \hline \alpha & \beta & \gamma & \epsilon & \phi \end{array} \right).$$

Consider any digraph corresponding to the matrix on the left hand, remove the edges entering  $v_{i+1}$  and turn the edge  $v_i v_{i+1}$  into a new vertex  $v$ . The edges from  $v_{i+1}$  now exit from  $v$ , and the edges to  $v_i$  enter  $v$ . Then we obtain the digraph corresponding to the right-hand matrix. Now observe that since any univalent subgraph of the original graph contains the edge  $v_i v_{i+1}$  (the only edge from  $v_i$ ), it contains no other edge entering  $v_{i+1}$ . Thus the transformation leads to removal of the single edge  $v_i v_{i+1}$  which has weight  $a_{i,i+1}$  indicated on the right side. The sign

of the subgraph will change since a single cycle will change its parity. On the other hand, each univalent subgraph for the right-hand matrix clearly is obtained from a uniquely determined univalent subgraph for the left-hand matrix.

**2.2.** Suppose an element of  $A$ , for instance at position  $(1, 1)$ , is represented as  $a_{11} + b_{11}$ . In the digraph  $\mathcal{A}$  replace two loops at  $v_1$  with weights  $a_{11}$  and  $b_{11}$  by a single loop with weight  $a_{11} + b_{11}$ , obtaining a graph  $\tilde{\mathcal{A}}$ . Each univalent subgraph  $H$  of the digraph  $\tilde{\mathcal{A}}$  with a loop at  $v_1$  corresponds to two univalent subgraphs in  $\mathcal{A}$  with a loop at  $v_1$  with weight  $a_{11}$  or  $b_{11}$  respectively. The sum of the weights of these subgraphs equals the weight of  $H$ . And if a univalent subgraph of  $\tilde{\mathcal{A}}$  contains no loop at  $v_1$  then  $\mathcal{A}$  contains a subgraph isomorphic to it.

Summing up over all univalent subgraphs we see that joining of two loops or, equivalently, replacement of the formal sum  $a_{11} + b_{11}$  by its value retains the determinant of the matrix unchanged as required.

**2.3. a)** Consider the matrix

$$A = \begin{pmatrix} a_{12} + a_{13} + a_{14} & -a_{12} & -a_{13} & -a_{14} \\ -a_{21} & a_{21} + a_{23} + a_{24} & -a_{23} & -a_{24} \\ -a_{31} & -a_{32} & a_{31} + a_{32} + a_{34} & -a_{34} \\ -a_{41} & -a_{42} & -a_{43} & a_{41} + a_{42} + a_{43} \end{pmatrix}.$$

This form of recording (non-diagonal elements are with minus signs, their sums on the diagonal are with pluses) will be considered as standard. The following argument for this example is easily generalized.

According to the statement of the preceding problem, for calculating  $\det A$  we have to list univalent subgraphs in graph  $\mathcal{A}$  shown at fig. 7 left. However we will describe the construction, which enables us to restrict this listing by the subgraphs of graph  $\mathcal{A}_1$  obtained from  $\mathcal{A}$  by removal of all loops and signs at the weights of edges (fig. 7 right).



Рис. 7. Graphs  $\mathcal{A}$  and  $\mathcal{A}_1$

Since the labels in graph  $\mathcal{A}$  are repeated, some subgraphs may have equal weight (see fig. 8, a; at the moment, we ignore signs of weights). The labels on the edges of graph  $\mathcal{A}$  are the numbers  $\pm a_{ij}$ , and indexes  $i$  and  $j$  for each label are different. It is evident that the edge outgoing from vertex  $v_i$  is marked by a label with the first index equal to  $i$ . This implies that labels of all edges of any univalent subgraph of graph  $\mathcal{A}$  are pairwise different. Then introduce *new rule for the imaging of univalent subgraphs* of graph  $\mathcal{A}$ . Write all the labels of edges of a univalent subgraph and redraw the subgraph (on the same set of vertices), namely: for each label  $\pm a_{ij}$  we draw the edge leading from the vertex  $v_i$  to  $v_j$  marked by the label itself  $\pm a_{ij}$  (see fig. 8, b). It is evident that the graph drawn by the new rule does not have loops. It is in fact a subgraph of graph  $\mathcal{A}_1$ , the only difference is that the weights of edges of our subgraph may have a superfluous sign minus. A little later we will remove this difference.

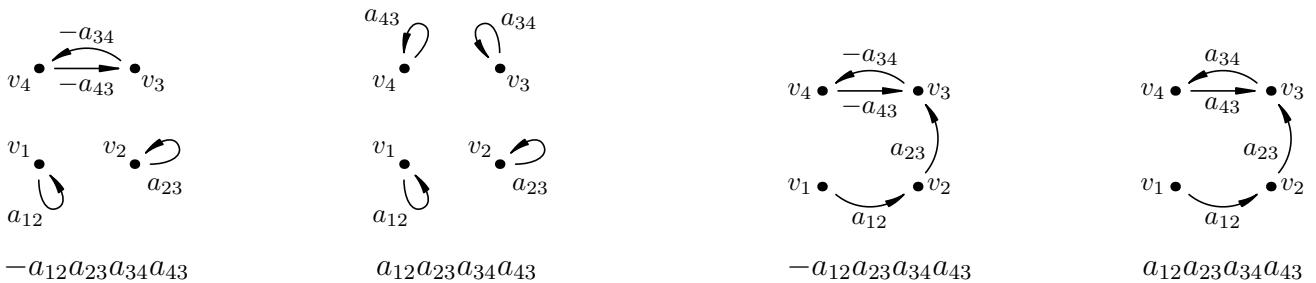


Рис. 8. New way for drawing graphs

The obtained subgraphs themselves are not univalent. Only the property that each vertex has one outgoing edge is remained from univalent graphs. A vertex may have either no incoming edge or several incoming edges. Call such graphs *sesquivalent*.

It is evident that any sesquivalent graph contains at least one cycle (move along arrows, then sometimes you will come to a vertex, where you have already been earlier), and if it contains more than one cycle then these cycles have no common vertices. Besides the cycles it may contain several trees planted on vertices of the cycles.

As it can be seen from fig. 8, b, identical sesquivalent graphs may have different edge labeling. The label of edge  $v_i v_j$  of a sesquivalent graph may be equal to  $+a_{ij}$  or  $-a_{ij}$ . However if this graph is obtained by the described rule from a univalent one then the assigning of the signs is not quite chaotic. Namely: a sesquivalent graph may be obtained from a univalent one if and only if:

1) for each of the cycles of this graph the property holds: either all edge labels are of the form  $+a_{ij}$  (such a cycle we call *positive*, in the univalent graph some set of loops corresponded to it), or all of them are of the form  $-a_{ij}$  (such a cycle we will call *negative*, in the univalent graph the same cycle corresponded to it);

2) the edges not belonging to any cycle, have labels of the form  $+a_{ij}$ .

The graphs possessing this property of edge labeling are called *admissible*.

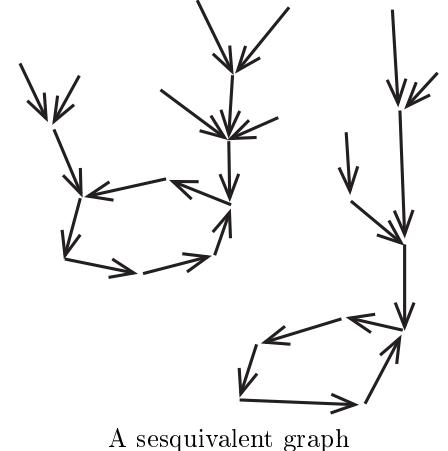
The rule for calculation of the weight of a sesquivalent graph is the same as for a univalent graph: the weight is equal to the product of edge weights, taken with the minus sign if the graph contains odd number of negative even cycles. We take into account only negative even cycles, since positive cycles of a sesquivalent graph correspond to sets of loops in the univalent graph, and loops do not affect the weight sign.

Dealing with sesquivalent graphs, it is convenient to write edge labels without signs at all but remember in addition about the sign of each cycle. In this case the weight of a sequivalent graph equals the product of weights of all its edges multiplied by  $(-1)^k$ , where  $k$  is the number of negative even cycles.

**Statement.** The determinant of matrix  $A$  equals the sum of weights of all admissible sesquivalent subgraphs in graph  $\mathcal{A}_1$ .

Properly, there is nothing to be proven. Admissible sesquivalent subgraphs of graph  $\mathcal{A}_1$  are in one-to-one correspondence with univalent subgraphs of graph  $\mathcal{A}$ , and this correspondence saves weights of subgraphs.

Turn to the problem solution. Now it is easy to check that  $\det A = 0$ . Indeed, consider whatever admissible sesquivalent subgraph and change the sign of the cycle passing through the vertex with the least number. We obtain another admissible subgraph. The second applying of this operation leads to the initial subgraph. Thus, with the help of this operation the set of all admissible sesquivalent subgraphs is split into pairs. But the sum of the weights of graphs in one



A sesquivalent graph

pair equals zero: if the pair is constructed by changing the sign of an even cycle then the numbers of negative cycles in graphs of this pair have different parity, and the sets of edge weights are identical; and if the pair is constructed by changing the sign of an odd cycle then the sign of the product of labels of this cycle does change.

b) Not to get involved in linear algebra, prove the problem statement generalizing the Matrix-tree theorem for the case of weighted oriented graphs. Let a complete digraph  $\mathcal{A}_1$  on  $n$  vertices without loops be given, in which between any two vertices  $v_i$  and  $v_j$  ( $i \neq j$ ) there exists as edge  $v_i v_j$  with weight  $a_{ij}$  as well as edge  $v_j v_i$  with weight  $a_{ji}$  (fig. 7, to the right). Matrix  $A$  from the problem condition is the Laplacian matrix of this graph.

We call a *rooted oriented spanning tree with root  $v_i$*  the acyclic graph on the set of vertices  $\{v_1, v_2, \dots, v_n\}$ , in which the outgoing degree for vertex  $v_i$  equals 0, and for any other vertex equals 1. In other words, for any vertex there exists the only path from it to  $v_i$ . The weight of the rooted oriented spanning tree equals the product of weights of the edges belonging to it.

The problem statement immediately follows from the theorem: the number  $(-1)^{i+j} \det A_{ij}$  equals the sum of weights of all rooted oriented trees with root  $v_i$ .

Let us prove this theorem. It is sufficient to consider the case  $i = n$ , the other cases are similar. Let  $\tilde{A}$  be an  $n \times n$  matrix such that its  $n$ -th row equals  $(0, \dots, 0, 1, 0, \dots, 0)$  (the unit is on  $j$ -th place), and the other matrix elements are the same as in matrix  $A$ . Then from the expansion of  $\det \tilde{A}$  in terms of  $n$ -th row we obtain

$$\det \tilde{A} = (-1)^{n+j} \cdot 1 \cdot \det A_{nj} \quad (5)$$

We will calculate the determinant  $\det A_{nj}$  with help of technique of sesquivalent graphs. As an example, we restrict the discussion to the case  $n = 5$ , let  $j = 2$ :

$$A_{25} = \begin{pmatrix} a_{12} + a_{13} + a_{14} + a_{15} & -a_{13} & -a_{14} & -a_{15} \\ -a_{21} & -a_{23} & -a_{24} & -a_{25} \\ -a_{31} & a_{31} + a_{32} + a_{34} + a_{35} & -a_{34} & -a_{35} \\ -a_{41} & -a_{43} & a_{41} + a_{42} + a_{43} + a_{45} & -a_{45} \end{pmatrix}.$$

It is convenient to assume that the rows of matrix  $A_{nj}$  are numbered from 1 to  $n-1$ , and the columns by numbers from 1 to  $n$ , but with omission of number  $j$ .

As in the previous part of the problem, one should choose one number in each row and each column (if the corresponding matrix element is written as a sum, one should take only one of the summands), after that construct edges of graph  $\mathcal{A}_1$  corresponding to the chosen numbers, and if an edge has weight with «superfluous» minus sign (for example, element  $-a_{13}$  has been chosen in the matrix) then we call such edge negative. We have obtained a graph on vertices  $\{v_1, \dots, v_n\}$  possessing the following properties (fig. 9).

- 1) Outgoing degree of vertices  $v_1, \dots, v_{n-1}$  equals 1, outgoing degree of vertex  $v_n$  equals 0.
- 2) One «negative» edge goes out from vertex  $v_j$ , and only «positive» edges may come in.
- 3) Negative edges form several cycles and one more «incomplete cycle», it is a path from  $v_j$  to  $v_n$  (this path becomes cycle, if we would supplement it by edge  $v_n v_j$  corresponding to element  $a_{nj}=1$  of matrix  $\tilde{A}$ ).
- 4) Positive edges may also form several cycles and also several oriented rooted trees planted in some vertices of the cycles (including the incomplete cycle).

The sign of such subgraph equals  $(-1)^{c+\ell}$ , where  $c$  is the number of negative even cycles,  $\ell$  is the number of edges in the incomplete cycle. Indeed, let us supplement the set of the chosen matrix elements generating the considering subgraph, by element  $a_{nj} = 1$ , and add edge  $v_n v_j$  to the subgraph. We have obtained the sesquivalent subgraph used in the calculation of  $\det \tilde{A}$ . The incomplete cycle will turn into a usual negative cycle, its contribution to the calculation of the sign of the subgraph will be just equal to  $(-1)^\ell$ . Let  $\pi$  be a permutation of the set  $\{1, 2, \dots, j-1, j+1, \dots, n\}$  which enumerates the columns of matrix  $A_{nj}$ . The operation of adding a new factor  $a_{nj}$  to the matrix elements chosen at the positions  $(1, \pi_1), (2, \pi_2), \dots, (n-1, \pi_{n-1})$  creates a permutation of the set  $\{1, 2, \dots, n\}$ , which has by  $n-j$  transpositions

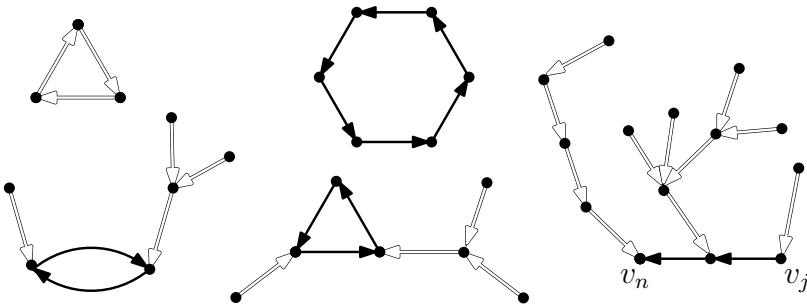


Рис. 9. «Negative» edges are indicated by black color, «positive» by white

more than  $\pi$ . Corrective sign  $(-1)^{n-j} = (-1)^{n+j}$  is assigned to all sesquivalent subgraphs in consideration and we see just it in formula (5).

Thus, the calculation of the determinant  $\det A_{ij}$  is reduced to the summation with appropriate signs of weights of all sesquivalent subgraphs with properties 1)–4). Applying the involution from the previous part of the problem (the changing of the sign of the cycle passing through the vertex with the least number), we cancel all subgraphs containing at least one cycle. Consider any of the remaining subgraphs, it is an oriented tree with root  $v_n$ . Let it contain  $\ell$  negative edges (these are the edges of the incomplete cycle), the sign of this subgraph equals  $(-1)^\ell$ , and the same is the product of the signs of “negative” edges. Therefore, the total weight of this subgraph is the product of the weights of edges of the tree.

Thus, the calculated determinant is the sum of the weights of all oriented trees with root  $v_n$ .

**2.4.** See [2, lemma 2.1]. In the following solution *1-factors* are just the *univalent* graphs. Split all the 1-factors of the graphs  $G$  and  $G'$  into groups, such that in every group the intersection of 1-factors with the subgraphs  $H$  and  $H'$  is the same. We will construct a bijection between the groups (and sometimes between individual 1-factors) that preserves the total weight.

1) If a 1-factor of the graph  $G$  has cycles that pass through edges  $x$  and  $y$  of the subgraph  $H$ , we map this 1-factor to the 1-factor of the graph  $G'$  in which the corresponding parts of these cycles are replaced by new edges  $x'$ ,  $y'$  (as in fig. 10, left). The parts of the initial cycles in the subgraph  $H$  contribute  $xy$  to the weight of the 1-factor. After the replacement, the contribution is  $x'y' = \frac{xy}{(wz-xy)^2}$  but we also have the multiplier  $(wz-xy)^2$  on the right hand side of (3). The total weight remains unchanged.

The case where the cycles contain edges  $w$  and  $z$  is treated analogously.



Рис. 10. Rebuilding of 1-factors

2) If a 1-factor of the graph  $G$  contains a long cycle passing through edges  $x, w$  in the subgraph  $H$ , and a cycle of the length 2 on the vertical edge (see fig. 10, right), then we map it to a 1-factor of the graph  $G'$  obtained by removing the 2-cycle and replacing the part of the long cycle by the new pair of edges  $z', y'$ . The preservation of weights can be checked as in the previous case.

We treat similar configurations in an analogous way.

3) Collect together all 1-factors of the graph  $G$  that coincide outside the subgraph  $H$  and contain a cycle passing through edges  $z, y, w$  (the contribution of this configuration to the weight of the 1-factor equals  $yzw$ ) or which contain a long cycle that passes through  $x$  and a 2-cycle along the edge  $y$  (this configuration contributes  $xy^2$  to the total weight). Observe that these two configurations have opposite signs, because the numbers of even cycles in them differ by 1. We map this set of 1-factors to the set of 1-factors in  $G$  that have the same structure outside the

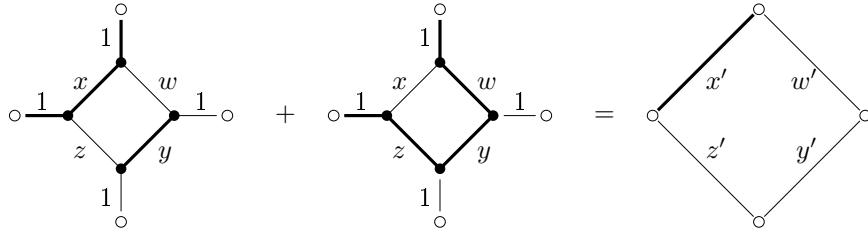


Рис. 11. Rebuilding of groups of 1-factors

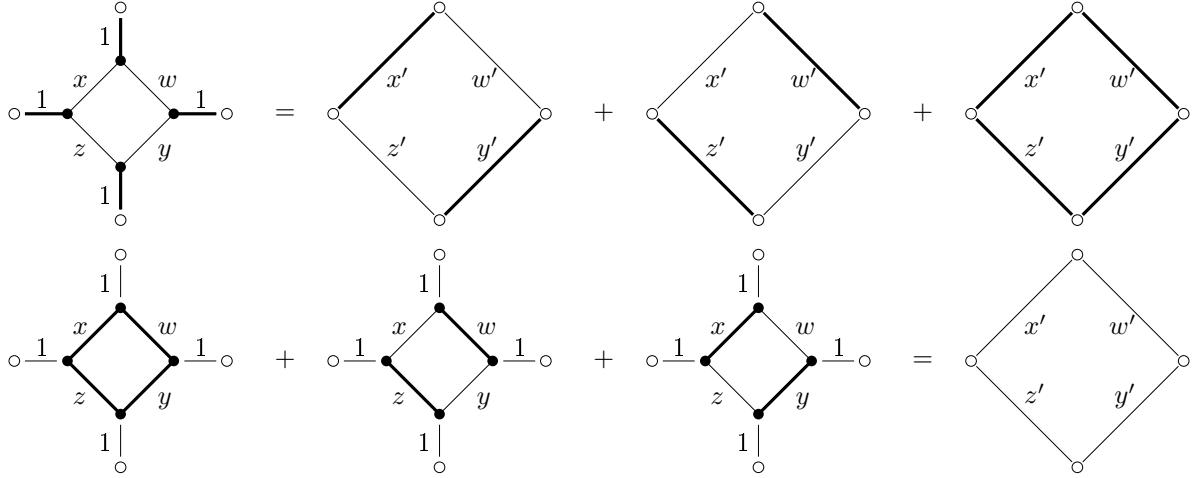


Рис. 12. The remaining identities

subgraph  $H$  (and so the contribution of the outer part is the same for both sets of 1-factors) and contain the edge  $x'$  (fig. 11, left). Thus again we see that the weights are equal because  $yzw - xy^2 = (wz - xy)^2 x'$ . The “dual” case is treated similarly (fig. 11, right).

4) We consider the remaining cases analogously (fig. 12). Note that the right cycle on the top of fig. 12, and the left cycle on the bottom of fig. 12 should be taken into account with two different orientations, which doubles their contribution. The equality of the weights at fig. 12 is due to the identities

$$1 = (wz - xy)^2(x'^2y'^2 + w'^2z'^2 - 2x'y'w'z') \quad \text{and} \quad x^2y^2 + w^2z^2 - 2xywz = (wz - xy)^2.$$

## 2.5. We have taken this problem from [2, example 2.2].

Applying the previous problem, we remove 4-cycles on the boundary of the cylinder step by step (fig. 13). To avoid zeros in denominators, we assume that the edges of the first cycle  $H_0$  on the boundary have weights  $x_0 = a$ ,  $z_0 = 1$ ,  $y_0 = a$ ,  $w_0 = 1$ , and all other edges in the graph have weight 1. After a single operation, the cycle  $H_0$  disappears, and we obtain a new cycle  $H_1$  on the boundary. The weights of its edges are the sums of the initial weights (equal to 1) and the new weights  $\frac{a}{1-a^2}$ ,  $\frac{1}{a^2-1}$ ,  $\frac{a}{1-a^2}$ ,  $\frac{1}{a^2-1}$  obtained by the formula (2). Thus

$$x_1 = 1 + \frac{a}{1-a^2}, \quad z_1 = 1 + \frac{1}{a^2-1}, \quad y_1 = 1 + \frac{a}{1-a^2}, \quad w_1 = 1 + \frac{1}{a^2-1}.$$

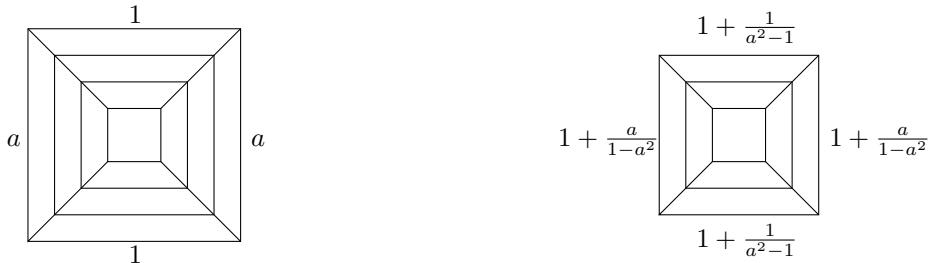


Рис. 13. Removing a cycle on the boundary of the cylinder

Then one can check by induction that after  $2n$  applications of these operations (it is more convenient to use induction step 2, because the formulae are slightly different for even and odd number of iterations) the weights of the edges of the boundary cycle are equal to

$$x_{2n} = y_{2n} = \frac{na^2 + a}{2na + 1}, \quad z_{2n} = w_{2n} = \frac{1 + 2na - na^2}{2na + 1},$$

and the product of the determinants of all removed cycles equals  $\det A(H_0) \det A(H_1) \dots \det A(H_{2n-1}) = (2na + 1)^2$ .

If  $m$  is even, say  $m - 1 = 2n + 1$ , then after  $2n$  operations the remaining graph consists of the unique 4-cycle with the weights given by the above formulas. The determinant of the matrix of this cycle equals

$$(x_{2n}y_{2n} - z_{2n}w_{2n})^2 = \left( \frac{(2n+1)a+1}{2na+1} \right)^2 (a-b)^2,$$

and the total determinant equals

$$\det A(H_0) \det A(H_1) \dots \det A(H_{2n}) (x_{2n}y_{2n} - z_{2n}w_{2n})^2 = ((2n+1)a+1)^2 (a-b)^2.$$

For  $a = b = 1$  this expression vanishes. If  $m$  is odd, we obtain by the similar reasoning that the determinant is equal to  $((m-1)a+1)^2$ , and for  $a = b = 1$  this is equal to  $m^2$ .

**3.1.** [1, theorem 2.1]. Consider a chess coloring of the figure, and split the edges of each univalent subgraph onto two groups: edges which start from black vertices and edges which start from white vertices. Edges of each group determine a matching, which can be interpreted as a tiling. This map is bijective.

**3.2.** [1, lemma 2.3]. Induction on the area. If the dual graph contains terminal vertex then cut the corresponding cell. Otherwise cut a suitable corner cell.

**3.3.** [1, theorem 2.4]. Consider an arbitrary univalent subgraph in  $G_F$ . Obviously the number of rising edges in it equals to the number of falling edges, denote this number by  $v$ . Let the univalent subgraph consist of  $k$  cycles. Each cycle is a polygon. Since all of the cycles have even length, they contain all the vertices in total, and the figure is simply connected, there is an even number of cells inside each cycle. Therefore applying the statement of the previous problem to each cycle, we can omit the term  $2d$  in the left hand side of the congruence. Now if we sum up over the set of all cycles then we obtain

$$A - B + 2 \cdot k \equiv \text{the total length of all vertical sides} = 2 \cdot v, \pmod{4}$$

where  $A$  is equal to the number of integer points with even ordinates and  $B$  is the number of integer points with odd ordinates on the boundary of cycles. Since the univalent subgraph covers all integer points of the figure, the difference  $A - B$  is even and does not depend on the subgraph. Put  $A - B = 2 \cdot t$ . Then  $2 \cdot v \equiv 2 \cdot t + 2 \cdot k \pmod{4}$ , and so  $v \equiv t + k \pmod{2}$ . Since  $t$  does not depend on the subgraph, the theorem is proven.

**3.4.** [1, lemma 2.5]. The statement is trivial if we use “horizontal zebra” coloring, but we will demonstrate another reasoning.

Let us interpret a tiling as a univalent subgraph (each domino is interpreted as 1-cycle), then the number of cycles equals the number of dominoes, the number of rising edges is equal to the number of vertical dominoes. Then

$$\begin{aligned} & \text{number of cycles} + \text{number of rising edges} = \\ & = \text{number of dominoes} + \text{number of vert. dominoes} \equiv \text{number of horiz. dominoes}. \end{aligned} \tag{6} \pmod{2}$$

We know from the previous problem that the parity of the sum at the l.h.s. does not depend on the subgraph. Therefore the parity of the number of horizontal dominoes in all tilings is the same. Hence the definition of sign of does not depend on tiling.

Let us formulate one generalization of the above observations. If  $\text{sgn}F = 1$ , i.e. an even number is in the right-hand side of the formula (6) then in any tiling (and therefore in any univalent subgraph by the statement of problem 3.3) the parity of the number of rising edges coincides with the parity of the number of the cycles, and if  $\text{sgn}F = -1$  then these parities are opposite. By the other words, for any univalent subgraph  $\pi$  in graph  $G_F$

$$(-1)^{\text{number of rising edges in } \pi} = \text{sgn}F \cdot (-1)^{\text{number of cycles in } \pi}. \quad (7)$$

Remind that graph  $G_F$  is bipartite, all its cycles are even, therefore we obtain the formula

$$\det A_F = \text{sgn}F \cdot \sum_{\pi} (-1)^{\text{number of rising edges in } \pi}. \quad (8)$$

**3.5.** [1, theorem 2.7]. Denote by  $\gamma_k$  the number of univalent subgraphs of  $G_F$  with  $k$  rising edges. Then

$$\det A_F = \text{sgn}F \cdot \sum_{\pi} (-1)^{\text{number of ascending edges in } \pi} = \text{sgn}F \cdot \sum_{k=0}^{+\infty} \gamma_k \cdot (-1)^k. \quad (9)$$

It is clear due to the bijection from the problem 3.1 that the coefficient of  $x^k$  in the expression  $f_F(x)^2$  is equal to the number of univalent subgraphs with exactly  $k$  vertical edges. The number of ascending edges in a univalent subgraph equals one half of the number of vertical edges, therefore  $f_F(x)^2 = \sum_{k=0}^{+\infty} \gamma_k x^{2k}$ . Substitute  $x = \mathbf{i}$ , and the formula (9) gives us the first equality. In particular, we have proven the equality

$$\det A_F = \text{sgn}F \cdot f_F(\mathbf{i})^2. \quad (10)$$

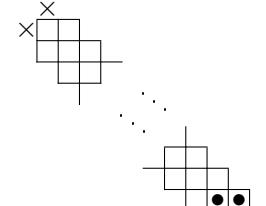
**3.6.** [1, theorem 2.8]. Let us calculate  $\det A_F$  by the formula (10). If a good pair consists of the tiling with  $k$  vertical dominoes and the tiling with  $k+2$  vertical dominoes then its contribution to  $f_F(\mathbf{i})$  is equal to  $\mathbf{i}^k + \mathbf{i}^{k+2} = 0$ . Therefore all good pairs contribute zero to  $f_F(\mathbf{i})$  and the first claim of the problem follows.

If the set of all tilings, except one, can be split into good pairs then we denote the number of vertical and horizontal dominoes in the remaining tiling by  $v$  and  $h$ ,  $h+v = s(F)$ . Then  $f_F(\mathbf{i}) = \mathbf{i}^v$  by the previous reasoning,  $\text{sgn}F = (-1)^h$  and therefore

$$\det A_F = \text{sgn}F \cdot f_F^2(\mathbf{i}) = (-1)^{h+v} = (-1)^{s(F)}.$$

**3.7.** [1, theorem 2.11]. The expression  $n(n-1)$  in the formula equals the area of any regular stamp. By problem 3.6 it is sufficient to check that the set of all tilings of each regular stamp, except one, can be split into good pairs and that the set of all tilings of each irregular stamp can be split into good pairs. We will check both statements by the induction on  $n$ . We need the following lemma [5, lemma 2.1].

**L e m m a** (about a “halfdiagonal”). Suppose figure  $F$  contains three diagonal sequences of cells, like on the figure to the right, and cells which are marked by crosses do not belong to the figure. Then the set of all tilings of figure  $F$  which do not contain the domino marked with bold circles can be split into good pairs.



**P r o o f o f t h e l e m m a.** Consider the middle of one of these diagonal sequences. Prove that there exists a  $2 \times 2$  square consisting of two dominoes of the tiling and containing two squares of this diagonal sequence (rearranging the dominoes in such square we easily split the set of the tilings into pairs). Indeed, if there is no such a square then looking through this sequences of squares starting from the left corner, we see that each next domino covering the diagonal square has also to cover either the square to the right or the square downward. Coming to the lower right corner we obtain the contradiction.

Turn to the problem solution.

1) We will check by induction on  $n$  (the size of stamp) that the set of all tilings of each regular stamp, except one, can be split into good pairs. The base is trivial.

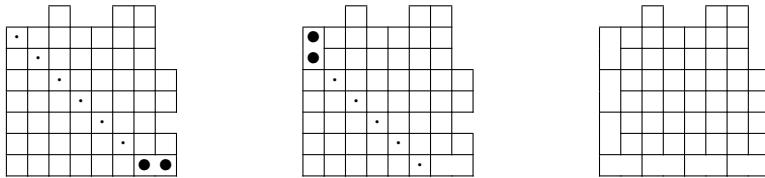


Рис. 14. Construction of an «unpaired» tiling of  $(n + 1)$ -stamp

Step of induction,  $n \rightarrow n + 1$ . Consider a regular  $(n + 1)$ -stamp. We will split the set of its tilings into good pairs. For this we take a look at the bottom-right and upper-left corner cells of the  $(n + 1)$ -stamp. One of these cells lies inside the  $n \times n$  square, let it be the upper-left cell. Apply the halfdiagonal lemma in the bottom-right direction starting from this cell. Then the set of tilings which do not contain the marked domino (figure 14, left) can be split into good pairs. Let's look at tilings, which contain this domino. Apply the halfdiagonal lemma again in the upper-left direction starting from the cell to the left of the marked domino (figure 14, middle). By this lemma the set of tilings which does not contain the marked domino in the upper-left corner, can be split into good pairs. The remaining tilings contain this domino. Apply the halfdiagonal lemma once again in the bottom-right direction from the cell below the domino, and so on. As a result of repeated application of the halfdiagonal lemma, we split the set of tilings into pairs except the tilings containing all the dominoes on the left and the bottom sides of our  $(n + 1)$ -stamp (fig. 14, right). There is a bijection between the remaining tilings and the tilings of the remaining  $n$ -stamp. Therefore all tilings except one can be split into good pairs.

2) Check by induction on  $n$  that the set of all tilings of each irregular stamp can be split into good pairs. The base is trivial.

Step of induction,  $n - 1 \rightarrow n$ . Consider an arbitrary  $n$ -stamp. We mark some cells of its  $n \times n$  square as at figure 15.

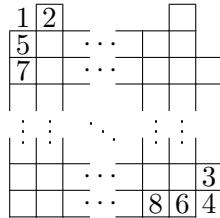


Рис. 15. Layout of the cells for the irregular stamp

Consider the following cases.

1) The figure does not contain cells 1 and 4. Consider the diagonal from 5 to 6. By the halfdiagonal lemma the set of all tilings can be split into pairs (because the marked domino does not belong to the figure). The case when four cells 1, 2, 3, 4 don't belong to the stamp is considered similarly.

2) The stamp contains the cell 1 but not the cell 4 (or vice versa). Consider the first case, the second one is similar. Apply the halfdiagonal lemma in the direction from 6 to 1. As in the proof of the previous item, we split the set of all tilings into pairs, except those tilings for which the position of dominoes on the leftmost column and bottom row is fixed as at figure 14, right. The set of exceptional tilings can be split into good pairs by induction hypothesis.

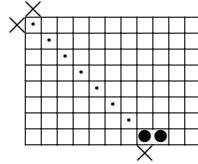
3) Cells 1 and 4 belong to the stamp but 2 and 3 do not belong. Then each tiling contains dominoes 1 – 5 and 4 – 6. Cut them. By the halfdiagonal lemma which we apply in the direction from 7 to 8, the set of all tilings can be split into good pairs.

4) Cells 1, 2, 4 belong to the stamp but 3 does not belong (or similarly 1, 3, 4 belong to the stamp but 2 does not belong). Obviously each tiling contains the dominoes 4 – 6. Cut it. Apply the halfdiagonal lemma in the direction from 8 to 7. Observe that each tiling contains the

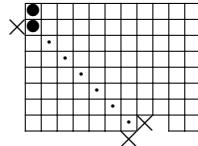
dominoes 5 – 7 and therefore each tiling contains the dominoes 1 – 2. We cut these dominoes and finish the proof by induction, like in item 2.

**3.8.** [1, theorem 2.12]. Check that the number of tilings of  $m \times n$  rectangle is odd iff the numbers  $m + 1$  and  $n + 1$  are coprime, in the case when the number of tilings is even all these tilings can be split into good pairs, and if it is odd then all tilings except one can be split into good pairs. Then the statement of the problem follows from Problem 3.6.

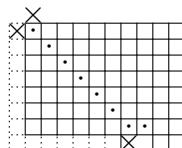
Induction realizes Euclidean algorithm. Consider the diagonal sequence of squares outgoing from the corner. By the halfdiagonal lemma, it is sufficient to investigate the parity of the numbers of tilings containing the marked domino.



Now we can take the diagonal sequence of squares below the row just considered, and looking through it from bottom to top apply the halfdiagonal lemma again.



Continuing to move down the diagonal in question and not changing the parity of the number of tilings, we can remove all the squares of the first column and also all the squares of the lower row to the left from the marked domino. Now we can apply the halfdiagonal lemma again.



Continuing further we will remove the squares of the second column and the second row (lying to the left from the domino that we had found). Acting in such a way, we will remove the rectangular part of size  $(n + 1) \times n$  from our  $m \times n$  rectangle finally. We have obtained  $(m - n - 1) \times n$  part that satisfies the induction hypothesis.

**4.1.** Let  $\mathcal{D}$  denote the set of all signed digraphs  $D$  obtained as described before the formulation of the problem from the terms of the superexpansion. We write  $\pi_D$  for the associated permutation. We divide  $\mathcal{D}$  into three parts as follows:

- $\mathcal{T}$ , the  $D \in \mathcal{D}$  with no directed cycle;
- $\mathcal{D}^+$ , the  $D \in \mathcal{D}$  with  $\text{sgn}(D) = +1$  and at least one directed cycle;
- $\mathcal{D}^-$ , the  $D \in \mathcal{D}$  with  $\text{sgn}(D) = -1$  and at least one directed cycle.

Here is a plan for the rest of the proof. We will show that all  $D \in \mathcal{T}$ , the “acyclic objects”, have positive signs, and they are in one-to-one correspondence with the spanning trees of  $G$ ; thus they count what we want. Then, by constructing a suitable bijection, we will prove that  $|\mathcal{D}^+| = |\mathcal{D}^-|$ —so the “cyclic objects” cancel out. We then have  $\det(L^-) = \sum_{D \in \mathcal{D}} \text{sgn}(D) = |\mathcal{T}| + |\mathcal{D}^+| - |\mathcal{D}^-| = |\mathcal{T}|$  and the theorem follows.

To realize this plan, we first collect several easy properties of the signed digraphs in  $\mathcal{D}$ .

- (i) *If  $i \rightarrow j$  is a directed edge, then  $\{i, j\}$  is an edge of  $G$ . (Clear.)*
- (ii) *Every vertex, with the exception of  $n$ , has exactly one outgoing edge, while  $n$  has no outgoing edge. (Obvious.)*
- (iii) *All incoming edges of  $n$  are positive. (Since  $L^-$  has only  $n - 1$  rows and columns.)*

- (iv) No vertex has more than one negative incoming edge. (This is because two negative incoming edges  $j \rightarrow i$  and  $k \rightarrow i$  would mean two circled entries  $\ell_{ji}$  and  $\ell_{ki}$  in the  $i$ th column.)
- (v) If a vertex  $i$  has a negative incoming edge, then the outgoing edge is also negative. (Indeed, a negative incoming edge  $j \rightarrow i$  means that the off-diagonal entry  $\ell_{ji}$  is circled, and hence none of the 1s in the diagonal entry  $\ell_{ii}$  may be circled—which would be the only way of getting a positive outgoing edge from  $i$ .)

*Claim A.* These properties characterize  $\mathcal{D}$ . That is, if  $D$  is a signed digraph satisfying (i)–(v), then  $D \in \mathcal{D}$ .

*Доказательство.* Given  $D$ , we determine the circled entry in each row  $i$ ,  $1 \leq i \leq n - 1$ , of  $L^-$ . We look at the single outgoing edge  $i \rightarrow j$ . If it is positive, we circle the appropriate 1 in  $\ell_{ii}$ , and if it is negative, we circle  $\ell_{ij}$ . We cannot have two circled entries in a single column, since they would correspond to the situations excluded in (iv) or (v).  $\square$

Next, we use (i)–(v) to describe the structure of  $D$ .

*Claim B.* Each  $D \in \mathcal{D}$  has the following structure (illustrated below).

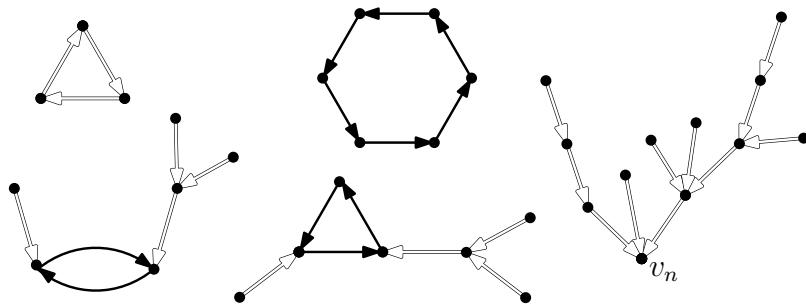


Рис. 16.

- (a) The vertex set is partitioned into one or more subsets  $V_1, V_2, \dots, V_k$  corresponding to the components of  $D$ , with no edges connecting different  $V_i$ . If  $V_1$  is the subset containing the vertex  $n$ , then the subgraph on  $V_1$  is a tree with all edges directed toward  $n$ . The subgraph on every other  $V_i$  contains a single directed cycle of length at least 2, and a tree (possibly empty) attached to each vertex of the cycle, with edges directed toward the cycle.
- (b) The edges not belonging to the directed cycles are all positive, and in each directed cycle either all edges are positive or all edges are negative.
- (c) Conversely, each possible  $D$  with this structure and satisfying (i) above belongs to  $\mathcal{D}$ .

*Sketch of a proof.* Part (a), describing the structure of the digraph, is a straightforward consequence of (ii) (a single outgoing edge for every vertex except for  $n$ ), and we leave it as an exercise. (If we added a directed loop to  $n$ , then every vertex has exactly one outgoing edge, and we get a so-called *functional digraph*, for which the structure as in (a) is well known.)

Concerning (b), if we start at a negative edge and walk on, condition (v) implies that we are going to encounter only negative edges. Thus, we cannot reach  $n$ , since its incoming edges are positive, and so at some point we start walking around a negative cycle. Finally, a negative edge cannot enter such a negative cycle from outside by (iv).

As for (c), if  $D$  has the structure as described in (a) and (b), the conditions are obviously satisfied and Claim A applies. This proves Claim B.

The first item in our plan of the proof is now very easy to complete.

All  $D \in \mathcal{T}$  have a positive sign and they are in one-to-one correspondence with the spanning trees of  $G$ . Indeed, if  $D \in \mathcal{D}$  has no directed cycles then  $D$  is a tree with positive edges directed toward the vertex  $n$ . Moreover,  $\pi_D$  is the identity permutation since all the circled elements in

the term corresponding to  $D$  lie on the diagonal of  $L^-$ . Thus  $\text{sgn}(D) = +1$ , and if we forget the orientations of the edges, we arrive at a spanning tree of  $G$ . Conversely, given a spanning tree of  $G$ , we can orient its edges toward  $n$ , and we obtain a  $D \in \mathcal{T}$ .

It remains to deal with the “cyclic objects”. For  $D \in \mathcal{D}^+ \cup \mathcal{D}^-$ , let the *smallest cycle* be the directed cycle that contains the vertex with the smallest number (among all vertices in cycles). Let  $\bar{D}$  be obtained from  $D$  by changing the signs of all edges in the smallest cycle.

Obviously  $\bar{\bar{D}} = D$ , and for  $D \in \mathcal{D}$  we have  $\bar{D} \in \mathcal{D}$  as well, as can be seen using Claim B. The following claim then shows that the mapping sending  $D$  to  $\bar{D}$  is a bijection between  $\mathcal{D}^+$  and  $\mathcal{D}^-$ , which is all that we need to finish the proof of the theorem.

*Claim C.*  $\text{sgn}(\bar{D}) = -\text{sgn}(D)$ .

*Proof.* We have  $\text{sgn}(D) = \text{sgn}(\pi_D)(-1)^m$ , where  $m$  is the number of negative edges of  $D$  and  $\pi_D$  is the associated permutation.

Let  $i_1, i_2, \dots, i_s$  be the vertices of the smallest cycle of  $D$ , numbered so that the directed edges of the cycle are  $i_1 \rightarrow i_2, i_2 \rightarrow i_3, \dots, i_{s-1} \rightarrow i_s, i_s \rightarrow i_1$ .

In one of  $D$  and  $\bar{D}$ , the smallest cycle is positive; say in  $D$  (if it is positive in  $\bar{D}$ , the argument is similar). Positive edges correspond to entries on the diagonal of  $L^-$ , and thus the  $i_j$  are fixed points of the permutation  $\pi_D$ , i.e.,  $\pi_D(i_j) = i_j, j = 1, 2, \dots, s$ . In  $\bar{D}$ , the smallest cycle is negative, and so for  $\pi_{\bar{D}}$  we have  $\pi_{\bar{D}}(i_1) = i_2, \dots, \pi_{\bar{D}}(i_{s-1}) = i_s, \pi_{\bar{D}}(i_s) = i_1$ , which means that  $i_1, i_2, \dots, i_s$  form a *cycle* of the permutation  $\pi_{\bar{D}}$ . Otherwise,  $\pi_D$  and  $\pi_{\bar{D}}$  coincide.

Now it is easy to check that  $\pi_{\bar{D}}$  can be converted to  $\pi_D$  by  $s-1$  transpositions (which “cancel” the cycle  $(i_1, i_2, \dots, i_s)$ ). Since each transposition changes the sign of a permutation, we have  $\text{sgn}(\pi_{\bar{D}}) = (-1)^{s-1}\text{sgn}(\pi_D)$ , and so

$$\text{sgn}(\bar{D}) = \text{sgn}(\pi_{\bar{D}})(-1)^{m+s} = (-1)^{s-1}\text{sgn}(\pi_D)(-1)^{m+s} = -\text{sgn}(D).$$

Claim C, and thus also the theorem, are proved.

**4.2. a)** Consider  $\bar{G}$ , in which  $V(\bar{G}) = V(G) \cup \{w\}$ ,  $E(\bar{G}) = E(G) \cup \{v_i w\}$ . Denote the Laplacian matrix of graph  $\bar{G}$  by  $\bar{L}$ . It is not difficult to understand that  $\bar{L}^- = L + E_{i,i}$ . The numbers of spanning trees of graphs  $G$  and  $\bar{G}$  coincide too. Consequently, by the Matrix-tree theorem, the number of spanning trees of graphs  $G$  and  $\bar{G}$  equals  $\det \bar{L}^- = \det(L + E_{i,i})$ , Q. E. D.

b)  $\det(L + E_{i,j}) - \det(L + E_{i,i}) = \det M$ ;  $M = (m_{kn})$ , where

$$m_{kn} = \begin{cases} \ell_{kn} & \text{for } k \neq i; \\ -1, & \text{if } k = i \text{ and } n = j; \\ 1, & \text{if } k = i \text{ and } n = i; \\ 0 & \text{in the other cases.} \end{cases} \quad (11)$$

Note that the sum of elements in each row of matrix  $M$  equals 0, and by problem 2.3  $\det M = 0$ . Therefore,  $\det(L + E_{i,j}) = \det(L + E_{i,i})$ , and the required statement follows from the previous part.

**4.3.** With light overwithundertwist this statement is immediately obtained similarly to the solution of problem 2.3.a).

**4.4.** The version with weights of this statement is proved in solution of problem 2.3.b).

**4.5.** This is the problem on linear algebra. One can read an elegant solution, for example, in D. Karpov “Graph theory” <https://ru.overleaf.com/project/5fd1061de5a509b3447a4f55>.

**4.6.** Apply the Matrix-tree theorem and calculate the determinant of matrix  $L^-$ . For a complete graph it is an  $(n-1) \times (n-1)$  matrix of the form

$$\det \begin{pmatrix} n-1 & -1 & \dots & -1 \\ -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & n-1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ -1 & n-1 & \dots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \dots & n-1 \end{pmatrix} = \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & n & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & n \end{pmatrix} = n^{n-2}.$$

Here in the first equality we have added the rows with numbers from 2 up to  $n - 1$  to the first row, the determinant has not changed from this action. In the second equality we conversely have added the first row to all the others. Finally, only the graph consisting of  $n - 1$  loops has nonzero weight among univalent graphs, and this implies the third equality.

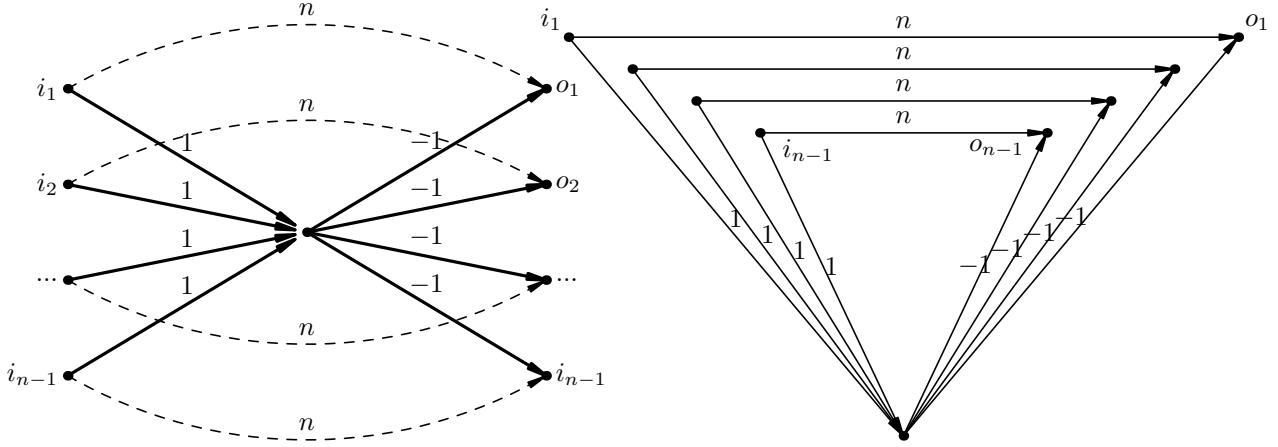


Рис. 17.

We give, however, a more combinatorial argument applying the generalization of the statement of problem 6.6 b).

*The weighted version of problem 6.6 b).* Let a graph satisfying to the condition of problem 6.6 a) be given. On each edge of the graph, write a real number which will be called the weight of the edge. The product of weights of the edges forming a path is called the weight of this path. The weight of a set of  $n$  paths is the product of weights of all paths from this set, multiplied by  $(-1)^{|\pi|}$ , where  $\pi$  is the permutation determined by this set of paths. Denote by  $a_{ij}$  the sum of weights of all paths from  $i$ th inlet to  $j$ th outlet. Then the determinant of matrix  $(a_{i,j})$  is equal to the sum of weights of all sets consisting of  $n$  non-intersecting paths.

The proof is similar to the proof 6.6 b.

So, we want to find the determinant of matrix  $L^-$ . Look at the graph on the picture (fig. 17). Left and right parts contain  $n - 1$  vertices each. Note that the number of paths from  $i$ th inlet to  $j$ th outlet is just equal to  $\ell_{ij}$ . Therefore, by the weighted version of problem 6.6 b),  $\det L^-$  is equal to the sum of weights of sets consisting of  $n$  non-intersecting paths. And there exists one set of  $n$  paths of weight  $n^{n-1}$ , where  $i$ th inlet is immediately connected with  $i$ th outlet, and  $n - 1$  sets of weight  $-n^{n-2}$ . Hence, the sum of weights of sets consisting of  $n$  non-intersecting paths is equal to

$$n^{n-1} - (n - 1) \cdot n^{n-2} = n^{n-2}.$$

According to the statement of the preceding problem, for calculating  $\det A$  we have to list univalent subgraphs in graph  $\mathcal{A}$  shown at fig. 7 left. However we will describe the construction, which enables us to restrict this listing by the subgraphs of graph  $\mathcal{A}_1$  obtained from  $\mathcal{A}$  by removal of all loops and signs at the weights of edges (fig. 7 right).

**4.7.** Apply the Matrix-tree theorem. The Laplacian matrix here looks as

$$L = \left( \begin{array}{cccccc} k & \dots & 0 & -1 & \dots & -1 \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & k & -1 & \dots & -1 \\ -1 & \dots & -1 & \ell & \dots & 0 \\ \vdots & & \vdots & \ddots & & \vdots \\ -1 & \dots & -1 & 0 & \dots & \ell \end{array} \right) \quad \left\{ \begin{array}{l} \ell \text{ rows} \\ k \text{ rows} \end{array} \right.$$

We will find the determinant of matrix  $M = L_{\ell, \ell+1}$  (the notation from problem 2.1 e). By problem 2.3.b)  $\det L^- = -\det M$ .

$$M = \left( \begin{array}{ccccccc} k & \dots & 0 & 0 & -1 & \dots & -1 \\ \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & k & 0 & -1 & \dots & -1 \\ -1 & \dots & -1 & -1 & 0 & \dots & 0 \\ -1 & \dots & -1 & -1 & \ell & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & \dots & -1 & -1 & 0 & \dots & \ell \end{array} \right) \quad \left. \begin{array}{l} \ell - 1 \text{ rows} \\ \\ k - 1 \text{ rows} \end{array} \right\}$$

Give two combinatorial calculations of the determinant of matrix  $M$ . The first way of determinant calculation is similar to determinant calculation in problem 4.6. Namely, look at fig. 18 left. It is not difficult to check that the sum of weights of paths from  $i$ -th inlet to  $j$ -th outlet equals  $m_{ij}$ . Therefore, by the weighted version of problem 6.6 b),  $\det M$  equals the sum of weights of the sets consisting of  $n$  non-intersecting paths. It is easy to understand that there exists exactly one such path, and its weight equals  $-k^{\ell-1}\ell^{k-1}$ , which finishes the calculation.

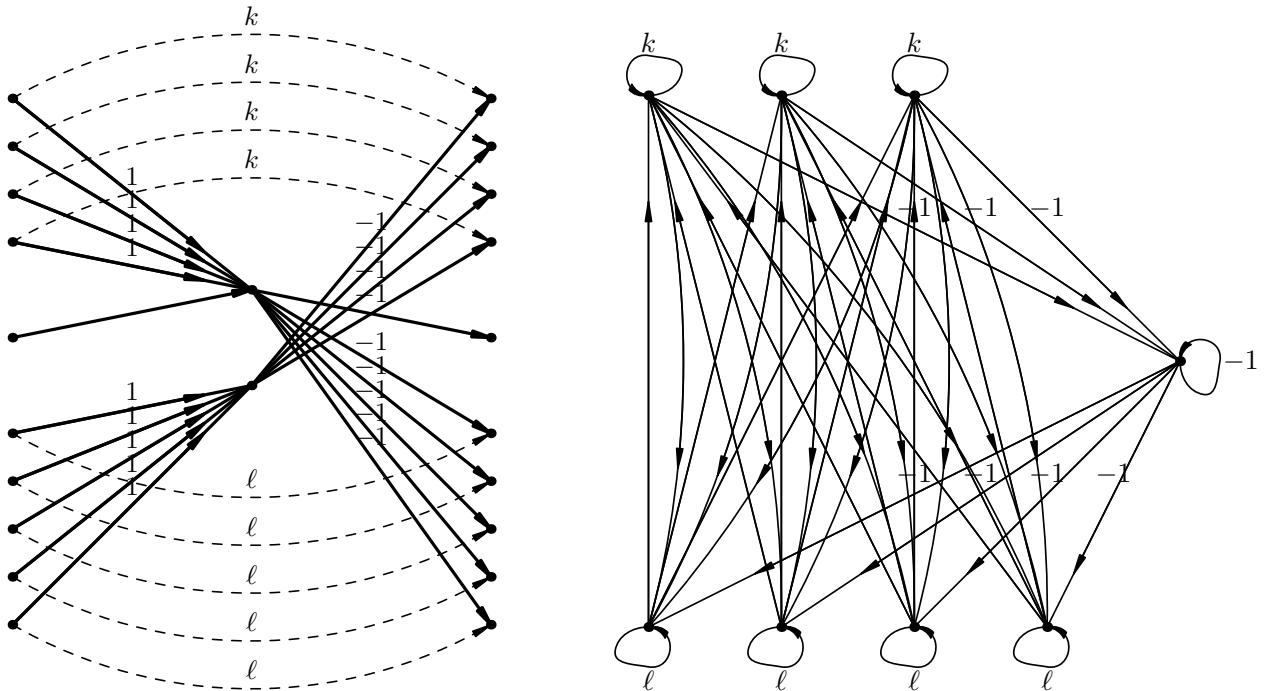
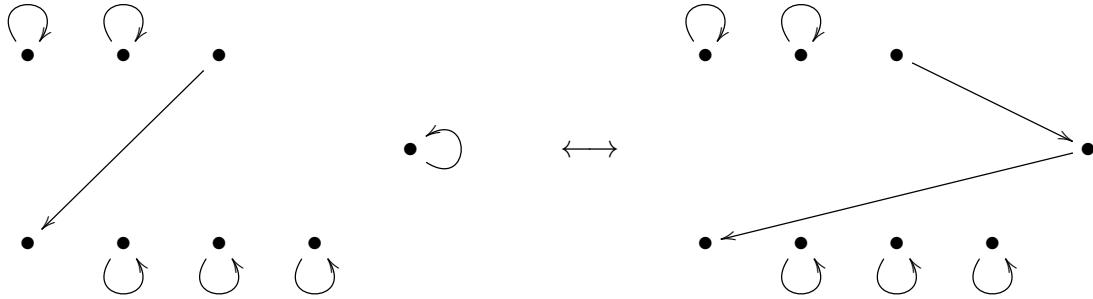


Рис. 18.

The second way of calculation uses the definition of determinant via univalent graphs. Fig. 18 right shows the graph such that  $\det M$  counts its univalent subgraphs. In this graph  $\ell - 1$  vertices of the first part are located on the top,  $k - 1$  vertices of the second part are located on the bottom, and a single special vertex is located at the right.

First, split univalent graphs into pairs which contain at least 2 edges going from the second part to the first. Namely, among all the edges going from the second part to the first, choose two edges the ends of which have the least number and interchange the ends of these edges. Then the permutation will change its parity. It is not difficult to understand that this correspondence is bijective on the given set, therefore all corresponding graphs will be cancelled.

Second, split univalent graphs into pairs containing exactly one edge going from the second part to the first. As there exists exactly one edge outgoing from the second part, there exists either exactly one edge incoming to the second part or a path consisting of two edges passing through the special vertex. Then rebuild the graph depending on from where this edge goes:



So we retain only univalent graphs such that no edge leads to the second part. It is clear that the only graph possessing this property is the graph consisting of all loops. The weight of this graph, and consequently also  $\det M$ , is equal to  $-k^{l-1}l^{k-1}$ .

**4.8.** Apply the Matrix-tree theorem. Expand  $\det L^-$  into univalent graphs by the combinatorial definition. If there exists at least one loop in a univalent graph then the univalent graph has even weight. Otherwise since the number of vertices in a univalent graph is odd, there exists a cycle of length at least 3. Therefore reversing of all arrows leads to another univalent graph of the same weight. Thus we have split some univalent graphs into pairs of equal weight, and for the others we have understood that they give even contribution. This immediately implies that the corresponding determinant is even.

**5.1.** The formula for the determinant implies that if  $G$  has no perfect matching, then  $\det(A)$  is the zero polynomial.

To show the converse, we fix a permutation  $\pi$  that defines a perfect matching, and we replace the variables in  $\det(A)$  as follows:  $x_{i,\pi(i)} := 1$  for every  $i = 1, 2, \dots, n$ , and all the remaining  $x_{ij}$  are 0. We have  $\text{sgn}(\pi) \cdot x_{1,\pi(1)}x_{2,\pi(2)} \cdots x_{n,\pi(n)} = \pm 1$  for this  $\pi$ .

For every other permutation  $\sigma \neq \pi$  there is an  $i$  with  $\sigma(i) \neq \pi(i)$ , thus  $x_{i,\sigma(i)} = 0$ , and therefore, all other terms in the expansion of  $\det(A)$  are 0. For this choice of the  $x_{ij}$  we thus have  $\det(A) = \pm 1$ .

**5.2.** We proceed by induction on  $m$ . The univariate case is clear, since there are at most  $d$  roots of  $p(x_1)$  by a well-known theorem of algebra. (That theorem is proved by induction on  $d$ : if  $p(\alpha) = 0$ , then we can divide  $p(x)$  by  $x - \alpha$  and reduce the degree.)

Let  $m > 1$ . Let us suppose that  $x_1$  occurs in at least one term of  $p(x_1, \dots, x_n)$  with a nonzero coefficient (if not, we rename the variables). Let us write  $p(x_1, \dots, x_m)$  as a polynomial in  $x_1$  with coefficients being polynomials in  $x_2, \dots, x_n$ :

$$p(x_1, x_2, \dots, x_m) = \sum_{i=0}^k x_1^i p_i(x_2, \dots, x_m),$$

where  $k$  is the maximum exponent of  $x_1$  in  $p(x_1, \dots, x_n)$ .

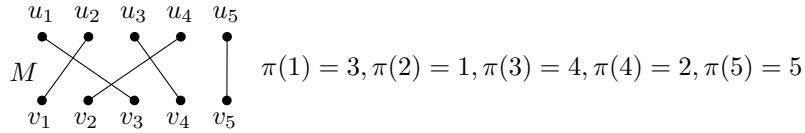
We divide the  $m$ -tuples  $(r_1, \dots, r_m)$  with  $p(r_1, \dots, r_m) = 0$  into two classes. The first class, called  $R_1$ , consists of the  $m$ -tuples with  $p_k(r_2, \dots, r_m) = 0$ . Since the polynomial  $p_k(x_2, \dots, x_m)$  is not identically zero and has degree at most  $d - k$ , the number of choices for  $(r_2, \dots, r_m)$  is at most  $(d - k)|S|^{m-2}$  by the induction hypothesis, and so  $|R_1| \leq (d - k)|S|^{m-1}$ .

The second class  $R_2$  are the remaining  $m$ -tuples, that is, those with  $p(r_1, r_2, \dots, r_m) = 0$  but  $p_k(r_2, \dots, r_m) \neq 0$ . Here we count as follows:  $r_2, \dots, r_m$  can be chosen in at most  $|S|^{m-1}$  ways, and if  $r_2, \dots, r_m$  are fixed with  $p_k(r_2, \dots, r_m) \neq 0$ , then  $r_1$  must be a root of the univariate polynomial  $q(x_1) = p(x_1, r_2, \dots, r_m)$ . This polynomial has degree (exactly)  $k$ , and hence it has at most  $k$  roots. Thus the number of  $m$ -tuples in the second class is at most  $k|S|^{m-1}$ , which gives  $d|S|^{m-1}$  altogether, finishing the induction step and the proof of the Schwartz–Zippel theorem.

**5.3.** Let us assume that  $G$  has a perfect matching and thus  $\det(A)$  is a nonzero polynomial of degree  $n$ . The Schwartz–Zippel theorem shows that if we calculate  $\det(A)$  for values of the variables  $x_{ij}$  chosen independently at random from  $S := \{1, 2, \dots, 2n\}$ , then the probability of getting 0 is at most  $\frac{1}{2}$ .

As usual, the probability of the failure can be reduced to  $2^{-k}$  by repeating the algorithm  $k$  times.

**6.1.** Let  $S_n$  denote the set of all permutations of the set  $\{1, 2, \dots, n\}$ . Every perfect matching  $M$  in  $G$  corresponds to a unique permutation  $\pi \in S_n$ , where  $\pi(i)$  is defined as the index  $j$  such that the edge  $\{u_i, v_j\}$  lies in  $M$ . Here is an example:

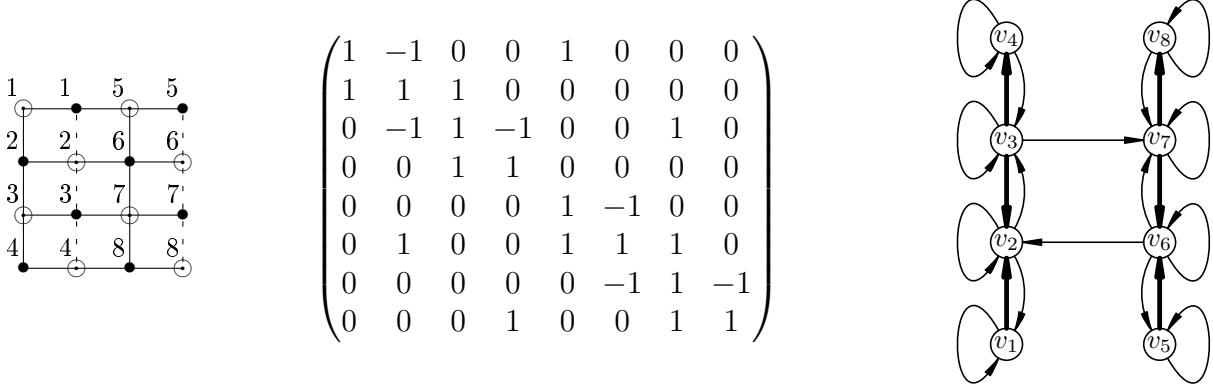


In the other direction, when does  $G$  have a perfect matching corresponding to a given permutation  $\pi \in S_n$ ? Exactly if  $b_{1,\pi(1)} = b_{2,\pi(2)} = \dots = b_{n,\pi(n)} = 1$ . Therefore, the number of perfect matchings in  $G$  equals

$$\sum_{\pi \in S_n} b_{1,\pi(1)} b_{2,\pi(2)} \cdots b_{n,\pi(n)},$$

and this is just the permanent of  $B$ .

**6.2.** Of course, the problem may be solved by calculation of the determinant, but not in our project! Number the vertices of the parts, write the bipartite adjacency matrix (black vertices correspond to the columns, white to the rows) and draw the graph, for which this matrix is the usual adjacency matrix:



The edges with weight  $-1$  are drawn by bold arrows. It remains to check that any even cycle of any univalent subgraph of this graph contains an odd number of negative edges (and here are no odd cycles except loops). For this graph, it is evident.

**6.3.** Let the signing  $\sigma$  as in the condition be fixed, and let  $M$  be a perfect matching in  $G$ , corresponding to a permutation  $\pi$ . We define the *sign* of  $M$  as the sign of the corresponding term in  $\det(B^\sigma)$ ; explicitly,

$$\text{sgn}(M) := \text{sgn}(\pi) b_{1,\pi(1)}^\sigma b_{2,\pi(2)}^\sigma \cdots b_{n,\pi(n)}^\sigma = \text{sgn}(\pi) \prod_{e \in M} \sigma(e).$$

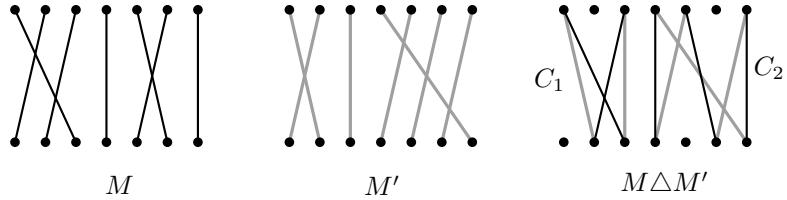
It is easy to see that  $\sigma$  is a Kasteleyn signing if (and only if) all perfect matchings in  $G$  have the same sign.

Let  $M$  and  $M'$  be two perfect matchings in  $G$ , with the corresponding permutations  $\pi$  and  $\pi'$ . Then

$$\begin{aligned} \text{sgn}(M)\text{sgn}(M') &= \text{sgn}(\pi)\text{sgn}(\pi') \left( \prod_{e \in M} \sigma(e) \right) \left( \prod_{e \in M'} \sigma(e) \right) \\ &= \text{sgn}(\pi)\text{sgn}(\pi') \prod_{e \in M \Delta M'} \sigma(e), \end{aligned}$$

where  $\Delta$  denotes the symmetric difference.

The symmetric difference  $M \Delta M'$  is a disjoint union of evenly placed cycles, as the picture below illustrates.

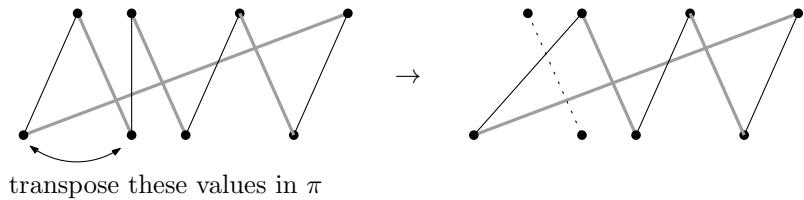


Let these cycles be  $C_1, C_2, \dots, C_k$ , and let the length of  $C_i$  be  $2\ell_i$ . Since  $C_i$  is evenly placed, it must be properly signed by the assumption in the lemma, and so we have  $\prod_{e \in C_i} \sigma(e) = (-1)^{\ell_i - 1}$ .

Thus  $\prod_{e \in M \triangle M'} \sigma(e) = (-1)^t$  with  $t := \ell_1 - 1 + \ell_2 - 1 + \dots + \ell_k - 1$ .

It remains to check that  $\pi$  can be converted to  $\pi'$  by  $t$  transpositions (then, by the properties of the sign of a permutation, we have  $\text{sgn}(\pi) = (-1)^t \text{sgn}(\pi')$ , and thus  $\text{sgn}(M) = \text{sgn}(M')$  as needed).

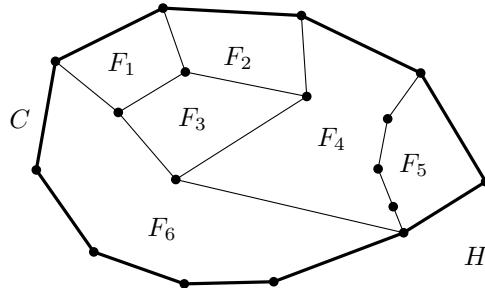
This can be done for one cycle  $C_i$  at a time. As the next picture illustrates for a cycle of length  $2\ell_i = 8$ , by modifying  $\pi$  with a suitable transposition we can “cancel” two edges of the cycle and pass to a cycle of length  $2\ell_i - 2$  (black edges belong to  $M$ , gray edges to  $M'$ , and the dotted edge in the right drawing now belongs to both  $M$  and  $M'$ ).



Continuing in this way for  $\ell_i - 1$  steps, we cancel  $C_i$ , and we can proceed with the next cycle.

**6.4.** Let  $C$  be an evenly placed cycle in  $G$ ; we need to prove that it is properly signed.

Let the length of  $C$  be  $2\ell$ . Let  $F_1, \dots, F_k$  be the inner faces enclosed in  $C$  in the drawing, and let  $C_i$  be the boundary cycle of  $F_i$ , of length  $2\ell_i$ . Let  $H$  be the subgraph of  $G$  obtained by deleting all vertices and edges drawn outside  $C$ ; in other words,  $H$  is the union of the  $C_i$ .



We want to see how the parity of  $\ell$  is related to the parities of the  $\ell_i$ . The number of vertices of  $H$  is  $r + 2\ell$ , where  $r$  is the number of vertices lying in the interior of  $C$ . Every edge of  $H$  belongs to exactly two cycles among  $C, C_1, \dots, C_k$ , and so the number of edges of  $H$  equals  $\ell + \ell_1 + \dots + \ell_k$ . Finally, the drawing of  $H$  has  $k + 1$  faces:  $F_1, \dots, F_k$  and the outer one.

Now we apply *Euler's formula*, which tells us that for every drawing of a connected planar graph, the number of vertices plus the number of faces equals the number of edges plus 2. Thus

$$r + 2\ell + k + 1 = \ell + \ell_1 + \dots + \ell_k + 2. \quad (12)$$

Next, we use the assumption that  $C$  is evenly placed. Since the graph obtained by deleting  $C$  from  $G$  has a perfect matching, the number  $r$  of vertices inside  $C$  must be even. Therefore, from (12) we get

$$\ell - 1 \equiv \ell_1 + \dots + \ell_k - k \pmod{2}. \quad (13)$$

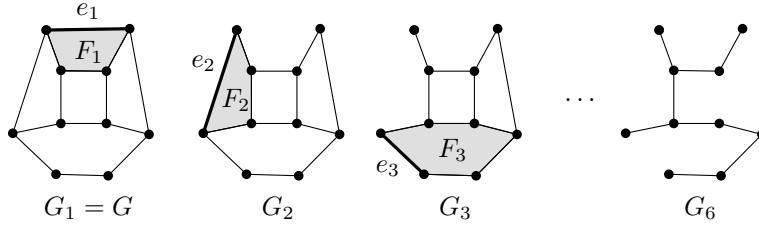
Let  $n_C$  be the number of negative edges in  $C$ , and similarly for  $n_{C_i}$ . The sum  $n_C + n_{C_1} + \dots + n_{C_k}$  is even because it counts every negative edge twice, and so

$$n_C \equiv n_{C_1} + \dots + n_{C_k} \pmod{2}. \quad (14)$$

Finally, we have  $n_{C_i} \equiv \ell_i - 1 \pmod{2}$  since the  $C_i$  are properly signed. Combining this with (13) and (14) gives  $n_C \equiv \ell - 1 \pmod{2}$ . Hence  $C$  is properly signed. Now the result follows from the result of 6.3.

**6.5.** Given a connected, 2-connected, planar, bipartite  $G$ , we fix some planar drawing, and we want to construct a signing as in Lemma B, with the boundary of every inner face properly signed.

First we start deleting edges from  $G$ , as the following picture illustrates.



We set  $G_1 := G$ , and  $G_{i+1}$  is obtained from  $G_i$  by deleting an edge  $e_i$  that separates an inner face  $F_i$  from the outer (unbounded) face (in the current drawing). The procedure finishes with some  $G_k$  that has no such edge. Then the drawing of  $G_k$  has only the outer face.

Now we choose the signs of the edges of  $G_k$  arbitrarily, and we extend this to a signing of  $G$  by going backward, choosing the signs for  $e_{k-1}, e_{k-2}, \dots, e_1$  in this order. When we consider  $e_i$ , it is contained in the boundary of the single inner face  $F_i$  in the drawing of  $G_i$ , so we can set  $\sigma(e_i)$  so that the boundary of  $F_i$  is properly signed. The assertion is proved.

**6.6.** We took this problem from [7].

a) The statement is evident. Choosing a permutation  $\pi$ , we define for each inlet  $i$  the outlet  $\pi(i)$  where the route should go, and the number of ways to choose a route equals  $a_{i\pi_i}$ . Then the product  $a_{1\pi_1}a_{2\pi_2}\dots a_{n\pi_n}$  is equal to the number of ways to choose a set of routes. Summing over all  $\pi$ , we obtain the total number of sets.

b) As in the reasoning from part a), the product  $a_{1\pi_1}a_{2\pi_2}\dots a_{n\pi_n}$  is equal to the number of ways to choose a set of routes. The sets of non-intersecting routes are taken into account only in the product defined by identity permutation. In the sum defining the determinant, this product has sign plus. It remains to check that the sets of intersecting routes one can split into pairs counted with different signs, then all of them will be cancelled in this sum.

Enumerate each path by the number of the inlet where this path begins. For each set of  $n$  non-intersecting paths defined by permutation  $\pi$ , define by  $i$  the least of the numbers of paths which intersect with other paths. Denote by  $O$  the first point of intersection of  $i$ th path with some other path, let it be  $j$ th path.

Interchange the fragments of  $i$ th and  $j$ th paths after point  $O$ , the obtained set of paths will form a pair with the considered set. The permutation that describes the obtained set, differs from the initial by the transposition  $(\pi_i, \pi_j)$  and therefore has the opposite sign.

In this reasoning we did not use that the graph is planar. It was essential for us only that this graph is nonpermutable, i.e. in the set of  $n$  non-intersecting paths the number of the outlet is equal to the number of the inlet for each path.

**6.7. a)** We have taken this problem from [3]. Let  $A_{mn}$  be the number of paths of lame king from a corner of  $m \times n$  rectangle to the opposite corner. Then

$$A_{n-1,n-1} = 2A_{n-2,n-1} + A_{n-2,n-2}$$

(to ensure this, consider three possibilities of the first king's move). Similarly,

$$B_n = A_{n-2,n-2} + A_{n-1,n-1} + 2A_{n-1,n-2}$$

(consider four possible combinations of the first and the last moves). Substituting the first equality into the second one, we obtain the required.

We will present an argument which gives the bijective proof of the required equality, related to the formal proof written above.

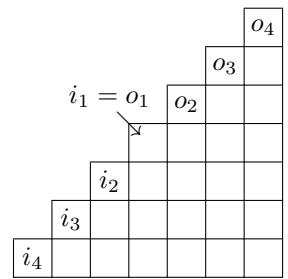
Value  $B_n$  is the number of paths leading from square  $a$  to square  $b$  of an  $n \times n$  board and not passing through the squares marked with asterisk and through square  $c$ . Value  $2A_{n-1}$  is the number of paths leading from square  $p$  to square  $e$  plus the number of paths leading from square  $q$  to square  $b$ . One-to-one correspondence between the sets of such paths is constructed as follows.

Consider an arbitrary path of lame king from  $p$  to  $e$ . Supplementing this path with steps  $a-p$  and  $e-b$  we obtain a path from  $a$  to  $b$  not passing through forbidden squares. The first step in the obtained path is horizontal, the last is vertical. Now consider an arbitrary path of lame king from  $q$  to  $b$ . If it does not pass through square  $c$ , then supplement it with step  $a-q$ . We obtain a path from  $a$  to  $b$  not passing through forbidden squares, in which the first step is diagonal, the last is diagonal or vertical. And in the case when this path passes through square  $c$ , remove step  $c-b$  from it, shift the obtained path  $q-c$  one square downward (we will obtain a path from  $p$  to  $d$ ), and complete this path by steps  $a-p$ ,  $d-b$  to obtain a path from  $a$  to  $b$ . In the resulting path the first step is horizontal, and the last is diagonal. It is evident that the constructed correspondence is one-to-one.

b) We have taken this statement in [4, lemma 5.1]. Consider matrix  $B^{(n)} = (B_{i,j})_{1 \leq i,j \leq n}$ , where  $B_{i,j}$  is the number of routes of lame king on  $i \times j$  board leading from the lower left corner to the upper right corner and not containing any cells of the left vertical and upper horizontal lines (except the initial and final positions). Similarly to the statement of the previous item it is proven that  $B^{(n)} = 2A^{(n)}$ . By the statement of problem 6.6, determinants  $\det A^{(n)}$  and  $\det B^{(n)}$  count the same number of the sets of routes. Thus,  $\det A^{(n)} = 2^n \det A^{(n-1)}$ , whence  $\det A^{(n)} = 2^{n(n+1)/2}$ .

x	x	x	x	x	c	b
x					d	e
x						
x						
x						
x	q					
a	p					

**6.8.** Answer: 1. We have taken this problem in [7]. Consider inlets and outlets shown in the figure. The numbers of paths from inlets to outlets are just Catalan numbers. Then  $\det H$  counts the number of the sets of non-intersecting routes from inlets to outlets. It is evident that such set of routes is unique.



**7.1.** Express  $\det A_G$  through univalent graphs by the combinatorial definition. Since  $G$  does not contain cycles, a univalent graph occurs with nonzero weight only if all the cycles in it have length 2, and this corresponds to perfect matching of  $G$ . The required result follows from the fact that a tree has not more than one perfect matching.

**7.2.** Express  $\det A_G$  through univalent graphs by the combinatorial definition. Since  $G$  does not contain cycles, a univalent graph occurs with nonzero weight only if there exist no cycles of length 3 or more. Then univalent graphs, consisting of  $k$  multiple edges and  $n - 2k$  loops, occur with weight  $(-1)^k x^{n-2k}$ . Now one can see that polynomials  $\chi G(x)$  and  $m_G(x)$  count the same combinatorial objects with the corresponding weights, so these polynomials coincide.

## Список литературы

- [1] V. Aksenov, K. Kokhas. Domino Tilings and Determinants // Journal of Mathematical Sciences. 2014. Vol. 200. P. 647–653.
- [2] V. Aksenov, K. Kokhas. Chip Removal. Urban Renewal Revisited // Journal of Mathematical Sciences. 2015. Vol. 209. P. 809–825.
- [3] Ivanov S. V., Kokhas K. P., Khrabrov A. St. Petersburg mathematical olympiads. Problem 05.58 (in Russian). St Petersburg: Nevsky Dialekt. 2007.
- [4] Kokhas K.P. Domino tilings of Aztec diamonds and squares // Journal of Mathematical Sciences. 2009. Vol. 158. P. 868–894.
- [5] Kokhas K. P. Domino dissections (in Russian)// Matematicheskoye prosvetshcheniye. Ser. 3. Iss. 9. 2005. P. 143–163.

- [6] *Kokhas K. P.* Sharing money in a secret society. In: *Berlov S.L., Petrov F.V., Smirnov A.V. e.a.* Problems of St. Petersburg mathematical olympiad for school students (in Russian). St. Petersburg: Nevsky dialekt; BHV-Peterburg. 2011. P. 81–103.
- [7] *Benjamin A. T., Cameron N. T.* Counting on determinants // American Mathematical Monthly. 2005. Vol. 112. № 6. P. 481–492.
- [8] *Brualdi R.A., Cvetković D.* A combinatorial approach to matrix theory and its applications. Taylor & Francis Group. 2009. P. 63–96.
- [9] *Matoušek J.* Thirty-three Miniatures. Mathematical and Algorithmic Applications of Linear Algebra. Providence: AMS. 2010. P. 77–83, 107–111.

# К многомерной комбинаторной геометрии\*

представляют Е. Коган, В. Ретинский, Е. Рябов<sup>†</sup> и А. Скопенков<sup>‡</sup>

## Введение

Многие области знания и техники — прежде всего математика, программирование и физика — часто работают с многомерным пространством. Решение нижеприведенных задач позволит освоить базовые навыки такой работы. Вы научитесь как развивать пространственное воображение и интуицию, так и проверять их строгими рассуждениями. Это полезно для последующего изучения компьютерной графики и необходимой для нее базы из линейной алгебры и геометрии.

Основные идеи представлены на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей, и со сведением научного языка к необходимому минимуму (см. задачи). За счет этого проект доступен для начинающих, хотя содержит красивые сложные результаты. Для изучения проекта не требуется предварительных знаний по стереометрии. Полезны пространственное воображение и умение решать системы линейных уравнений (см. задача 1.2).

В этом проекте мы обобщаем следующий результат (см. задачи S, D, SD и §3, а также §4 и §5).

**Теорема Радона для плоскости.** *Для любых 4 точек на плоскости либо одна из них лежит внутри треугольника, образованного оставшимися точками, либо их можно разбить на две пары так, что отрезок, соединяющий точки в первой паре, пересекает отрезок, соединяющий точки во второй паре.*

**S = same size.** Из любых 5 точек плоскости можно выбрать такие две непересекающиеся пары точек, что отрезки, образованные этими парами, пересекаются.

В этом тексте под треугольником  $\Delta$  подразумевается часть плоскости, ограниченная его контуром  $\partial\Delta$  (т.е. объединением сторон). Эта часть может быть отрезком.

**D = dimension.** Для любых 5 точек в пространстве либо одна из них лежит внутри тетраэдра, образованного оставшимися точками, либо их можно разбить на пару и тройку так, что отрезок, соединяющий точки в паре, пересекает треугольник, образованный точками в тройке.

В этом тексте интересные нетривиальные задачи называются теоремами.

**Теорема SD:** теорема Радона для пространства о множествах почти одинакового размера.

(3) *Из любых 6 точек пространства можно выбрать такие непересекающиеся пару и тройку точек, что отрезок, соединяющий точки пары, пересекает треугольник, образованный тройкой.*

---

\*Благодарим Д. Елисеева за перевод части текста и А. Рябичева за полезные замечания.

<sup>†</sup>Е. Коган, В. Ретинский, Е. Рябов — Высшая Школа Экономики, Москва.

<sup>‡</sup><https://users.mccme.ru/skopenko>. Московский Физико-Технический Институт, Независимый Московский Университет.

(4) Из любых 7 точек четырехмерного пространства можно выбрать две непересекающиеся тройки точек, для которых соответствующие треугольники пересекаются.

Определение четырехмерного пространства и обозначения, необходимые для доказательств, приведены в §1 и в §2. Для доказательства теоремы SD.4 вам понадобится теорема S'D, приведенная ниже.

Пусть  $\Delta$  и  $\Delta'$  — два невырожденных треугольника в пространстве, контуры которых не пересекаются, и никакие четыре из вершин которых не лежат в одной плоскости. Треугольники называются **зацепленными**, если контур первого пересекает второй ровно в одной точке.

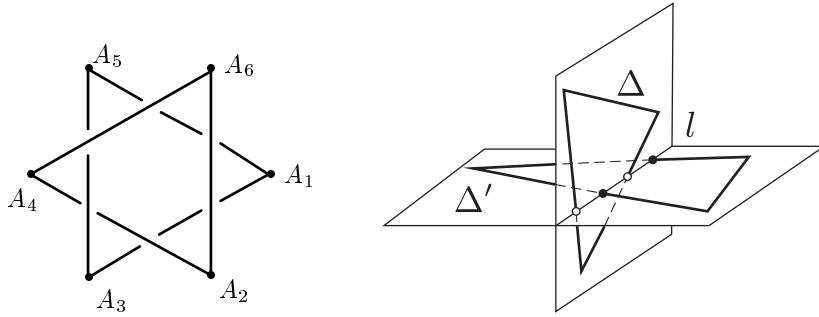


Рис. 1: Зацепленные треугольники и зацепленные пары точек

**Теорема S'D:** теорема Радона для пространства о зацепленности множеств одинакового размера; линейная теорема Конвея-Гордона-Закса, 1981-1983.

Если среди 6 точек пространства никакие 4 не лежат в одной плоскости, то существуют два зацепленных треугольника с вершинами в этих точках.

Для доказательства вам понадобится утверждение QS из §3.

Другие «олимпиадные» задачи — теорема D(d) в §1, 2.3.c, 2.5.b, 2.7.b, 3.2, 3.6.(4'-3). Нерешенные задачи — 3.6.(4-3),(4-2),(4'-2) и в §4, §5.

После ЛКТГ можете порешать §4 и §5. В §5 есть простое доказательство импликации  $DMT \Rightarrow SDMT$  (со сменой параметра), которое является одним из шагов в недавнем построении контрпримера к топологической гипотезе Тверберга [Sk16].

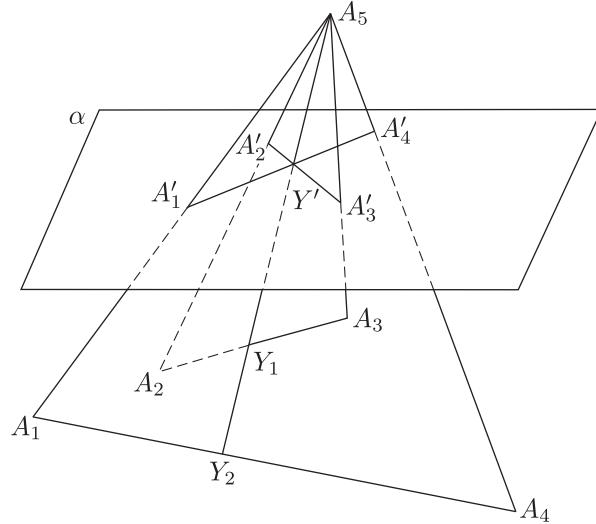


Рис. 2: Указание к задаче D (к теореме Радона для пространства)

## Рекомендации участникам.

Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. Если задача выделена словом «теорема» («лемма», «следствие» и т. д.), то её утверждение более важное. Как правило, мы приводим (в виде задачи) *формулировку* красивого или важного утверждения *перед* его *доказательством*. В таких случаях для доказательства утверждения могут потребоваться следующие задачи. Мы не лишаем Вас удовольствия самостоятельно найти момент, когда Вы наконец-то сможете доказать такое утверждение. Вообще, если Вы застряли на какой-то задаче, попробуйте перейти к следующим, они могут оказаться полезными. *Замечания* и задачи, помеченные звездочками, формально не используются в дальнейшем. В тексте определения важных понятий помечены **жирным шрифтом**, чтобы затем было проще их найти.

Участник (или команда), решавший задачи проекта, получает «боб» за каждое **письменное решение для пользователя** (не являющееся просто ответом), оцененное в «+» или «+.». См. рекомендации <https://www.mccme.ru/circles/oim/home/pism.pdf>. Дополнительные бобы могут выдаваться за красивые решения, решения сложных задач или оформление некоторых решений в системе ТЕХ. У жюри бесконечно много бобов. У каждой участника (или команды) в начале 1 боб. Решения можно сдавать и **устно, и письменно для разработчика**, отдавая один боб за каждые пять попыток (неважно, удачных или нет).

Участники (или команды) сдают решения личным сообщением Егору Рябову через <https://mattermost.turgor.ru>. Направляйте ему же вопросы и просьбы о подсказке по задачам, которые у Вас долго не получаются. (Мы сами распределим между собой проверку решений и ответы на вопросы.) Те, кто успешно работают над проектом, завоюют право получить интересные *дополнительные задачи для исследования*.

Пожалуйста, сообщите нам, если Вы знаете решения каких-то из предложенных задач. (E.g. or if you attended courses by A. Skopenkov on a similar subject.) Это не противоречит Вашему участию в проекте, но это и не обязывает Вас решать этот проект. После проверки у Вас некоторых из задач, названных Вами решенными заранее (Аркадием Скопенковым, [skopenko@mccme.ru](mailto:skopenko@mccme.ru)), Вы сможете пользоваться результатами всех этих задач. При этом решения этих задач не будут считаться Вашим достижением на ЛКТГ. Зато у Вас появится возможность дойти до более сложных задач. Мы будем рады их выдать, они уже готовы!

# 1 Как работать с четырехмерным пространством?

В задачах 1.1, 1.4.abc, 1.5.abcd, 1.8.cd и 1.9.be достаточно привести правильный ответ. (Задача 1.8.a разобрана.)

**1.1.** Сколько точек может быть в пересечении прямой и плоскости в трехмерном пространстве?

**1.2.** Сколько решений может быть у системы линейных уравнений

- (a)  $2 \times 2$ ; (b)  $2 \times 3$  (2 уравнения, 3 переменных); (c)  $3 \times 2$ ?

Определим

- *прямую* как множество действительных чисел;

• *плоскость*  $\mathbb{R}^2$  как множество всех упорядоченных пар  $(x, y)$  действительных чисел  $x$  и  $y$ ;

• *трехмерное пространство*  $\mathbb{R}^3$  как множество всех упорядоченных троек  $(x, y, z)$  действительных чисел;

- четырехмерное пространство  $\mathbb{R}^4$  как множество всех упорядоченных четверок  $(x, y, z, t)$  действительных чисел.

Определение  $d$ -мерного пространства  $\mathbb{R}^d$  для  $d > 4$  дается аналогично.

В этом тексте «трехмерное пространство  $\mathbb{R}^3$ » коротко называется «пространством».

Для точек  $A = (x_1, y_1, z_1, t_1), B = (x_2, y_2, z_2, t_2) \in \mathbb{R}^4$  и числа  $\lambda \in \mathbb{R}$  обозначим

$$\lambda A := (\lambda x_1, \lambda y_1, \lambda z_1, \lambda t_1) \quad \text{и} \quad A + B := (x_1 + x_2, y_1 + y_2, z_1 + z_2, t_1 + t_2).$$

**1.3.** Разбивает ли двумерная плоскость четырехмерное пространство на куски? Т.е. для любых ли двух точек, не лежащих в двумерной плоскости  $x = y = 0$  четырехмерного пространства  $(x, y, z, t)$ , существует ломаная, соединяющая эти точки и не пересекающая плоскость?

Для точек  $A, B \in \mathbb{R}^4$  отрезком  $AB$  называется множество  $\{\lambda A + (1-\lambda)B : \lambda \in [0, 1]\}$ . Ломаной  $A_1 A_2 \dots A_n$  называется объединение отрезков  $A_i A_{i+1}$  по всем  $i = 1, 2, \dots, n-1$ .

*Указание.* Для точек  $A = (x_0, y_0, z_0, t_0)$  и  $B$ , не лежащих на плоскости  $x = y = 0$ , определим точки

$$A_x = A + (1, 0, 0, 0) = (x_0 + 1, y_0, z_0, t_0) \quad \text{и} \quad A_y = A + (0, 1, 0, 0) = (x_0, y_0 + 1, z_0, t_0).$$

Докажите, что хотя бы одна из ломаных  $AB$ ,  $AA_x B$  и  $AA_y B$  не пересекает плоскость  $x = y = 0$ .

**1.4.** Чем является пересечение *двумерной сферы*

$$S^2 := \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$$

со следующими множествами:

- прямая  $x = y = 0$ , содержащая центр сферы;
- плоскость  $x = 0$ , содержащая центр сферы;
- пересечение положительного октанта в  $\mathbb{R}^3$  и объединения двумерных координатных плоскостей, то есть множество

$$\{(x, y, z) \in \mathbb{R}^3 : x \geq 0, y \geq 0, z \geq 0 \text{ и } xyz = 0\}.$$

**1.5.** Чем является пересечение *трехмерной сферы*

$$S^3 := \{(x, y, z, t) \in \mathbb{R}^4 : x^2 + y^2 + z^2 + t^2 = 1\}$$

со следующими множествами:

- прямая  $x = y = z = 0$ , содержащая центр сферы;
- плоскость  $x = y = 0$ , содержащая центр сферы;
- (трехмерная) гиперплоскость  $x = 0$ , содержащая центр сферы;
- пересечение положительной «одной шестнадцатой»  $\mathbb{R}^4$  и объединения двумерных координатных плоскостей, то есть множество

$$\{(x, y, z, t) \in \mathbb{R}^4 :$$

$: x \geq 0, y \geq 0, z \geq 0, t \geq 0$  и хотя бы два из четырех чисел  $x, y, z, t$  равны нулю}.

Подмножество  $L \subset \mathbb{R}^4$  называется **прямой**, если  $L$  не является точкой и найдутся точки  $A, B \in \mathbb{R}^4$ , для которых  $L = \{A + Bt : t \in \mathbb{R}\}$ .

Подмножество  $L \subset \mathbb{R}^4$  называется (двумерной) **плоскостью**, если  $L$  не является ни точкой, ни прямой, и найдутся точки  $A, B, C \in \mathbb{R}^4$ , для которых  $L = \{A + Bt + Cu : t, u \in \mathbb{R}\}$ .

Ранее уже было введено определение прямой. Однако далее под прямой подразумевается другое — подмножество в  $\mathbb{R}^d$ , определение которого аналогично вышеприведенному. Аналогичное замечание справедливо и для плоскости.

**1.6.** Напишите аналогичное определение (трехмерной) **гиперплоскости** в  $\mathbb{R}^4$ .

В решениях следующих задач о четырехмерном пространстве вы можете использовать без доказательств

- все строго сформулированные Вами верные факты о решениях систем линейных уравнений;

- результаты задачи 1.7.

**1.7. \*** (a) Подмножество  $L \subset \mathbb{R}^4$  является гиперплоскостью тогда и только тогда, когда  $L \neq \emptyset, L \neq \mathbb{R}^4$  и существуют  $a, b, c, d, e \in \mathbb{R}$ , такие что

$$L = \{(x, y, z, t) \in \mathbb{R}^4 : ax + by + cz + dt = e\}.$$

(b) Подмножество  $L \subset \mathbb{R}^4$  является плоскостью тогда и только тогда, когда  $L \neq \emptyset, L \neq \mathbb{R}^4, L$  не является гиперплоскостью и существуют  $a_1, b_1, c_1, d_1, e_1, a_2, b_2, c_2, d_2, e_2 \in \mathbb{R}$ , для которых

$$L = \{(x, y, z, t) \in \mathbb{R}^4 : a_1x + b_1y + c_1z + d_1t = e_1, a_2x + b_2y + c_2z + d_2t = e_2\}.$$

(c) Сформулируйте и докажите аналогичное утверждение для прямой в  $\mathbb{R}^4$ .

**1.8.** Чем может быть пересечение в  $\mathbb{R}^4$ :

- (a) прямой и гиперплоскости?    (b) прямой и плоскости?
- (c) плоскости и гиперплоскости?    (d) двух гиперплоскостей?    (e) двух плоскостей?

*Подсказка к (a).* Ответ. Пустое множество, точка, прямая.

*Примеры.* Прямая  $x = y = z = 0$  пересекается с гиперплоскостью  $x = 1$  по пустому множеству. Прямая  $x = y = z = 0$  пересекается с гиперплоскостью  $t = 0$  по точке. Прямая  $x = y = z = 0$  пересекается с гиперплоскостью  $x = 0$  по прямой.

*Доказательство того, что другие пересечения невозможны.* Достаточно доказать, что если пересечение в  $\mathbb{R}^4$  прямой  $l$  и гиперплоскости содержит хотя бы две точки, то пересечение совпадает с прямой  $l$ . Это верно, так как *для любых двух точек существует единственная прямая, содержащая обе эти точки*. Последний факт легко выводится из определения прямой. (Во многих других изложениях этот факт принимается за аксиому.)

**1.9.** Для различных точек  $X, Y \in \mathbb{R}^4$  определим *прямую*  $XY$  как  $\{X + (Y - X)t = (1-t)X + tY : t \in \mathbb{R}\}$ . Для точек  $X, Y, Z \in \mathbb{R}^4$ , не лежащих на одной прямой, определим *плоскость*  $XYZ$  как

$$\{X + (Y - X)t + (Z - X)u = (1 - t - u)X + tY + uZ : t, u \in \mathbb{R}\}.$$

Никакие пять из восьми точек 1,2,3,4,5,6,7,8 в  $\mathbb{R}^4$  не лежат на одной гиперплоскости. Чем может быть пересечение:

- (b) прямой 12 и плоскости 567?    (d) гиперплоскостей 1234 и 5678?
- (e) плоскостей 123 и 567?

**Выпуклой оболочкой** конечного набора точек  $A_1, \dots, A_n \in \mathbb{R}^d$  называется множество

$$\langle A_1, \dots, A_n \rangle := \{\lambda_1 A_1 + \dots + \lambda_n A_n : \lambda_1, \dots, \lambda_n \geq 0, \lambda_1 + \dots + \lambda_n = 1\}.$$

**1.10.** Выпуклая оболочка конечного набора точек на плоскости — наименьший (по включению, или по площади) выпуклый многоугольник, их содержащий.

**Теорема D(d):** теорема Радона.

*Любые  $d+2$  точки  $d$ -мерного пространства можно разбить на два множества, выпуклые оболочки которых пересекаются.*

**Напутствие.** Обычно только простейшие свойства в планиметрии и стереометрии выводятся из аналитических определений (или же принимаются за аксиомы). Более сложные свойства могут быть выведены из простейших «синтетически» (т.е., как в школьной геометрии, без использования аналитических определений). Часто бывает удобно свести двумерную задачу к одномерной (т.е., к задаче на прямой), а трехмерную задачу — к двумерной. Аналогично, лучший подход к следующим четырехмерным задачам — это аналогия с трехмерными задачами, или сведение к ним.

## 2 Леммы о четности

**Лемма 2.1** (о четности). *Если из 6 вершин двух треугольников на плоскости никакие 3 не лежат на прямой, то контуры этих треугольников пересекаются в четном числе точек.*

*Доказательство.* Контур треугольника разбивает плоскость.<sup>1</sup> Ломаная, составленная из сторон одного треугольника заходит внутрь другого треугольника столько же раз, сколько выходит наружу.  $\square$

Несколько точек плоскости **находятся в общем положении**, если никакие три из них не лежат на прямой и никакие три отрезка, их соединяющие, не имеют общей внутренней точки.

**2.2.** (а) Находятся ли все точки окружности в общем положении?

(б) Если вершины двух плоских ломаных находятся в общем положении, то ломаные пересекаются в конечном числе точек.

*Указание:*  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ .

**2.3.** (а) Плоскость нельзя представить в виде объединения конечного числа прямых.

(б) Существуют ли 100 точек общего положения на плоскости?

(с) На плоскости имеется 14 точек общего положения: 7 красных и 7 желтых. Тогда количество всех точек пересечения красных отрезков (т.е. отрезков, соединяющих красные точки) с желтыми отрезками четно.

**Лемма 2.4** (о четности). *Если никакие 4 из 7 вершин треугольника и тетраэдра в пространстве не лежат на одной плоскости, то контур треугольника пересекается с гранями тетраэдра в четном числе точек.*

Несколько точек в пространстве **находятся в общем положении**, если никакие 4 из них не лежат на одной плоскости, и никакие отрезок, треугольник и треугольник, натянутые на них, не имеют общей внутренней точки. Пример шести точек общего положения изображен на рис. 3.

---

<sup>1</sup>Этот факт, в отличие от *кусочно-линейной теоремы Жордана* [Sk20, §1.4], доказывается без использования леммы о четности.

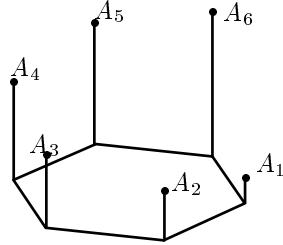


Рис. 3: Шесть точек общего положения в пространстве

**2.5.** (а) Существуют ли 100 точек общего положения в пространстве?

(б) В пространстве имеется 17 точек общего положения: 7 красных и 10 желтых. Тогда количество всех точек пересечения красных отрезков (т.е. отрезков, соединяющих красные точки) с желтыми треугольниками четно.

**Лемма 2.6** (о четности). *Если никакие 5 из 8 вершин двух тетраэдров в четырехмерном пространстве не лежат на одной гиперплоскости, тогда поверхности этих тетраэдров пересекаются в четном числе внутренних точек.*

*Указание:* возьмите сечение гиперплоскостью одного из тетраэдров.

Несколько точек в четырехмерном пространстве **находятся в общем положении**, если никакие 5 из них не лежат на одной гиперплоскости, и никакие три треугольника, натянутые на них, не имеют общей внутренней точки.

**2.7.** (а) Существуют ли 100 точек общего положения в четырехмерном пространстве?

(б) В четырехмерном пространстве имеется 16 точек общего положения: 8 красных и 8 желтых. Назовем *красными/желтыми* двумерные треугольники, натянутые на красные/желтые точки. Тогда количество точек пересечения красных треугольников с желтыми треугольниками четно.

### 3 Количествоенные версии

**Q = quantitative.** Если никакие 3 из 4 точек плоскости не лежат на прямой, то существует ровно одно их разбиение на два множества из теоремы Радона для плоскости.

**QS:** количественная теорема Радона для плоскости о множествах одинакового размера; линейная теорема ван Кампена-Флореса для плоскости.

Если среди 5 точек плоскости никакие 3 не лежат на прямой, то количество точек пересечения внутренностей отрезков, соединяющих данные точки, нечетно.

**QD:** количественная теорема Радона для пространства.

(3) Если никакие 4 из 5 точек пространства не лежат в одной плоскости, то существует ровно одно их разбиение на два множества, выпуклые оболочки которых пересекаются.

(4) Сформулируйте и докажите четырехмерный и  $d$ -мерный аналог.

**Теорема QSD:** количественная теорема Радона для пространства о множествах почти одинакового размера.

(3) *Если среди 6 точек пространства никакие 4 не лежат в одной плоскости, то количество точек пересечения внутренностей отрезков, соединяющих данные точки, с (двумерными) треугольниками, натянутыми на данные точки, четно.*

(4) Если среди 7 точек четырехмерного пространства никакие 5 не лежат в одной гиперплоскости, то количество точек пересечения (двумерных) треугольников, натянутых на данные точки, нечетно.

Для теоремы QSD.4 вам понадобится теорема QS'D ниже.

Свойство быть зацепленными не симметрично априори.

**Лемма 3.1** (о симметрии). *Треугольники  $\Delta$  и  $\Delta'$  в пространстве зацеплены тогда и только тогда, когда  $\Delta'$  и  $\Delta$  зацеплены.*

**3.2.** В пространстве имеется 13 точек: 3 красных и 10 желтых. Никакие четыре из них не лежат в одной плоскости. Докажите, что количество желтых треугольников, зацепленных с красным треугольником, четно. *Красным (желтым) треугольником* называется любой треугольник с красными (желтыми) вершинами. Треугольники, отличающиеся перестановкой вершин, считаются одинаковыми.

**3.3.** В пространстве отрезок  $p$  находится под отрезком  $q$  (при взгляде из точки  $O$ ), если существует луч  $OX$  с концом  $O$ , пересекающая отрезок  $p$  в точке  $P := p \cap OX$ , а отрезок  $q$  в точке  $Q := q \cap OX$ ,  $P \neq Q$ , так, что  $Q$  лежит внутри отрезка  $OP$ .

Пусть никакие четыре из точек  $O, A_1, \dots, A_5$  в пространстве не лежат в одной плоскости, и существует плоскость, отделяющая  $O$  от  $A_1, \dots, A_5$ . Тогда треугольники  $OA_1A_2$  и  $A_3A_4A_5$  зацеплены тогда и только тогда, когда  $A_1A_2$  расположен под нечетным числом сторон треугольника  $A_3A_4A_5$ .

**Теорема QS'D:** количественная теорема Радона для пространства о зацепленности множеств одинакового размера.

*Если среди 6 точек пространства никакие 4 не лежат в одной плоскости, то количество неупорядоченных пар зацепленных треугольников с вершинами в этих точках нечетно.*

Теоремы SD и QSD показывают, что при переходе от размерности 2 к размерности 3 свойство существования пересечения сохраняется, в то же время четность числа пересечений изменяется. Нечетномерные аналоги SD и QSD имеют более сильную форму: теоремы S'D и QS'D.

Следующие свойства расцепленности связаны со свойствами пересечений QS, QSD.

**3.4. (2)** Существуют 5 точек плоскости, никакие 3 из которых не лежат на одной прямой и такие, что любой отрезок, соединяющий 2 из них, пересекает контур треугольника, образованного остальными 3-мя, в четном числе точек.

(2') Для любых 5 точек плоскости, никакие 3 из которых не лежат на одной прямой, число отрезков, соединяющих 2 из них, и пересекающих контур треугольника, образованного остальными 3-мя, ровно в одной точке, четно.

Задача 3.4 означает, что каждая пара точек «расцеплена» (т.е., не «зацеплена») с треугольником, образованном остальными 3-мя. Мы не будем приводить аналогичные пояснения для свойств 3.5.3, 3.6.(4-2),(4-3) ниже.

В пространстве вместо свойства расцепленности 3.4 есть свойство зацепленности (теорема QS'D) и следующие свойства расцепленности.

**3.5. (3)** Существуют 6 точек в пространстве, никакие 4 из которых не лежат в одной плоскости и такие, что любой отрезок, соединяющий 2 из них, пересекает поверхность тетраэдра, образованного оставшимися 4-мя точками, в четном числе точек.

(3') Если никакие 4 из 6 точек пространства не лежат в одной плоскости, то количество точек пересечения отрезков, их соединяющих, с поверхностями тетраэдров, образованных оставшимися 4-мя точками, четно.

Здесь можно сделать замечание, аналогичное замечанию после теоремы QSD.

Было бы интересно доказать утверждение 3.6.(4'-3), гипотезы 3.6.(4-3),(4'-2),(4-2) и их аналоги в больших размерностях. (Мы благодарны М. Танцеру за присланное нам доказательство PL версии утверждения 3.6.(4-3).)

**3.6. (4'-3)** Если никакие 5 из 7 точек в четырехмерном пространстве не лежат в одной гиперплоскости, то количество треугольников, образованных 3-мя из них, и пересекающих тетраэдр, образованный оставшимися 4-мя точками, ровно в одной точке, четно.

(4-3) Существуют 7 точек в четырехмерном пространстве, никакие 5 из которых не лежат в одной гиперплоскости и такие, что любой треугольник, образованный 3-мя из них, пересекает поверхность тетраэдра, образованного оставшимися 4-мя точками, в четном числе точек.

(4'-2) Если никакие 5 из 7 точек в четырехмерном пространстве не лежат в одной гиперплоскости, то количество точек пересечения отрезков, их соединяющих, с трехмерными поверхностями четырехмерных симплексов, образованных оставшимися 5-ю точками, четно.

(4-2) Существуют 7 точек в четырехмерном пространстве, никакие 5 из которых не лежат в одной гиперплоскости и такие, что любой отрезок, соединяющий 2 из них, пересекает поверхность четырехмерного симплекса, образованного оставшимися 5-ю точками, в четном числе точек.

## 4 Кратные версии (M)

**M = multiplicity.** Любые 17 точек на плоскости можно разбить на 3 множества, выпуклые оболочки которых имеют общую точку.

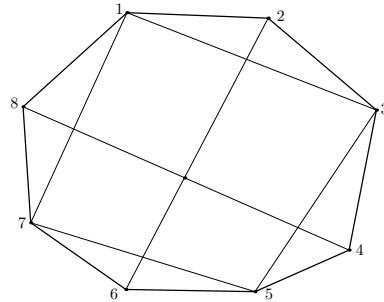


Рис. 4: Общая точка трех выпуклых оболочек

*Доказательство.* Вершины любого выпуклого 8-угольника на плоскости можно разбить на 3 множества, выпуклые оболочки которых имеют общую точку (рис. 4).

Если у выпуклой оболочки данного множества из 17 (или даже из 11) точек не менее 8 вершин, то разобьем эти восемь вершин на 3 множества как выше. Если же у нее менее 8 вершин, то обозначим через  $S_1$  множество этих вершин. Оставшихся точек не менее 4. Поэтому их можно разбить на два множества, выпуклые оболочки которых пересекаются. Это пересечение лежит и в выпуклой оболочке множества  $S_1$ .

**Теорема 4.1** (M:  $r$ -кратная теорема Радона для плоскости; теорема Тверберга для плоскости, 1965). *Любые 7 точек плоскости можно разбить на 3 множества, выпуклые оболочки которых имеют общую точку.*

*Любые  $3r - 2$  точки плоскости можно разбить на  $r$  множества, выпуклые оболочки которых имеют общую точку.*

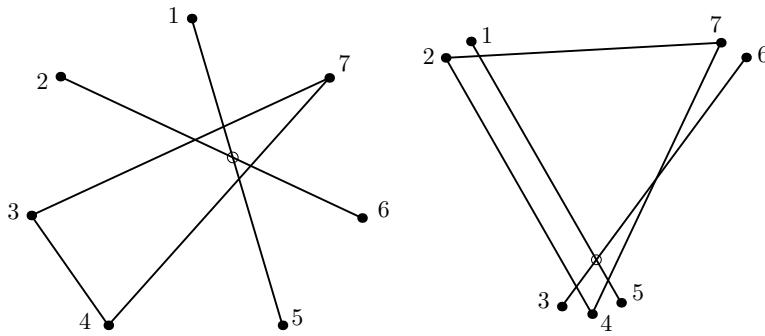


Рис. 5: Общая точка трех выпуклых оболочек

Прежде, чем доказывать теоремы М и DM, рекомендуем решить задачи 4.2, 4.3, 4.4, 4.6.

**4.2** (ср. с теоремой М). (а) Существуют 6 точек плоскости, при любом разбиении которых на 3 множества выпуклые оболочки этих множеств не имеют общей точки.

*Указание.* Возьмем по паре точек около каждой вершины треугольника.

(б) Существуют 7 точек плоскости, ни одна из которых не лежит ни в одном из треугольников, образованных оставшимися точками.

*Указание.* Возьмем вершины выпуклого 7-угольника.

(с) Существуют 7 точек плоскости со следующим свойством. Возьмем любые два отрезка, соединяющие две непересекающиеся пары данных точек. Тогда либо эти отрезки не пересекаются, либо их точка пересечения не лежит в треугольнике, образованном тремя оставшимися точками из данных.

*Указание.* Возьмем вершины правильного треугольника и его центр. Добавим к взятым точкам середины отрезков, соединяющих вершины с центром.

(д) Обобщите эти примеры на  $r$ -кратный случай.

*Количественная трехкратная теорема Радона для плоскости (QM) неизвестна!*

**4.3.** Существуют ли 6 точек на плоскости, при любом разбиении которых на 3 множества выпуклые оболочки некоторых двух из этих множеств не пересекаются?

**4.4.** (а) Для вершин правильного 7-угольника число разбиений из теоремы М равно 7.

*Указание.* Каждое такое разбиение похоже на повернутое разбиение с рис. 5 слева.

(б) Для точек рисунка 5 справа число разбиений из теоремы М равно 4.

*Указание.* Это следует из того, что для каждого такого разбиения одна из выпуклых оболочек — это треугольник с первой вершиной 4, второй вершиной 1 или 2 и третьей вершиной 6 или 7.

*Замечание.* Отсюда вытекает, что следующая сумма имеет разную четность для двух вышеупомянутых 7-элементных множеств  $M_a, M_b$

$$v(M_i) := \sum_{\{R_1, R_2, R_3\} : M_i = R_1 \sqcup R_2 \sqcup R_3} |\langle R_1 \rangle \cap \langle R_2 \rangle \cap \langle R_3 \rangle|.$$

См. подробнее [Sk18, §2].

**Теорема 4.5** (DM:  $r$ -кратная теорема Радона для пространства; теорема Тверберга для пространства, 1965). *Любые  $4r - 3$  точки пространства можно разбить на  $r$  множеств, выпуклые оболочки которых имеют общую точку.*

**4.6** (ср. с теоремой DM). (а) Существуют 8 точек пространства, при любом разбиении которых на 3 множества выпуклые оболочки этих множеств не имеют общей точки.

- (b) Существуют  $4r - 4$  точек пространства, при любом разбиении которых на  $r$  множеств выпуклые оболочки этих множеств не имеют общей точки.
- (c) Существуют  $(r - 1)(d + 1)$  точек  $d$ -мерного пространства, при любом разбиении которых на  $r$  множеств выпуклые оболочки этих множеств не имеют общей точки.

**4.7. \*** Сформулируйте и докажите аналог задачи 4.3 для пространства.

В доказательствах теорем М и ДМ можно использовать без доказательства цветную теорему Каратеодори (доказательство которой не является частью этого проекта).

**Теорема 4.8** (Барань; цветная теорема Каратеодори). *Пусть точка  $0 \in \mathbb{R}^n$  лежит в выпуклой оболочке каждого из  $n + 1$  конечных множеств  $M_0, M_1, \dots, M_n \subset \mathbb{R}^n$ . Тогда существуют точки  $t_i \in M_i$ , для которых  $0 \in \langle t_0, t_1, \dots, t_n \rangle$ .*

**Теорема 4.9** (SM: трехкратная теорема Радона для малой размерности о множествах одинакового размера; линейная теорема Саркарии, 1991). *\* Из любых 11 точек пространства можно выбрать 3 попарно непересекающиеся тройки так, чтобы три треугольника, образованные этими тройками, имели общую точку.*

**4.10** (ср. с теоремой SM). Существуют 10 точек пространства, из которых нельзя выбрать 3 попарно непересекающиеся тройки, выпуклые оболочки которых имеют общую точку.

**Теорема 4.11** (SDM:  $r$ -кратная теорема Радона для произвольной размерности о множествах одинакового размера; линейная теорема Саркарии-Воловикова, 1991-1996). *\* Если  $r$  — степень простого, то из любых  $(kr + 2)(r - 1) + 1$  точек пространства  $\mathbb{R}^{kr}$  можно выбрать такие  $r$  попарно непересекающихся наборов по  $k(r - 1) + 1$  точке в каждом, что выпуклые оболочки этих наборов имеют общую точку.*

Верен ли аналог этой теоремы для  $r = 6$ , **неизвестно!**

*Количественные версии (QSM), (QDM), (QSMD) неизвестны, даже если  $r$  — степень простого! Версия ( $S'M$ ) о трехкратной зацепленности неизвестна, см. [Skr].*

## 5 Приложение: топологические версии (T)

Начнем с усиления непланарности графа  $K_5$  — топологической версии (ST) теоремы Радона для плоскости о множествах одинакового размера.

Будем рассматривать такие изображения графа на плоскости, при которых ребра изображаются ломаными и допускаются самопересечения. Формализуем это пояснение для графа  $K_n$ .

**Кусочно-линейным (PL) отображением**  $f : K_n \rightarrow \mathbb{R}^2$  графа  $K_n$  в плоскость назовем набор  $\binom{n}{2}$  (незамкнутых) ломаных, попарно соединяющих некоторые  $n$  точек на плоскости. **Образом**  $f(\sigma)$  **ребра**  $\sigma$  назовем ломаную, соответствующую ребру  $\sigma$ . **Образом** набора ребер назовем объединение образов ребер из набора.

**Теорема 5.1** (ST). *Для любого PL отображения графа  $K_5$  в плоскость найдутся два несмежных ребра, образы которых пересекаются.*

Теорема (ST) выводится из ее количественной версии (QST): при «случайном» изображении графа  $K_5$  на плоскости количество точек пересечения несмежных ребер нечетно (в выводе используется аппроксимация [Sk20, Лемма об аппроксимации 1.4.6b].)

Пусть  $f : K_n \rightarrow \mathbb{R}^2$  — PL отображение. Оно называется PL отображением **общего положения**, если все вершины ломаных находятся в общем положении. Тогда образы

любых двух несмежных ребер пересекаются в конечном числе точек. Назовем **числом ван Кампена** (или инвариантом самопересечения)  $v(f)$  четность числа точек пересечения образов несмежных ребер.

**Теорема 5.2 (QST).** Для любого PL отображения общего положения графа  $K_5$  в плоскость число ван Кампена нечетно.

**Пример 5.3.** (a) Выпуклый пятиугольник и его диагонали образуют такое PL отображение общего положения  $f : K_5 \rightarrow \mathbb{R}^2$ , что  $v(f) = 1$ .

(b) Выпуклый четырехугольник и его диагонали образуют такое PL отображение общего положения  $f : K_4 \rightarrow \mathbb{R}^2$ , что  $v(f) = 1$ . Треугольник и точка внутри него образуют такое PL отображение общего положения  $f : K_4 \rightarrow \mathbb{R}^2$ , что  $v(f) = 0$ .

**Лемма 5.4** (о четности). Если вершины двух замкнутых плоских ломаных находятся в общем положении, то ломаные пересекаются в четном числе точек.<sup>2</sup>

**Доказательство теоремы (QST).** Ввиду задачи QS достаточно доказать, что  $v(f) = v(f')$  для любых двух PL отображений общего положения  $f, f' : K_5 \rightarrow \mathbb{R}^2$ , отличающихся только на внутренности одного ребра  $\sigma$ , причем  $f|_\sigma$  линейно (см. рис.). Ребра графа  $K_5$ , несмежные с  $\sigma$ , образуют цикл  $\Delta$ . Тогда

$$v(f) - v(f') = |(f\sigma \cup f'\sigma) \cap f\Delta| \mod 2 = 0.$$

Здесь второе равенство справедливо по лемме о четности.

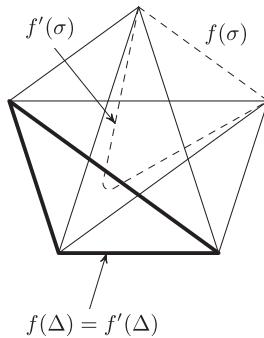


Рис. 6: Независимость  $v(f)$  от  $f$

**Утверждение 5.5.** Возьмем замкнутую плоскую ломаную  $L$ , вершины которой находятся в общем положении.

(a) Дополнение до  $L$  допускает шахматную раскраску (такую, что соседние области покрашены в разные цвета, см. рис.).

(b) Концы ломаной  $P$ , вершины которой находятся с вершинами ломаной  $L$  в общем положении, имеют одинаковый цвет, если и только если  $|P \cap L|$  четно.

**Внутренностью по модулю 2** плоской ломаной, вершины которой находятся в общем положении, называется объединение черных областей шахматной раскраски (при условии, что «бесконечная» область белая).

<sup>2</sup>Эта лемма нетривиальна, поскольку ломаные могут иметь самопересечения, и поскольку теорема Жордана нетривиальна. Выводить лемму о четности из теоремы Жордана или формулы Эйлера неразумно, ибо их доказательства используют лемму о четности или близкое утверждение. Интересные приложения леммы о четности 5.4 к теореме Жордана и алгоритмическим вопросам приведены в [Sk20, §1.4].

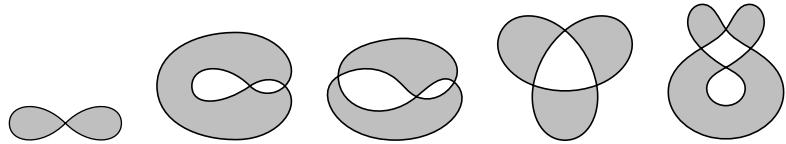


Рис. 7: Внутренности по модулю 2 ломаных

**Теорема 5.6** (Т: топологическая теорема Радона для плоскости; Баймоч-Барань, 1979). Для любого PL отображения общего положения  $f : K_4 \rightarrow \mathbb{R}^2$  либо

- образы некоторых несмежных ребер пересекаются, либо
- образ некоторой вершины лежит во внутренности по модулю 2 образа цикла из трех ребер, не содержащих эту вершину.

Эта теорема выводится из ее количественной версии (QT).

Для любого PL отображения общего положения  $f : K_4 \rightarrow \mathbb{R}^2$  назовем **числом Радона**  $\rho(f) \in \mathbb{Z}_2$  сумму четностей

- числа точек пересечения образов несмежных ребер, и
- числа тех вершин графа  $K_4$ , образы которых лежат во внутренности по модулю 2 образа цикла из трех ребер, не содержащих эту вершину.

**Теорема 5.7** (QT). Для любого PL отображения общего положения графа  $K_4$  в плоскость число Радона нечетно.

*Доказательство.* Ввиду задачи Q достаточно доказать, что  $\rho(f) = \rho(f')$  для любых двух PL отображений общего положения  $f, f' : K_4 \rightarrow \mathbb{R}^2$ , отличающихся только на внутренности одного ребра  $\sigma$ , причем  $f|_\sigma$  линейно (см. рис.). Обозначим через  $\tau$  ребро графа  $K_4$ , не соседнее с ребром  $\sigma$ , через  $S$  — внутренность по модулю 2 ломаной  $\partial S := f\sigma \cup f'\sigma$ . Получим

$$\rho(f) - \rho(f') = (|\partial S \cap f\tau| + |S \cap f(\partial\tau)|) \mod 2 = 0.$$

Здесь второе равенство следует из утверждения 5.5.b.  $\square$

**Числом оборотов** замкнутой ориентированной плоской ломаной  $A_1 \dots A_n$  вокруг не лежащей на ней точки  $O$  называется следующая сумма ориентированных углов, деленная на  $2\pi$ :

$$A_1 \dots A_n \cdot O := (\angle A_1 O A_2 + \angle A_2 O A_3 + \dots + \angle A_{n-1} O A_n + \angle A_n O A_1) / 2\pi.$$

**Пример 5.8.** (a) Число оборотов (произвольно ориентированного) многоугольника вокруг точки вне него равно 0, а вокруг точки внутри него равно  $\pm 1$ .

(b) Для любой замкнутой ориентированной ломаной ее внутренность по модулю 2 состоит из всех тех точек, вокруг которых число оборотов нечетно.

(c) Для каждой ломаной (с произвольной ориентацией) на рис. и точки на ваш выбор (в любой из ограниченных областей) найдите число оборотов ломаной вокруг точки.

Больше информации можно найти на [Wn].

**Лемма 5.9.** Рассмотрим замкнутую и незамкнутую ломаные  $L$  и  $P$  на плоскости, все вершины которых находятся в общем положении. Обозначим через  $P_0$  и  $P_1$  начальную и конечную точки  $P$ . Тогда  $L \cdot P = L \cdot P_1 - L \cdot P_0$ .

Число  $L \cdot P$  определяется как сумма знаков точек пересечения ломаных  $L$  и  $P$ . Эта лемма показывает, что дополнение до  $L$  имеет *нумерацию Мебиуса-Александера*, то есть «целочисленную шахматную раскраску».

**Теорема 5.10** (МТ: топологическая теорема Тверберга для плоскости; Барань-Шлосман–Сюч 1981, Езайдын 1987, Воловиков 1996). *Если  $r$  — степень простого, то для любого PL отображения  $f : K_{3r-2} \rightarrow \mathbb{R}^2$  либо  $r-1$  треугольников оборачиваются вокруг одной вершины, либо  $r-2$  треугольников оборачиваются вокруг пересечения двух ребер, где никакие два из указанных треугольников, ребер и вершин не имеют общих вершин.*

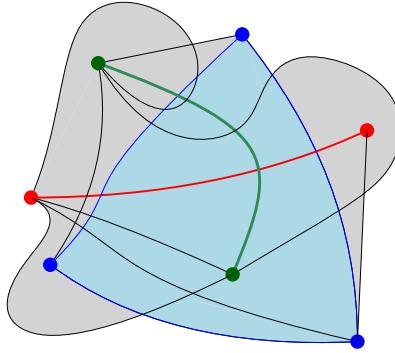


Рис. 8: Топологическая теорема Тверберга на плоскости,  $r = 3$

Верен ли аналог этой теоремы для  $r = 6$ , **неизвестно!**

*Количественная версия (QMT) неизвестна*, даже если  $r$  — степень простого!

Обозначим через  $\Delta_N$  симплекс размерности  $N$ .

**Теорема 5.11** (DT: топологическая теорема Радона). *Для любого непрерывного отображения  $\Delta_{d+1} \rightarrow \mathbb{R}^d$  образы некоторых его непересекающихся граней пересекаются.*

Попробуйте сформулировать утверждение (QDT). Оно верно.

**Теорема 5.12** (DMT: топологическая теорема Тверберга). *Если  $r$  — степень простого, то для любого PL отображения  $f : \Delta_{(d+1)(r-1)} \rightarrow \mathbb{R}^d$  существуют попарно непересекающиеся грани  $\sigma_1, \dots, \sigma_r \subset \Delta_{(d+1)(r-1)}$ , для которых  $f(\sigma_1) \cap \dots \cap f(\sigma_r) \neq \emptyset$ .*

*Количественная версия (QDMT) неизвестна*, даже если  $r$  — степень простого!

Аналог теоремы (DMT) неверен, если  $r$  — не степень простого (для  $d > 2r$ ). Для этих контрпримеров важны работы М. Езайдына (1987), М. Громова (2010), Ф. Фрика, П. Благоевича, Г. Циглера (2014-2015), И. Мабийяра и У. Вагнера (2015). Мы не обсуждаем соотношение вкладов разных авторов, поскольку это соотношение непростое. Читатель может составить собственное мнение, изучив доказательства и точные ссылки на каждый его шаг, см. обзоры [Sk16]. Контрпримеры были сначала построены для  $d > 3r$ , а затем для  $d > 2r$  (Аввакумов-Мабийяр-Скопенков-Вагнер, 2015).

Верен ли аналог этой теоремы для  $d \leq 2r$  и  $r$  не степени простого (например, для  $d = 2$  и  $r = 6$ ), **неизвестно!**

Попробуйте сформулировать утверждения (SDT), (QSdT), (SMT), (QSMT), (SDMT), и (QSDMT)!

Утверждения (SDT) и (QSdT) верны (теорема ван Кампена-Флореса, 1932-34).

Утверждения (SMT), (SDMT) верны, если  $r$  — степень простого ( $r$ -кратная теорема ван Кампена-Флореса, Саркарья 1991, Воловиков 1996). Утверждения (SMT) и (SDMT) неверны для  $d \leq 2r$  и  $r$  не степени простого (Мабийяр-Вагнер 2015 для «коразмерности»)

$\geq 3$ , Аввакумов-Мабийяр-Скопенков-Вагнер 2015 для «коразмерности» 2). см. обзоры [Sk16]. Верны ли этих утверждения для «коразмерности» 1, **неизвестно!**.

*Количественные версии (QSMT) и (QSDMT) неизвестны*, даже если  $r$  — степень простого!

## Answers, hints, solutions

**D.** Является частным случаем теоремы Радона D(d).

**SD.** (3) Введём обозначения из первого абзаца перехода индукции в доказательстве теоремы Радона для  $d = 2$ . Воспользуемся утверждением S для множества  $M$ . Получим разбиение на два двухэлементных множества  $U'_1$  и  $U'_2$ , выпуклые оболочки которых пересекаются. Повторим 4, 5 и 6 абзацы в доказательстве теоремы Радона. Получим, что  $X_2 \in \langle O, U_1 \rangle \cap \langle U_2 \rangle$ , что и требовалось.

(4) Существует гиперплоскость  $\alpha$ , для которой ровно одна точка из набора лежит по одну сторону от  $\alpha$ , а остальные — по другую. Обозначим точки через  $O, A_1, \dots, A_6$  так, чтобы  $\alpha$  отделяла  $O$  от  $A_1, \dots, A_6$ . Для  $1 \leq i \leq 6$  обозначим  $A'_i := OA_i \cap \alpha$ . Ясно, что никакие 4 точки из  $A'_1, \dots, A'_6$  не лежат на одной плоскости. Воспользуемся теоремой S'D для точек  $A'_1, \dots, A'_6$ . Получим два зацепленных треугольника  $\Delta_1$  и  $\Delta_2$  (например,  $\Delta_1 = A'_2 A'_3 A'_5$ ,  $\Delta_2 = A'_1 A'_4 A'_6$ ).

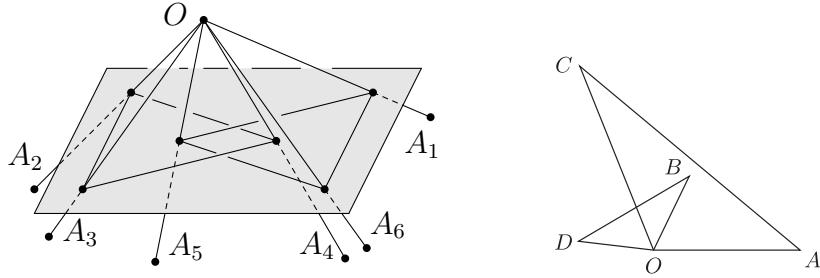


Рис. 9: Слева: гиперплоскость в  $\mathbb{R}^4$  (изображенная как плоскость в пространстве) пересекает отрезки  $OA_1, \dots, OA_6$  в 6 точках  $A'_1, \dots, A'_6$ , которые являются вершинами двух зацепленных треугольников. Справа: сечение плоскостью  $\gamma$ :  $\Delta_1^\gamma = OAC$ ,  $\Delta_2^\gamma = OBD$ .

Обозначим через  $\gamma$  плоскость, содержащую  $O$  и прямую пересечения зацепленных треугольников. Ясно, что  $\gamma \cap \alpha$  — прямая, и  $\Delta_j^\gamma := \gamma \cap O\Delta_j$  — треугольники ( $j = 1, 2$ ). Единственная сторона треугольника  $\Delta_j^\gamma$ , не содержащая точку  $O$  — это  $\gamma \cap \Delta_j$ , а две другие стороны треугольника  $\gamma \cap \Delta_j$  являются пересечением плоскости  $\gamma$  и боковых поверхностей тетраэдра  $O\Delta_j$ .

Раз треугольники  $\alpha \cap O\Delta_1$  и  $\alpha \cap O\Delta_2$  зацеплены, то точки пересечения прямой  $\gamma \cap \alpha$  с контурами треугольников  $\Delta_1^\gamma$  и  $\Delta_2^\gamma$  чередуются вдоль прямой. Следовательно, эти контуры пересекаются в точке, отличной от  $O$ .

Эта точка пересечения либо является пересечением сторон треугольников  $\gamma \cap \Delta_1$  и  $\gamma \cap \Delta_2$ , либо, не умаляя общности, стороны треугольника  $\gamma \cap \Delta_1$  и объединения двух сторон треугольника  $\Delta_2^\gamma$ , содержащих  $O$ . В первом случае  $\Delta_1$  пересекается с  $\Delta_2$ . Во втором случае  $\Delta_1$  пересекается с боковой гранью  $O\Delta_2$ .

**S'D.** Следует из теоремы QS'D.

**1.1.** 0, если они параллельны; 1, если прямая пересекает плоскость;  $\infty$ , если прямая полностью лежит в плоскости.

**1.4.** (a) Пара точек  $(0, 0, 1)$  и  $(0, 0, -1)$ .

(b) Окружность  $\begin{cases} x = 0, \\ y^2 + z^2 = 1 \end{cases}$ .

(c) Объединение четвертей трех окружностей:

$$\begin{cases} x = 0, y \geq 0, z \geq 0 \\ y^2 + z^2 = 1 \end{cases}, \quad \begin{cases} y = 0, x \geq 0, z \geq 0 \\ x^2 + z^2 = 1 \end{cases} \quad \text{и} \quad \begin{cases} z = 0, x \geq 0, y \geq 0 \\ x^2 + y^2 = 1 \end{cases}.$$

**1.5.** (a) Пара точек  $(0, 0, 0, 1)$  и  $(0, 0, 0, -1)$ .

(b) Окружность  $\begin{cases} x = y = 0 \\ z^2 + t^2 = 1 \end{cases}$ .

(c) Сфера  $\begin{cases} x = 0 \\ y^2 + z^2 + t^2 = 1 \end{cases}$ .

(d) Граф  $K_4$ , образованный объединением четвертей шести окружностей, одна из которых —  $\begin{cases} x = y = 0, z \geq 0, t \geq 0 \\ z^2 + t^2 = 1 \end{cases}$ .

**1.8.** (b) Пустое множество, точка (если прямая пересекает плоскость), прямая (если прямая содержится в плоскости).

(c) Пустое множество, прямая (если плоскость пересекает гиперплоскость), плоскость (если плоскость содержится в гиперплоскости).

(d) Пустое множество, плоскость (если они пересекаются), гиперплоскость (если они совпадают).

(e) Пустое множество, точка или прямая (если они пересекаются), плоскость (если они совпадают).

**1.9.** (b) Пустое множество; (e) точка.

*Замечание.* Из ответа к (b) следует, что если никакие 5 из 6 вершин двух треугольников в  $\mathbb{R}^4$  не лежат в одной гиперплоскости, то контур первого не пересекает второй. Это означает, что никакие два треугольника «общего положения» в  $\mathbb{R}^4$  «не зацеплены».

**D(d).** Индукция по  $d$ . База для  $d = 1$  очевидна.

*Переход* от  $d$  к  $d + 1$ . Существует  $d$ -мерная гиперплоскость  $\alpha$ , для которой ровно одна точка из данного набора лежит по одну сторону от  $\alpha$ , а остальные — по другую. Обозначим через  $O$  одну точку набора, а через  $M$  множество оставшихся точек набора так, чтобы  $\alpha$  отделяла  $O$  от  $M$ . Для любой точки  $A \in M$  обозначим  $A' := \alpha \cap OA$ .

Воспользуемся теоремой Радона для множества  $M' := \{A' \mid A \in M\}$  из  $d + 2$  точек в  $d$ -мерном пространстве  $\alpha$ . Получим разбиение на два множества  $U'_1$  и  $U'_2$ , выпуклые оболочки которых пересекаются в точке  $X'$ . Обозначим  $U_1 := \{A \mid A' \in U'_1\}$  и  $U_2 := \{A \mid A' \in U'_2\}$ .

Ясно, что  $U'_1 \subset \langle O, U_1 \rangle$ . Следовательно,  $X' \in \langle O, U_1 \rangle$ , и, более того, весь отрезок  $OX'$  содержится в  $\langle O, U_1 \rangle$ . Обозначим через  $X_1$  точку, для которой прямая  $OX'$  пересекает  $\langle O, U_2 \rangle$  по отрезку  $OX_1$ . Тогда  $X_1 \in \langle U_1 \rangle$  и  $X' \in OX_1$ .

Аналогично, через  $X_2$  обозначим точку, для которой прямая  $OX'$  пересекает  $\langle O, U_2 \rangle$  по отрезку  $OX_2$ . Тогда  $X_2 \in \langle U_2 \rangle$  и  $X' \in OX_2$ .

Точки  $X_1$  и  $X_2$  лежат на луче  $OX'$ . Не умоляя общности,  $X_2$  лежит между  $O$  и  $X_1$ . Тогда  $X_2 \in \langle O, U_1 \rangle \cap \langle U_2 \rangle$ , что и требовалось.

**2.2.** (a) Нет, не находятся. Любые три диаметра пересекаются в одной точке.

**2.3.** (a) Рассмотрим произвольную прямую  $l$ , отличную от данных. Ей принадлежит бесконечное число точек, а каждая прямая пересекает  $l$  не более чем в одной точке. Следовательно, найдется точка на  $l$ , не принадлежащая ни одной из данных прямых.

(b) Да, существуют. Докажем индукцией по  $n$ , что существует  $n$  точек общего положения на плоскости. База для  $n = 1$  очевидна, переход следует из утверждения 2.3.а.

(c) Указание. Объединение красных отрезков есть сумма по модулю 2 контуров красных треугольников. И  $(A \oplus B) \cap C = (A \cap C) \oplus (B \cap C)$ .

**2.4.** Тетраэдр разбивает пространство, далее аналогично лемме о четности 2.1.

**2.5. (a)** Ответ: да, существуют. Построение аналогично задаче 2.3.b.

(b) Следует из леммы о четности 2.4 аналогично утверждению 2.3.c.

**2.7. (a)** Ответ: да, существуют. Построение аналогично построениям в задачах 2.3.b и 2.5.a.

(b) Следует из леммы о четности 2.1 аналогично утверждениям 2.3.c и 2.5.b.

**QSD.** (3) Любые два треугольника, натянутые на две непересекающиеся тройки отмеченных вершин, пересекаются либо по пустому множеству, либо по отрезку. Отметим все концы всех отрезков, являющихся пересечением треугольников. Ввиду общности положения концов четное число, и точка является концом тогда и только тогда, когда точка является пересечением отрезка с треугольником.

(4) Сведем доказательство теоремы к следующему предложению.

**Предложение.** Пусть  $O\Delta_1$  и  $O\Delta_2$  — два тетраэдра, имеющих ровно одну общую вершину. Пусть также  $\alpha$  — гиперплоскость, отделяющая точку  $O$  от вершин треугольников  $\Delta_1$  и  $\Delta_2$ . Тогда поверхности тетраэдров  $O\Delta_1$  и  $O\Delta_2$  пересекаются в четном числе внутренних точек тогда и только тогда, когда треугольники  $\alpha \cap O\Delta_1$  и  $\alpha \cap O\Delta_2$  зацеплены в пространстве  $\alpha$ .

*Доказательство теоремы.* Просуммируем количество внутренних точек пересечения граней тетраэдров  $O\Delta_1$  и  $O\Delta_2$  по всем разбиениям точек  $A_1, \dots, A_6$  на два треугольника  $\Delta_1$  и  $\Delta_2$ . По предложению и теореме QS'D эта сумма нечетна. Отметим, что никакая пара боковых граней тетраэдров  $O\Delta_1$  и  $O\Delta_2$  не имеет внутренних точек пересечения. Теперь ясно, что в сумме каждая пара пересекающихся по внутренней точке треугольников с вершинами в данных точках подсчитана ровно один раз. Следовательно, искомых пар нечетно, что и требовалось доказать.  $\square$

Для доказательства предложения необходимо повторить доказательство теоремы SD(4). Вместо 3-го абзаца необходимо сослаться на следующее очевидное утверждение.

**Утверждение.** На плоскости даны два треугольника  $OAB$  и  $OCD$  и прямая  $l$ , пересекающая отрезки  $OA$ ,  $OB$ ,  $OC$  и  $OD$ . Контуры треугольников  $OAB$  и  $OCD$  пересекаются в четном числе точек тогда и только тогда, когда пересечения прямой  $l$  с контурами треугольников  $OAB$  и  $OCD$  чередуются вдоль прямой.

**3.1.** Рассмотрите  $\Delta \cap \Delta'$ .

**QS'D.** Существует плоскость  $\alpha$ , для которой ровно одна точка из набора лежит по одну сторону от  $\alpha$ , а остальные — по другую. Обозначим точки через  $O, A_1, \dots, A_5$  так, чтобы  $\alpha$  отделяла  $O$  от  $A_1, \dots, A_5$ .

Следующие количества имеют одну и ту же четность:

- количество  $P$  неупорядоченных пар зацепленных треугольников с вершинами в точках  $O, A_1, \dots, A_5$ .

- количество  $Q$  отрезков  $A_iA_j$ , расположенных под нечетным числом сторон «дополнительного» треугольника  $A_kA_lA_m$ .

- количество упорядоченных пар  $(A_iA_j, A_kA_l)$  отрезков, для которых  $A_iA_j$  лежит ниже  $A_kA_l$ .

- количество точек пересечения отрезков с вершинами в  $A'_1, \dots, A'_5$ .

Здесь сравнение  $P \equiv Q \pmod{2}$  следует из утверждения 3.3.

По теореме QS последнее количество нечетно, следовательно, требуемое количество  $P$  также нечетно.

**3.5. (3)** В качестве примера можно взять вершины, расположенные как на рисунке 3.

(3') Это свойство равносильно теореме QSD.3.

**3.6.(4'-3).** Пометим все точки пересечения пар треугольников, натянутых на две непересекающиеся тройки данных точек. Тогда искомая величина имеет ту же четность, что и удвоенное количество помеченных точек. Следовательно, искомая величина четна.

**4.6. (a)** Возьмем по паре точек в каждой вершине тетраэдра.

(c) Возьмем по  $r - 1$  точек в каждой вершине  $d$ -мерного симплекса.

## Список литературы

- [AMS+] *S. Avvakumov, I. Mabillard, A. Skopenkov and U. Wagner. Eliminating Higher-Multiplicity Intersections, III. Codimension 2, Israel J. Math., to appear.* arxiv:1511.03501.
- [Ko18] \* *E. Колпаков.* Доказательство теоремы Радона при помощи понижения раз мерности, Мат. Просвещение, 23 (2018), arXiv:1903.11055.
- [La] *B. Лапушкин,* Доказательство теоремы Радона. <https://www.mccme.ru/circles/oim/mmks/works2019/lapushkin4.pdf>
- [RRS] \* *V. Retinskij, A. Ryabichev and A. Skopenkov.* Motivated exposition of the proof of the Tverberg Theorem (in Russian). Mat. Prosveschenie, to appear. arXiv:2008.08361.
- [Sk14] \* *A. Skopenkov.* Realizability of hypergraphs and Ramsey link theory, arXiv:1402.0658.
- [Sk16] \* *A. Skopenkov,* A user's guide to the topological Tverberg Conjecture, Russian Math. Surveys, 73:2 (2018), 323–353. arXiv:1605.05141. Section 4 of the published version is available as *A. Skopenkov, On van Kampen-Flores, Conway-Gordon-Sachs and Radon theorems*, arXiv:1704.00300.
- [Sk18] \* *A. Skopenkov.* Invariants of graph drawings in the plane. Arnold Math. J., 6 (2020) 21–55; full version: arXiv:1805.10237.
- [Sk20] \* *A. Skopenkov.* Algebraic Topology From Geometric Viewpoint (in Russian), MCCME, Moscow, 2020 (2nd edition). Electronic version: <http://www.mccme.ru/circles/oim/home/combttop13.htm#photo>
- [Sk] \* *A. Скопенков.* Алгебраическая топология с алгоритмической точки зрения, <http://www.mccme.ru/circles/oim/algor.pdf>.
- [Skr] \* *A. Skopenkov.* Realizability of hypergraphs, slides for talks, [https://www.mccme.ru/circles/oim/algor1\\_beamer.pdf](https://www.mccme.ru/circles/oim/algor1_beamer.pdf).
- [Wn] \* [https://en.wikipedia.org/wiki/Winding\\_number](https://en.wikipedia.org/wiki/Winding_number)  
В этом списке звездочками отмечены книги, обзоры и популярные статьи.

# Towards higher-dimensional combinatorial geometry\*

presented by E. Kogan, V. Retinskiy, E. Riabov<sup>†</sup> and A. Skopenkov<sup>‡</sup>

## Introduction

Many fields of science and technology, primarily mathematics, computer science and physics, often work with higher-dimensional space. Solving the following problems allows to acquire basic skills of such work. You will both develop spatial imagination and intuition, and learn how to check them by rigorous arguments. This is useful for further learning of computer graphics, as well as for necessary methods of linear algebra and geometry.

The main ideas are presented as ‘olympic’ examples in easiest specific cases, free of technical details and only with minimal amount of scientific terminology (see the problems). This makes the project accessible for beginners though still containing beautiful and complicated results. The project does not require preliminary knowledge of stereometry. Geometric intuition in space and ability to solve systems of linear equations will be useful (see Problem 1.2).

In this project we generalize the following result (see the following problems S, D, SD and §3).

**Radon theorem in the plane.** *For any 4 points in the plane either one of them belongs to the triangle with vertices at the others, or they can be decomposed into two pairs such that the segment joining the points of the first pair intersects the segment joining the points of the second pair.*

**S = same size.** From any 5 points in the plane one can choose two disjoint pairs such that segments joining them intersect.

In this text a triangle  $\Delta$  is the part of plane bounded by the outline  $\partial\Delta$ . This part can be a line segment.

**D = dimension.** For any 5 points in the space either one of them belongs to the tetrahedron with vertices at the others, or the segment joining some two of them intersects the triangle formed by the remaining three of them.

In this text interesting non-trivial problems are called theorems.

**Theorem SD:** Radon theorem for sets of almost the same size.

(3) *From any 6 points in the space one can choose a disjoint pair and a triple such that the segment joining points of the pair intersects the triangle formed by the triple.*

(4) *(linear van Kampen-Flores theorem, 1932) From any 7 points in 4-dimensional space one can choose two disjoint triples such that the corresponding triangles intersect.*

Definition of 4-dimensional space and of notions required for proofs are presented in §1 and in §2. For a proof of Theorem SD.4 you would also need Theorem S'D below.

---

\*We are grateful to D. Eliseev for translation of a part of the text and to A. Ryabichev for helpful comments.

<sup>†</sup>E. Kogan, V. Retinskiy, E. Riabov — Higher School of Economics, Moscow.

<sup>‡</sup><https://users.mccme.ru/skopenko>. Moscow Institute of Physics and Technology, Independent University of Moscow.

Take two non-degenerate triangles in the space no 4 of whose vertices lie in a plane. Such triangles are **linked** if the outline of the first triangle intersects second triangle at exactly one point.

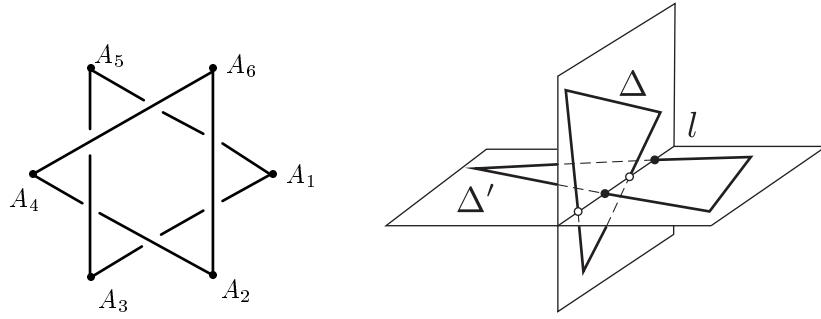


Figure 1: Linked triangles and linked pairs of points

**Theorem S'D:** spatial Radon theorem on linking of same size sets; linear Conway-Gordon-Sachs theorem, 1981-1983.

*If no 4 of 6 points in the space lie in a plane then there are two linked triangles with vertices in these points.*

For a proof you would need assertion QS of §3.

Other ‘olympic’ problems are Theorem D(d) in §1, 2.3.c, 2.5.b, 2.7.b, 3.2, 3.6.(4'-3). Open problems — 3.6.(4-3),(4-2),(4'-2).

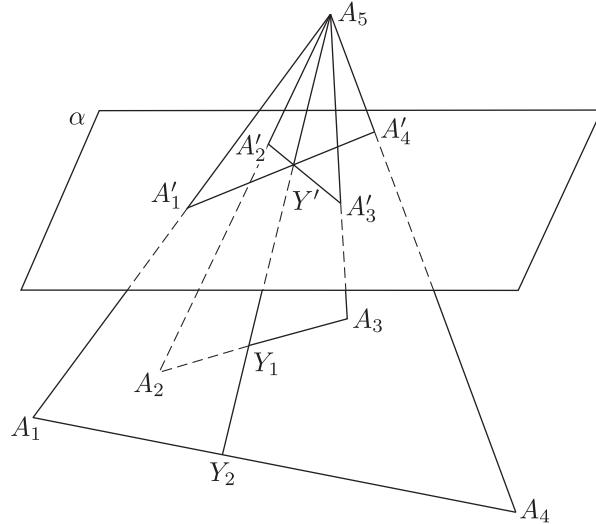


Figure 2: Hint to problem D

### Recommendations for participants

If a mathematical statement is formulated as a problem, then the objective is to prove this statement. If a problem is named ‘theorem’ (‘lemma’, ‘corollary’, etc.), then this statement is considered to be more important. Usually we *formulate* a beautiful or important statement *before* giving a sequence of results (lemmas, assertions, etc) which constitute its proof. In this case, in order to prove this statement, one may need to solve some of the subsequent problems. We give hints on that after the statements but we do not want to deprive you of the pleasure of finding the right moment when you finally are ready to prove the statement. In general, if you are stuck on a certain problem, try looking at the next ones. They may turn out to be helpful. *Remarks* and problems marked by star are not used in the sequel. Important definitions are highlighted in **bold** for easy navigation.

For every **solution written for a user** (see recommendations below) marked with either ‘+’ or ‘+.’ a student (or a group of students) gets a ‘bean’. The jury may also award extra beans for beautiful solutions, solutions of hard problems, or solutions typeset in  $\text{\TeX}$ . The jury has infinitely many beans. Every participant (or group of participants) initially has 1 bean. One may submit a solution **in oral form** or as **written for a developer**, and one loses a bean with each 5 attempts (successful or not).

Participants (or teams) can submit their solutions by a personal communication to Egor Riabov at <https://mattermost.turgor.ru>. Please also send him questions and requests for hints on problems which you are stuck with. Students who successfully work on the project are entitled to ask interesting *extra problems for investigation*.

Participants (or teams) from Serbia and Croatia may submit their solutions to Prof. Rade Živaljević at [rade@mi.sanu.ac.rs](mailto:rade@mi.sanu.ac.rs).

### How to write a proof for a user

We give some recommendations on how to write a proof that could be included in a mathematical book or research paper (which is a ‘reliable reference’, cf. <https://arxiv.org/pdf/2101.03745.pdf>, p. 2). These recommendations are by no means complete. You can learn to write proofs (solutions of problems) by trying to write them and discussing your text with a teacher.

See also [https://en.wikipedia.org/wiki/KISS\\_principle](https://en.wikipedia.org/wiki/KISS_principle)

<http://people.apache.org/~fhanik/kiss.html>

*A genius makes his own rules, but a ‘how to’ article is written by one ordinary mortal for the benefit of another... Most things that an article such as this one can say have at least one counterexample in the practice of some natural born genius. Authors of articles such as this one know that, but in the first approximation they must ignore it, or nothing would ever get done.*

(P. Halmos, How to talk mathematics.)

(1) Only write sentences that make sense.<sup>1</sup>

(1a) In particular, long sentence usually does not make sense because it is unclear which exactly parts of long sentence words ‘and’, ‘or’, ‘then’ are tying together. So break long sentences into short ones.

(2) Introduce notation and each definition explicitly with ‘define’, ‘denote’, ‘let’, ‘set’, ‘put’. For example, the phrase ‘ $a = b + c$ ’ without these words means ‘the previously defined object  $a$  equals to the sum of the previously defined objects  $b$  and  $c$ ’.

(5) Do not put any part of your solution in parentheses. Parentheses do not make clear the logical relation between the phrase in and outside the parentheses. (Parentheses are used for remarks which are not part of the solution.)

---

<sup>1</sup>For example, none of the following two sentences makes sense:

$$1 + 2 + \dots + n = \frac{n(n+1)}{2},$$

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \text{ for a positive integer } n,$$

because it is not written for which  $n$  the statement is stated. The following statements do make sense:

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \text{ for every positive integer } n,$$

$$1 + 2 + \dots + n = \frac{n(n+1)}{2} \text{ for some positive integer } n,$$

$$1 + 2 + \dots + n = 100 \text{ for some positive integer } n.$$

However, the second of them is not interesting and the third is not correct.

# 1 How to work with four-dimensional space?

For Problems 1.1, 1.4.abc, 1.5.abcd, 1.8.cd and 1.9.be below it suffices to give correct answers.  
(Solution of Problem 1.8.a is already presented in this text.)

**1.1.** How many intersection points can a line and a plane have in the space?

**1.2.** How many solutions can have a system of linear equations

- (a)  $2 \times 2$ ; (b)  $2 \times 3$  (2 equations, 3 variables); (c)  $3 \times 2$ ?

We define

- the *line* as the set of all real numbers;
- the *plane*  $\mathbb{R}^2$  as the set of all ordered pairs  $(x, y)$  of real numbers  $x$  and  $y$ ;
- *three-dimensional space (3-space)*  $\mathbb{R}^3$  as the set of all ordered triples  $(x, y, z)$  of real numbers;
- *four-dimensional space (4-space)*  $\mathbb{R}^4$  as the set of all ordered quadruples  $(x, y, z, t)$  of real numbers.

Definition of *d-dimensional space (d-space)*  $\mathbb{R}^d$  for  $d > 4$  is analogous.

For points  $A = (x_1, y_1, z_1, t_1), B = (x_2, y_2, z_2, t_2) \in \mathbb{R}^4$  and number  $\lambda \in \mathbb{R}$  denote

$$\lambda A := (\lambda x_1, \lambda y_1, \lambda z_1, \lambda t_1) \quad \text{and} \quad A + B := (x_1 + x_2, y_1 + y_2, z_1 + z_2, t_1 + t_2).$$

**1.3.** A 2-dimensional plane does not split the 4-dimensional space. I.e., for each two points outside the plane  $x = y = 0$  in 4-space, there exists a broken line which joins these points and does not intersect this plane.

For points  $A, B \in \mathbb{R}^4$  a *segment*  $AB$  is the set  $\{tA + (1 - t)B : t \in [0, 1]\}$ . A *broken line* is the union of segments  $A_i A_{i+1}$  over all  $i = 1, 2, \dots, n - 1$ .

*Hint.* For points  $A = (x_0, y_0, z_0, t_0)$  and  $B$  which do not lie in the plane  $x = y = 0$  define points

$$A_x = A + (1, 0, 0, 0) = (x_0 + 1, y_0, z_0, t_0) \quad \text{and} \quad A_y = A + (0, 1, 0, 0) = (x_0, y_0 + 1, z_0, t_0).$$

Prove that one of the broken lines  $AB$ ,  $AA_x B$  and  $AA_y B$  does not intersect the plane  $x = y = 0$ .

**1.4.** What is the intersection of the *2-dimensional sphere*

$$S^2 := \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$$

with the following sets:

- (a) the line  $x = y = 0$ , containing the center of the sphere;
- (b) the plane  $x = 0$ , containing the center of the sphere;
- (c) the intersection of the positive octant of  $\mathbb{R}^3$  and the union of the 2-dimensional coordinate planes, i.e.

$$\{(x, y, z) \in \mathbb{R}^3 : x \geq 0, y \geq 0, z \geq 0 \text{ and } xyz = 0\}.$$

**1.5.** What is the intersection of the *3-dimensional sphere*

$$S^3 := \{(x, y, z, t) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + t^2 = 1\}$$

with the following sets:

- (a) the line  $x = y = z = 0$ , containing the center of the sphere;
- (b) the plane  $x = y = 0$ , containing the center of the sphere;

- (c) the (3-dimensional) hyperplane  $x = 0$ , containing the center of the sphere;  
(d) the intersection of the positive ‘sixteenth’ of  $\mathbb{R}^4$  and the union of the 2-dimensional coordinate planes, i.e.

$$\{(x, y, z, t) \in \mathbb{R}^4 :$$

$: x \geq 0, y \geq 0, z \geq 0, t \geq 0$  and at least two of the four numbers  $x, y, z, t$  are zeros}.

A subset  $L \subset \mathbb{R}^4$  is called a **line** if  $L$  is not a point and there are points  $A, B \in \mathbb{R}^4$  such that  $L = \{A + Bt : t \in \mathbb{R}\}$ .

A subset  $L \subset \mathbb{R}^4$  is called a (2-dimensional) **plane** if  $L$  is neither a line nor a point, and there are points  $A, B, C \in \mathbb{R}^4$  such that  $L = \{A + Bt + Cu : t, u \in \mathbb{R}\}$ .

We already introduced definition of a line before. However, below ‘line’ means a subset of  $\mathbb{R}^d$  whose definition is similar to the one given above. Analogous remark applies to plane.

**1.6.** Write analogous definition of a (3-dimensional) **hyperplane** in  $\mathbb{R}^4$ .

In your solutions of the following problems on 4-space you can use without proof

- all rigorously formulated and correct facts on solutions of systems of linear equations;
- the results of Problem 1.7.

**1.7.** \* (a) A subset  $L \subset \mathbb{R}^4$  is a hyperplane if and only if  $L \neq \emptyset, L \neq \mathbb{R}^4$  and there exist  $a, b, c, d, e \in \mathbb{R}$  such that

$$L = \{(x, y, z, t) \in \mathbb{R}^4 : ax + by + cz + dt = e\}.$$

(b) A subset  $L \subset \mathbb{R}^4$  is a plane if and only if  $L \neq \emptyset, L \neq \mathbb{R}^4, L$  is not a hyperplane and there exist  $a_1, b_1, c_1, d_1, e_1, a_2, b_2, c_2, d_2, e_2 \in \mathbb{R}$  such that

$$L = \{(x, y, z, t) \in \mathbb{R}^4 : a_1x + b_1y + c_1z + d_1t = e_1, a_2x + b_2y + c_2z + d_2t = e_2\}.$$

(c) State and prove analogous result for a line in  $\mathbb{R}^4$ .

**1.8.** What could be the intersection in  $\mathbb{R}^4$  of:

- (a) a line and a hyperplane?    (b) a line and a plane?
- (c) a plane and a hyperplane?    (d) two hyperplanes?    (e) two planes?

*Hint to (a).* Answer. The empty set, a point, a line.

*Examples.* The empty set is the intersection of the line  $x = y = z = 0$  and the hyperplane  $x = 1$ . A point is the intersection of the line  $x = y = z = 0$  and the hyperplane  $t = 0$ . A line is the intersection of the line  $x = y = z = 0$  and the hyperplane  $x = 0$ .

*Proof that other intersections are impossible.* It suffices to prove that if the intersection in  $\mathbb{R}^4$  of a line  $l$  and a hyperplane contains at least two points, then the intersection coincides with the line  $l$ . This holds because *for any two points there exists a unique line containing both these points*. The latter fact is easily proved using the definition of a line. (In many other expositions this fact is accepted as an axiom.)

**1.9.** For different points  $X, Y \in \mathbb{R}^4$  define the *line XY* as  $\{X + (Y - X)t = (1 - t)X + tY : t \in \mathbb{R}\}$ . For points  $X, Y, Z \in \mathbb{R}^4$  not belonging to any line define the *plane XYZ* as

$$\{X + (Y - X)t + (Z - X)u = (1 - t - u)X + tY + uZ : t, u \in \mathbb{R}\}.$$

No five of eight points 1,2,3,4,5,6,7,8 in  $\mathbb{R}^4$  belong to a hyperplane. What could be the intersection of:

- (b) the line 12 and the plane 567?    (d) the hyperplanes 1234 and 5678?
- (e) the planes 123 and 567?

The **convex hull** of a finite collection of points  $A_1, \dots, A_n \in \mathbb{R}^d$  is by definition the set

$$\langle A_1, \dots, A_n \rangle := \{\lambda_1 A_1 + \dots + \lambda_n A_n : \lambda_1, \dots, \lambda_n \geq 0, \lambda_1 + \dots + \lambda_n = 1\}.$$

**1.10.** The convex hull of a finite collection of points in the plane is the least (by inclusion, or by area) convex polygon containing all these points.

**Theorem D(d):** the Radon theorem, 1929.

*Any  $d + 2$  points in  $d$ -space can be split into two subsets whose convex hulls intersect.*

**Edification.** Usually only the simplest properties of planar and spatial geometric objects are deduced from the analytic definition (or just accepted as axioms). More complicated properties can be deduced in a ‘synthetic’ (‘geometric’) way from the simplest ones (i.e., as in school geometry, without using the analytic definition). Often it is convenient to reduce a planar problem to a linear one (i.e., to a problem in a line), and a spatial problem to a planar one. Similarly, the best approach to the following four-dimensional problems is an analogy to, or a reduction to, spatial ones.

## 2 Parity Lemmas

As a specific goal of this subsection one can consider propositions 2.3.c, 2.5.b, 2.7.b, which illuminate the non-triviality of the material.

**Lemma 2.1** (parity). *If out of 6 vertices of two triangles in the plane, no 3 lie on a line, then the outlines of these triangles intersect each other at an even number of points.*

*Proof.* The outline of a triangle splits the plane.<sup>2</sup> The polygonal line formed by the sides of one triangle goes *inside* the other triangle as many times as it goes *outside*.  $\square$

Some points in the plane **are in general position**, if no 3 of them lie in the same line, and no three segments joining them have a common interior point.

**2.2.** (a) Are all the points of some circle in general position?

(b) If the vertices of two polygonal lines in the plane are in general position, then the polygonal lines intersect at a finite number of points.

Hint:  $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ .

**2.3.** (a) The plane is not a union of a finite number of lines.

(b) Are there 100 general position points in the plane?

(c) There are 14 general position points in the plane: 7 red and 7 yellow. Then the number of all the intersection points of the red segments (i.e., the segments joining the red points) with the yellow segments is even.

**Lemma 2.4** (Parity). *If no 4 among the 7 vertices of a triangle and a tetrahedron in 3-space lie in the same plane, then the outline of the triangle and the surface of the tetrahedron intersect at an even number of points.*

Some points in 3-space **are in general position**, if no 4 of them lie in the same plane, and no segment, triangle and triangle spanned by them have a common interior point. E.g. in general position are the 6 points in Figure 3.

**2.5.** (a) Are there 100 general position points in the 3-space?

(b) In the 3-space there are 17 general position points: 7 red and 10 yellow. Then the number of all the intersection points of the red segments (i.e., the segments joining the red points) with yellow triangles is even.

**Lemma 2.6** (Parity). *If no 5 among the 8 vertices of two tetrahedra in 4-space lie in the same hyperplane, then the surfaces of the tetrahedra intersect at an even number of points.*

---

<sup>2</sup>This fact, in contrast to the *piecewise linear Jordan theorem* [Sk20, §1.4], is proved without using the Parity Lemma.

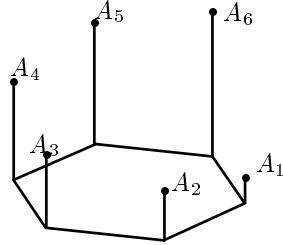


Figure 3: Six general position points in 3-space

Hint: Take the section by the hyperplane containing one of the tetrahedra.

Some points in 4-space **are in general position**, if no 5 of them lie in the same hyperplane, and no three triangles spanned by them have a common interior point.

**2.7.** (a) Are there 100 general position points in the 4-space?

(b) In the 4-space there are 16 general position points: 8 red and 8 yellow. We call *red/yellow* 2-dimensional triangles spanned by red/yellow points. Then the number of all the intersection points of the red triangles with the yellow triangles is even.

### 3 Quantitative versions

**Q = quantitative.** If no 3 of 4 points in the plane lie on a line, then there exists exactly one partition of these points into two subsets as in the above Radon theorem in the plane.

**QS:** the quantitative Radon theorem for same size sets in the plane; linear van Kampen-Flores theorem in the plane.

If no 3 of 5 points in the plane lie on a line, then the number of common interior points of the segments joining these 5 points is odd.

**QD:** the quantitative Radon theorem.

(3) If no 4 of 5 points in 3-space lie in a plane, then there exists exactly one partition of these points into two subsets whose convex hulls intersect.

(4) State and prove analogous result for 4-space and for  $d$ -dimensional space.

**Theorem QSD:** the quantitative Radon theorem for sets of almost the same size.

(3) *If no 4 of 6 points in 3-space lie in a plane, then the number of intersection points of interiors of segments joining pairs of points, and (2-dimensional) triangles spanned by these points, is even.*

(4) *If no 5 of 7 points in 4-space lie in a hyperplane, then the number of intersection points of (2-dimensional) triangles spanned by these 7 points is even.*

For a proof of Theorem QSD.4 you would need Theorem QS'D below.

The property of being linked is not symmetric a priori.

**Lemma 3.1** (Symmetry). *Triangles  $\Delta$  and  $\Delta'$  in 3-space are linked if and only if  $\Delta'$  and  $\Delta$  are linked.*

**3.2.** There are 13 points in 3-space: 3 red and 10 yellow. No 4 of them lie in a plane. Then the number of yellow triangles linked with red triangle is even. We call triangle *red* (*yellow*) if all of its vertices are red (*yellow*). Triangles which differ only by a permutation of vertices are considered to be the same.

**3.3.** In 3-space a segment  $p$  is *below* a segment  $q$  (looking from point  $O$ ), if there exists a half-line  $OX$  with the endpoint  $O$  that intersects the segment  $p$  at a point  $P := p \cap OX$ , the segment  $q$  at a point  $Q := q \cap OX$ ,  $P \neq Q$ , so that  $Q$  is in the segment  $OP$ .

Assume that no 4 of points  $O, A_1, \dots, A_5$  in 3-space lie in a plane, and there is a plane splitting  $O$  from  $A_1, \dots, A_5$ . The triangles  $OA_1A_2$  and  $A_3A_4A_5$  are linked if and only if  $A_1A_2$  is below an odd number of sides of the triangle  $A_3A_4A_5$ .

**Theorem QS'D:** the quantitative spatial Radon theorem on linking of same size sets.

*If no 4 of 6 points in 3-space lie in a plane, then the number of non-ordered pairs of linked triangles with vertices in these points is odd.*

Theorems SD and QSD show that under transition from dimension 2 to dimension 3 the property of the existence of intersection is preserved, while the parity of the number of intersections change. The odd-dimensional version of SD and QSD have a stronger form: Theorems S'D and QS'D.

The following unlinking properties are related to intersection properties QS, QSD.

**3.4.** (2) There are 5 points in the plane such that no 3 of them lie in a line, and every segment joining 2 of them intersects the outline of the triangle formed by the 3 remaining points at an even number of points.

(2') If no 3 of 5 points in the plane lie in a line, then the number of those segments joining 2 of them that intersect the outline of the triangle formed by the remaining 3 points exactly at one point, is even.

Assertion 3.4.2 means that every pair of points is ‘unlinked’ with the triangle formed by the remaining points. We do not spell out analogous interpretations of properties 3.5.3, 3.6.(4-2),(4-3) below.

In 3-space instead of unlinking properties 3.4 there is a linking property (Theorem QS'D from §3) and the following unlinking properties.

**3.5.** (3) There are 6 points in 3-space such that no 4 of them lie in a plane, and every segment joining 2 of them intersects the surface of the tetrahedron formed by the remaining 4 points at an even number of points.

(3') If no 4 of 6 points in 3-space lie in a plane, then the number of intersection points of segments joining them and surfaces of tetrahedra formed by the remaining 4 points, is even.

One can make a remark analogous to the one after Theorem QSD.

It would be interesting to prove the following statement 3.6.(4'-3), conjectures 3.6.(4-3),(4'-2),(4-2) and their higher-dimensional analogues. (We are grateful to M. Tancer for sending me proof of the PL version of 3.6.(4-3).)

**3.6.** (4'-3) If no 5 of 7 points in 4-space lie in a hyperplane, then the number of those triangles spanned by 3 of them that intersect exactly at one point the surface of the tetrahedron formed by the 4 remaining points, is even.

(4-3) There are 7 points in 4-space such that no 5 of them lie in a hyperplane, and every triangle formed by 3 of them intersects the surface of the tetrahedron formed by the 4 remaining points at an even number of points.

(4'-2) If no 5 of 7 points in 4-space lie in a hyperplane, then the number of intersection points of segments joining them and 3-dimensional surfaces of 4-dimensional simplices formed by the 5 remaining points, is even.

(4-2) There are 7 points in 4-space such that no 5 of them lie in a hyperplane, and every segment joining 2 of them intersects the 3-dimensional surface of the 4-simplex formed by the 5 remaining points at an even number of points.

## 4 Multiple versions (M)

**M = multiplicity.** Any 17 points in the plane can be split into three sets whose convex hulls have a common point.

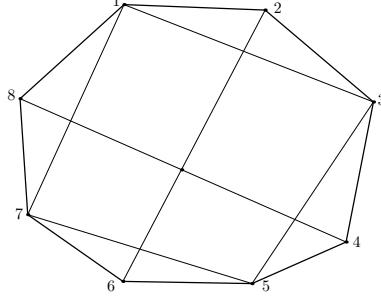


Figure 4: The common point of three convex hulls

*Proof.* The vertices of any convex octagon in the plane can be split into three sets whose convex hulls have a common point (fig. 4).

Suppose that the convex hull of the given set of 17 (or even 11) points has at least 8 vertices. Then split these 8 vertices into three sets as above. If the convex hull has less than 8 vertices, then denote by  $S_1$  the set of these vertices. There remain at least 4 points. Thus they can be split into two sets whose convex hulls intersect. This intersection lies in the convex hull of  $S_1$  as well.

**Theorem 4.1** (M:  $r$ -fold Radon theorem in the plane; the Tverberg theorem in the plane, 1965). *Any 7 points in the plane can be split into three sets whose convex hulls have a common point.*

*Any  $3r - 2$  points in the plane can be split into  $r$  sets whose convex hulls have a common point.*

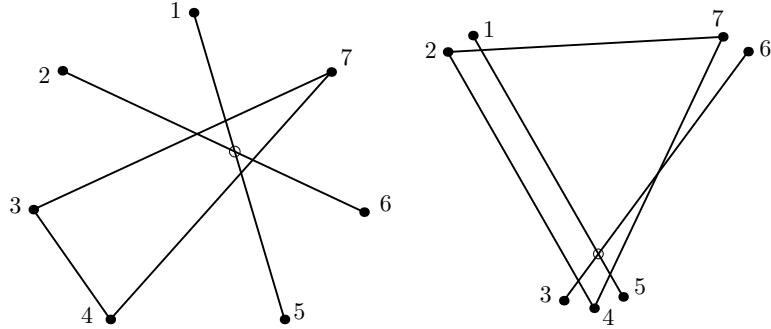


Figure 5: The common point of three convex hulls

Before proving Theorems M and DM, it is advisable to solve problems 4.2, 4.3, 4.4, 4.6.

**4.2** (cf. Theorem M). (a) There are 6 points in the plane such that any partition of the points into three sets the convex hulls of these sets do not have a common point.

*Hint.* Take a pair of points near each vertex of a triangle.

(b) There are 7 points in the plane no one of which lies in any triangle formed by any triple of the remaining points.

*Hint.* Take the vertices of a convex heptagon.

(c) There are 7 points in the plane with the following property. Take any two segments joining two disjoint pairs of the given 7 points. Then either the segments do not intersect or the point of their intersection does not lie in the triangle formed by the three remaining given points.

*Hint.* Take the vertices of an equilateral triangle and its center. Also take the middle-points of the segments joining the vertices and the center.

(d) State and prove  $r$ -fold versions of these examples.

*The quantitative 3-fold Radon theorem in the plane (QM) is unknown!*

**4.3.** Are there 6 points in the plane such that for any partition of these points into three sets the convex hulls of some two of these sets are disjoint?

**4.4.** (a) For the vertices of regular heptagon the number of partitions from Theorem M is 7.

*Hint.* Every such partition looks like a rotated partition of fig. 5, left.

(b) For the points in fig. 5, right, the number of partitions from Theorem M is 4.

*Hint.* This follows because for every such partition one of the convex hulls is a triangle with one vertex 4, another vertex 1 or 2, and the third vertex 6 or 7.

*Remark.* Hence the following sum has different parity for the two above 7-element sets  $M_a, M_b$

$$v(M_i) := \sum_{\{R_1, R_2, R_3\} : M_i = R_1 \sqcup R_2 \sqcup R_3} |\langle R_1 \rangle \cap \langle R_2 \rangle \cap \langle R_3 \rangle|.$$

See further [Sk18, §2].

**Theorem 4.5** (DM: spatial  $r$ -fold Radon theorem; the spatial Tverberg theorem, 1965). *Any  $4r - 3$  points in 3-space can be split into  $r$  sets whose convex hulls have a common point.*

**4.6** (cf. Theorem DM). (a) There are 8 points in 3-space such that for any partition of these points into three sets the convex hulls of these sets do not have a common point.

(b) There are  $4r - 4$  points in 3-space such that for any partition of these points into  $r$  sets the convex hulls of these sets do not have a common point.

(c) There are  $(r - 1)(d + 1)$  points in  $d$ -space such that for any partition of these points into  $r$  sets the convex hulls of these sets do not have a common point.

**4.7. \*** State and solve the spatial version of Problem 4.3.

In the proof of Theorems M and DM you can use without proof the Coloured Caratheodory Theorem (whose proof is not a part of this project).

**Theorem 4.8** (Barany; the Coloured Caratheodory Theorem). *Suppose that the point  $0 \in \mathbb{R}^n$  lies in the convex hull of every set among finite sets  $M_0, M_1, \dots, M_n \subset \mathbb{R}^n$ . Then there are points  $m_i \in M_i$  such that  $0 \in \langle m_0, m_1, \dots, m_n \rangle$ .*

**Theorem 4.9** (SM: low-dimensional 3-fold Radon theorem for same size sets; the linear Sarkaria theorem, 1991). \* *From any 11 points in 3-space one can choose three pairwise disjoint triples such that the three triangles formed by these triples have a common point.*

**4.10** (cf. Theorem SM). There are 10 points in 3-space such that there are no three pairwise disjoint triples of these points for which the three triangles formed by these triples have a common point.

**Theorem 4.11** (SDM:  $r$ -fold Radon theorem for arbitrary dimension for same-sized sets; the linear Sarkaria-Volovikov theorem, 1991-1996). \* *Let  $r$  be a prime power. From any  $(kr + 2)(r - 1) + 1$  points in  $\mathbb{R}^{kr}$  one can choose  $r$  pairwise disjoint sets such that each set contains  $k(r - 1) + 1$  points and the convex hulls of these sets have a common point.*

**It is unknown** whether the version of this theorem for  $r = 6$  is true!

*Quantitative versions (QSM), (QDM), (QSDM) are unknown*, even for  $r$  a prime power! *The version of (S'M) on 3-fold linking is unknown*, see [Skr].

For topological versions see [Sk18, §2], [Sk16].

# Answers, hints, solutions

**1.1.** 0, if they are parallel; 1, if the line intersects the plane;  $\infty$ , if the line is contained in the plane.

**1.4.** (a) The pair of the points  $(0, 0, 1)$  and  $(0, 0, -1)$ .

(b) The circumference  $\begin{cases} x = 0, \\ y^2 + z^2 = 1 \end{cases}$ .

(c) The union of three quarters of circumferences:

$$\begin{cases} x = 0, y \geq 0, z \geq 0 \\ y^2 + z^2 = 1 \end{cases}, \quad \begin{cases} y = 0, x \geq 0, z \geq 0 \\ x^2 + z^2 = 1 \end{cases} \quad \text{and} \quad \begin{cases} z = 0, x \geq 0, y \geq 0 \\ x^2 + y^2 = 1 \end{cases}$$

**1.5.** (a) The pair of the points  $(0, 0, 0, 1)$  and  $(0, 0, 0, -1)$ .

(b) The circumference  $\begin{cases} x = y = 0, \\ z^2 + t^2 = 1 \end{cases}$ .

(c) The sphere  $\begin{cases} x = 0, \\ y^2 + z^2 + t^2 = 1 \end{cases}$ .

(d) The graph  $K_4$  formed by the union of six quarters of circumferences, one of the quarters being  $\begin{cases} x = y = 0, z \geq 0, t \geq 0 \\ z^2 + t^2 = 1 \end{cases}$ .

**1.8.** (b) The empty set, a point (if the line intersects the plane), a line (if the line is contained in the plane).

(c) The empty set, a line (if the plane intersects the hyperplane), a plane (if the plane is contained in the hyperplane).

(d) The empty set, a plane (if they intersect), a hyperplane (if they coincide).

(e) The empty set, a point or a line (if they intersect), a plane (if they coincide).

**1.9.** (b) The empty set; (e) a point.

**2.2.** (a) No.

**2.3.** (c) The union of the red segments is the sum modulo 2 of the outlines of the red triangles. Also  $(A \oplus B) \cap C = (A \cap C) \oplus (B \cap C)$ .

**3.1.** Consider  $\Delta \cap \Delta'$ .

**3.3.** Since no 4 of the given points  $O, A_1, \dots, A_5$  lie in the same plane, the number of those sides of the triangle  $A_3A_4A_5$  that are higher than  $A_1A_2$  equals to the number of intersection points of the outline of the triangle  $A_3A_4A_5$  with the triangle  $OA_1A_2$ . Also, a segment cannot intersect a triangle by more than 2 points. All this implies the required assertion.

**3.5.** (3) Take points on a helix, see fig. 3.

(3') The property (3') is equivalent to Theorem QSD.3.

**QSD.** (3) We may assume that there is a unique ‘highest’ point  $O$  among the given ones. Consider a ‘horizontal’ plane slightly below the point  $O$ . Take the intersection of this plane with the segment  $OA_j$ , for every given point  $A_j$  (see figure 6). Then by QS there are 4 given points  $A, B, C, D$  such that the triangles  $OAB$  and  $OCD$  have a common point other than  $O$ . Now QSD.3 follows.

**S'D, QS'D.** We may assume that there is a unique ‘highest’ point  $O$  among the given ones. Consider a ‘horizontal’ plane  $\alpha$  slightly below the point  $O$ . Denote by  $A'_1, \dots, A'_5$  the intersection points of  $\alpha$  and segments joining  $O$  to other given points. In the plane  $\alpha$  we obtain a picture analogous to fig. 1, left.

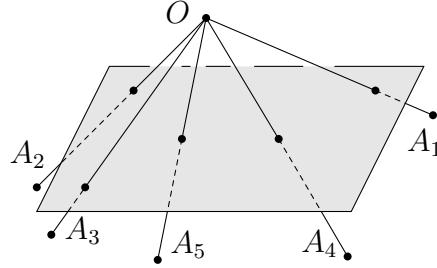


Figure 6: A plane in 3-space intersects the segments  $OA_j$  by 5 points.

Then the following numbers have the same parity:

- the number of linked unordered pairs of triangles formed by given points;
- the number of segments  $A_iA_j$  that are below an odd number of sides of their ‘complementary’ triangles  $A_kA_lA_m$ ,  $\{i, j, k, l, m\} = \{1, 2, 3, 4, 5\}$ ;
- the number of ordered pairs  $(A_iA_j, A_kA_l)$  of segments of which the first is below the second;
- the number of intersection points of segments whose vertices are  $A'_1, \dots, A'_5$ .

By QS the latter number is odd.

**SD.** (4) We may assume that there is a unique ‘highest’ point  $O$  among the given ones. Consider a ‘horizontal’ 3-dimensional hyperplane  $\alpha$  such that  $O$  and the other given points  $A_1, \dots, A_6$  lie on different sides of  $\alpha$ . For  $i = 1, \dots, 6$  denote by  $A'_i$  the intersection point of  $\alpha$  and the segment  $OA_i$  (see figure 7, left). Clearly, no 4 of the 6 points  $A'_1, \dots, A'_6$  lie in the same plane. Hence by Theorem S'D there are two linked triangles with vertices at these 6 points.

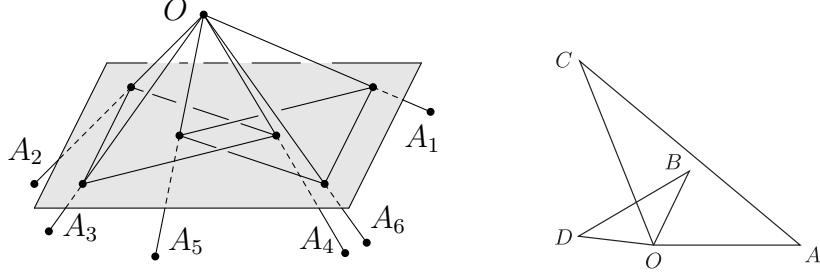


Figure 7: *Left:* a hyperplane in 4-space (shown as a plane in 3-space) intersects the segments  $OA_1, \dots, OA_6$  at 6 points  $A'_1, \dots, A'_6$  which are vertices of two linked triangles. *Right:* section by the plane  $\gamma$ :  $\Delta_1^\gamma = OAC$ ,  $\Delta_2^\gamma = OBD$ .

Denote by  $\Delta_1$  and  $\Delta_2$  the triangles formed by  $A_1, \dots, A_6$  so that the linked triangles are the intersections  $\alpha \cap O\Delta_1$  and  $\alpha \cap O\Delta_2$  of the hyperplane  $\alpha$  with tetrahedra  $O\Delta_1$  and  $O\Delta_2$  (e.g.  $\Delta_1 = A_2A_3A_4$  and  $\Delta_2 = A_1A_5A_6$ ). Denote by  $\gamma$  the plane containing  $O$  and the intersection line of the planes of the linked triangles. Then  $\gamma \cap \alpha$  is a line and  $\Delta_j^\gamma := \gamma \cap O\Delta_j$  is a triangle for  $j = 1, 2$  (see figure 7, right). The side of  $\Delta_j^\gamma$  not containing  $O$  is  $\gamma \cap \Delta_j$ . The two sides of  $\Delta_j^\gamma$  containing  $O$  form the intersection of  $\gamma$  and the lateral surface of the tetrahedron  $O\Delta_j$  (whose base is  $\Delta_j$ ).

Since the triangles  $\alpha \cap O\Delta_1$  and  $\alpha \cap O\Delta_2$  are linked, the intersection points of the line  $\gamma \cap \alpha$  and the outlines of  $\Delta_1^\gamma$  and  $\Delta_2^\gamma$  alternate along the line (see figure 1, right). Hence the outlines have a common point distinct from  $O$ .

This point is either the intersection of the sides  $\gamma \cap \Delta_1$  and  $\gamma \cap \Delta_2$  or, without loss of generality, of the side  $\gamma \cap \Delta_1$  and the union of the two sides of  $\Delta_2^\gamma$  containing  $O$ . In the first

case  $\Delta_1$  intersects  $\Delta_2$ . In the second case  $\Delta_1$  intersects the lateral surface of the tetrahedron  $O\Delta_2$ .

**QSD.** (4) The result is reduced to Theorem QS'D analogously to the proof of SD.4, by a simple additional counting analogous to the proof of Theorem QS'D below. We need the following assertion.

*For triangles  $\Delta_1$  and  $\Delta_2$  formed by  $A_1, \dots, A_6$  and having disjoint vertices, the number of intersection points of the surfaces of the tetrahedra  $O\Delta_1$  and  $O\Delta_2$  is even if and only if the triangles  $\alpha \cap O\Delta_1$  and  $\alpha \cap O\Delta_2$  are linked in  $\alpha$ .*

**4.6.** (a) Take a pair of points at each vertex of a tetrahedron.

(c) Take the union of sets of  $r - 1$  points at each vertex of a  $d$ -dimensional simplex.

## References

- [Ko18] \* *E. Kolpakov.* A proof of Radon Theorem via lowering of dimension, Mat. Prosveschenie, 23 (2018), arXiv:1903.11055.
- [RRS] \* *V. Retinskiy, A. Ryabichev and A. Skopenkov.* Motivated exposition of the proof of the Tverberg Theorem (in Russian). Mat. Prosveschenie, to appear. arXiv:2008.08361.
- [Sk14] \* *A. Skopenkov.* Realizability of hypergraphs and Ramsey link theory, arXiv:1402.0658.
- [Sk16] \* *A. Skopenkov,* A user's guide to the topological Tverberg Conjecture, Russian Math. Surveys, 73:2 (2018), 323–353. arXiv:1605.05141. Section 4 of the published version is available as *A. Skopenkov, On van Kampen-Flores, Conway-Gordon-Sachs and Radon theorems*, arXiv:1704.00300.
- [Sk18] \* *A. Skopenkov.* Invariants of graph drawings in the plane. Arnold Math. J., 6 (2020) 21–55; full version: arXiv:1805.10237.
- [Sk20] \* *A. Skopenkov.* Algebraic Topology From Geometric Viewpoint (in Russian), MC-CME, Moscow, 2020 (2nd edition). Electronic version: <http://www.mccme.ru/circles/oim/home/combttop13.htm#photo>
- [Sk] \* *A. Skopenkov.* Algebraic Topology From Algorithmic Viewpoint, draft of a book, mostly in Russian, <http://www.mccme.ru/circles/oim/algory.pdf>.
- [Skr] \* *A. Skopenkov.* Realizability of hypergraphs, slides for talks, [https://www.mccme.ru/circles/oim/algory1\\_beamer.pdf](https://www.mccme.ru/circles/oim/algory1_beamer.pdf).

*In this list books, surveys and expository papers are marked by stars*

# Фазовые пространства

проект представляют\*: Анастасия Еннэ, Андрей Плосконосов,  
Андрей Рябичев и Евгений Хинко

## Аннотация

В этом проекте мы предлагаем участникам ряд задач, для решения которых полезно ввести *фазовое пространство*. В части до промежуточного финиша мы демонстрируем большое количество примеров таких задач. В части после промежуточного финиша мы даём несколько сложных задач, для решения которых нужно глубоко исследовать геометрические и топологические свойства фазовых пространств, возникающих в них.

## 1 Задачи до промежуточного финиша

### 1.1 Введение

Во многих математических задачах бывает удобно рассмотреть “множество состояний” некоторой системы. Такое множество обычно называют *фазовым пространством* данной системы. Данные о состоянии системы могут включать не только координаты точек, но и, как это часто бывает в механике, их скорости.

Работать с возникающим в некой задаче фазовым пространством удобно не просто как с множеством точек, а вводя на нём дополнительную структуру. Например: геометрическую структуру (как на множестве точек плоскости); функцию расстояния между точками; понятие площади/объёма для подмножеств фазового пространства; отношение инцидентности (если фазовое пространство является собой множество вершин графа). Правильный выбор такой структуры может сильно упростить описание происходящего в задаче, тогда сама задача становится тривиальной.

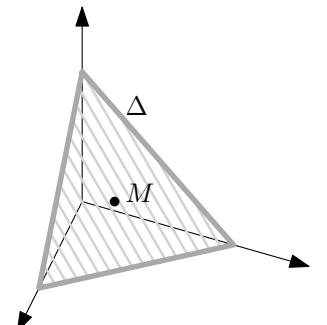
Рассмотрим следующий пример.

**Задача 0.** За столом сидят трое ребят, у каждого есть тарелка с кашей. Раз в минуту они одновременно делают следующее: каждый ребёнок делит кашу в своей тарелке пополам и перекладывает части двум другим. Докажите, что через несколько таких ходов у всех будет одинаковое количество каши с точностью до 1%.

*Решение.* Скажем, что общее количество каши равно 1. Обозначим через  $(x_1, x_2, x_3)$  набор чисел, соответствующий количеству каши в тарелках детей. Все возможные положения системы лежат в плоскости  $x_1 + x_2 + x_3 = 1$ . При этом  $x_1 \geq 0$ ,  $x_2 \geq 0$  и  $x_3 \geq 0$ . Таким образом, *наше фазовое пространство — правильный треугольник  $\Delta$  с вершинами  $(1, 0, 0)$ ,  $(0, 1, 0)$  и  $(0, 0, 1)$* .

Заметим, что преобразование

$$(x_1, x_2, x_3) \mapsto (y_1, y_2, y_3) = \left( \frac{x_2+x_3}{2}, \frac{x_1+x_3}{2}, \frac{x_1+x_2}{2} \right)$$



\*Мы благодарим за продуктивные обсуждения и ценные советы по улучшению проекта П. Бибикова, С. Дориченко, А. Канель-Белова, П. Кожевникова, А. Плахова, М. Скопенкова и Г. Челнокова.

есть не что иное, как гомотетия треугольника  $\Delta$  с коэффициентом  $-\frac{1}{2}$  относительно точки пересечения медиан  $M = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ . Проверьте это самостоятельно.

Отметим все положения системы, в которых у детей одинаковое количество каши с точностью до 1%. Полученное подмножество треугольника  $\Delta$  содержит маленький круг с центром в  $M$ . После достаточно большого числа итераций все точки  $\Delta$  окажутся внутри такого круга, откуда следует требуемое в задаче.  $\square$

## 1.2 Геометрическая вероятность

В каждой из следующих задач требуется формализовать понятие вероятности, и затем исходя из данного вами определения вычислить ответ.

**Задача 1** (Нетерпеливые дуэлянты). Два друга договорились встретиться между полуднем и часом дня, но не условились о точном времени встречи. Каждый из них приходит в случайный момент времени из указанного промежутка и ждёт другого 10 минут, а затем уходит. С какой вероятностью друзьям удастся встретиться?

**Задача 2.** Палочку ломают в двух случайных местах. С какой вероятностью из частей можно будет сложить треугольник? Сравните ответы для следующих способов *действовать случайно*:

- (a) выберем первую точку случайным образом, сломаем палочку в этой точке, выберем одну из двух частей равновероятно, и затем случайным образом выберем вторую точку разлома на ней;
- (b) независимо выберем две случайные точки и сломаем палочку в каждой из них;
- (c) выберем случайное представление длины палочки  $l$  в виде суммы трёх упорядоченных слагаемых  $l = x_1 + x_2 + x_3$  (ср. с задачей 0).

**Задача 3.** Марсоход разъезжает по ровной поверхности негостеприимной планеты (будем считать её плоской). Он выбирает случайное направление и проезжает в выбранном направлении километр. С какой вероятностью, сделав три таких итерации и проехав три километра, марсоход пересечёт свой след?

**Задача 4** (Игла Бюффона). Плоскость разлинована параллельными прямыми, расстояние между соседними равно 1 см. На плоскость бросают иголку длины 1 см. С какой вероятностью иголка пересечёт какую-нибудь из прямых?

## 1.3 Пространства конфигураций

**Задача 5.** На координатной плоскости нарисован многоугольник площади  $> 1$ . Докажите, что в нём найдутся две такие точки  $A$  и  $B$ , такие что обе координаты вектора  $AB$  целые.

**Задача 6.** На плоскости расположен многоугольник площади  $< 1$  и даны 1000 точек. Докажите, что многоугольник можно сдвинуть на вектор длины  $< \sqrt{\frac{1000}{\pi}}$  так, чтобы он не покрывал ни одну из точек.

**Задача 7.** Данна единичная сфера. *Большая окружность* — окружность радиуса 1, расположенная на сфере. *Ломаной на сфере* будем называть кривую, составленную из дуг больших окружностей.

- (a) На единичной сфере дана ломаная  $\gamma$  длины  $< \pi$ . Докажите, что найдётся большая окружность, не пересекающая  $\gamma$ .
- (b) На единичной сфере дана несамопересекающаяся ломаная  $\gamma$  длины  $> \pi k$ . Докажите, что найдётся большая окружность, пересекающая  $\gamma$  более чем в  $k$  точках и не содержащая ни одного ребра  $\gamma$ .

**Задача 8.** В пространстве расположены два тетраэдра. Для любой плоскости, проекции тетраэдров на неё либо обе являются треугольниками, либо обе являются четырехугольниками. Докажите что тетраэдры подобны.

**Задача 9.** На плоскости вбито  $k$  гвоздей. Проводятся прямые, не пересекающие ни один из гвоздей. Две прямые назовём эквивалентными, если одну из них можно переместить во вторую, не задев ни одного гвоздя. Тогда множество всех таких прямых разбивается на классы эквивалентности; каждый класс состоит из прямых, эквивалентных друг другу. Найдите (a) минимальное (b) максимальное число классов эквивалентности прямых для данного  $k$ .

**Задача 10.** В гонке по пересечённой местности участвуют 8 машин. Трасса представляет собой прямую дорогу, на которой есть несколько заболоченных участков. Каждая машина движется по сухим участкам дороги с постоянной скоростью (каждая со своей), а по заболоченным участкам — с другой постоянной скоростью (также каждая со своей).

Машины стартуют из одной точки, но в разное время, временные промежутки между стартаами могут различаться. На дистанции дежурят 500 судей. Каждый судья отметил, в каком порядке мимо него проехали машины, напротив судьи обгонов не происходило. Докажите, что мимо каких-то двух судей машины проехали в одинаковом порядке.

## 1.4 Дискретные фазовые пространства

**Задача 11.** Маша задумала двузначное число. Вася называет двузначные числа, его задача назвать число, отличающееся от числа Маши в каждом разряде не более чем на 1. Какого наименьшего числа ходов Васе заведомо хватит?

**Задача 12.** Маша задумала двузначное число. Теперь задача Васи — назвать число, совпадающее с числом Маши в одном разряде, а в другом отличающееся не более чем на 1. Хватит ли ему (a) 18 попыток; (b) 20 попыток; (c) 22 попыток?

**Задача 13.** По кругу расположено несколько ящиков, по ним некоторым образом разложены шарики. За один ход разрешается взять все шарики из любого ящика и разложить их, двигаясь по часовой стрелке, начиная со следующего ящика и кладя в каждый ящик по одному шарику.

(a) Докажите, что если на каждом следующем ходе шарики берут из того ящика, в который положили последний шарик на предыдущем ходе, то в какой-то момент повторится начальное размещение шариков.

(b) Докажите, что за несколько ходов из любого начального размещения шариков по ящикам можно получить любое другое.

**Задача 14.** (a) В одной из клеток бесконечной в обе стороны полоски стоит невидимый корабль. За ход разрешается делать один выстрел. После каждого хода корабль сдвигается на некоторое число клеток (число клеток и направление сдвига каждый раз одни и те же, но не известны игроку). Придумайте стратегию, позволяющую наверняка попасть в корабль.

(b) Та же задача на плоскости: корабль стоит в одной из клеток и каждый ход сдвигается на один и тот же неизвестный целочисленный вектор. Игрок делает по одному выстрелу за ход.

## 1.5 Избранные задачи

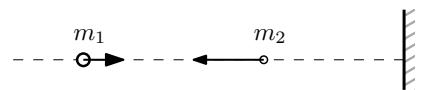
**Задача 15.** Даны три сосуда вместимостью 6, 7 и 12 литров. Два меньших сосуда заполнены. Можно ли отмерить 9 литров воды, переливая воду между сосудами?

**Задача 16.** Имеются три бассейна. Из первого с постоянной скоростью выливается вода, а во второй и третий бассейны вода поступает с постоянными скоростями. Изначально в первом

бассейне было столько же воды, сколько в двух других в сумме; через некоторое время во втором бассейне стало столько же воды, сколько в двух других в сумме; ещё через какое-то время в третьем бассейне стало столько же воды, сколько в первых двух в сумме. Возможно ли, что ни в начале, ни в конце этого промежутка времени ни один из бассейнов не был пустым?

**Задача 17** (Упрощённая модель «хищник-жертва»). В лесу живёт  $x$  зайцев и  $y$  волков. Будем считать, что если волков нет, то зайцы размножаются с постоянной скоростью  $a_0$ , если же в лесу  $y > 0$  волков, то они съедают  $a_1y$  зайцев каждую единицу времени (т. е.  $x'(t) = a_0 - a_1y$ ). Также будем считать, что если зайцев нет, то волки умирают с постоянной скоростью  $b_0$ , наличие же  $x > 0$  зайцев позволяет волкам размножаться со скоростью  $b_1x$  (т. е.  $y'(t) = -b_0 + b_1x$ ). Найдите зависимость количества зайцев и волков от времени. Для каких  $a_0$ ,  $a_1$ ,  $b_0$  и  $b_1$  эта зависимость периодична?

**Задача 18.** Два шарика с массами  $m_1$  и  $m_2$  движутся по прямой, как показано на рисунке. Между шариками, а также между шариками и стенкой, происходят упругие соударения.



- (a) Докажите, что между шариками за всё время произойдёт конечное число соударений.
- (b) Как количество соударений зависит от отношения начальных скоростей шариков и от их масс?

При соударениях шариков действуют закон сохранения импульса  $\sum m_i v_i = \text{const}$  и закон сохранения энергии  $\sum m_i v_i^2 = \text{const}$ . Удар о стенку происходит абсолютно упруго (с сохранением скорости). Можно считать, что шарик, ближайший к стенке, в начальный момент движется от неё.

# Указания и решения к задачам до промежуточного финиша

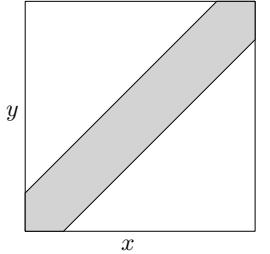
## Геометрическая вероятность

Для решения задач нам нужно определить понятие вероятности. Пусть  $X$  — многоугольник на плоскости, точки которого моделируют множество исходов в нашей задаче. Пусть  $A \subset X$  — некоторое подмножество. Будем говорить, что *вероятность попасть в  $A$*  равна отношению площади<sup>1</sup>  $A$  к площади  $X$ . В этой ситуации  $X$  мы называем *вероятностным пространством*, а его подмножества — *событиями*. Более подробное введение в теорию вероятностей см., например, в [Sh].

**Решение задачи 1.** Ответ:  $\frac{11}{36}$ .

Отождествим возможное время прихода человека с отрезком  $[0; 1]$ . Тогда время прихода двух людей отождествляется с квадратом  $[0; 1] \times [0; 1]$ . А именно, точке  $(x, y)$  соответствует ситуация, когда первый человек пришёл в момент  $x$ , а второй — в момент  $y$ .

Закрасим точки, соответствующие ситуациям, когда друзьям удастся встретиться. Они образуют полоску площади  $\frac{11}{36}$ .  $\square$

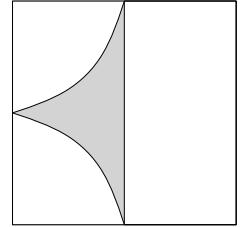
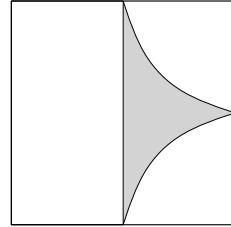


**Решение задачи 2. (a)** Ответ:  $\ln 2 - \frac{1}{2}$ .

Скажем, что при выборе первой точки разлома мы выбираем случайную точку на отрезке  $[0; 1]$ . Далее, отождествим каждую из получившихся частей с отдельной копией отрезка  $[0; 1]$ . Таким образом, наше вероятностное пространство состоит из двух квадратов (координата первого выбора откладывается в каждом из них по оси абсцисс, а координата второго выбора — по оси ординат).

Отметим точки  $X$ , соответствующие разломам, из которых можно сложить треугольник. Допустим, первый разлом делается в точке  $x \in [0; 1]$ . Затем мы выбрали первый из двух кусков, отождествили его с отрезком  $[0; 1]$  и выбрали на нём точку  $y$ . Из полученных трёх кусков можно сложить треугольник, если  $x > \frac{1}{2}$ ,  $xy < \frac{1}{2}$  и  $x(1-y) < \frac{1}{2}$ . Это подмножество имеет площадь

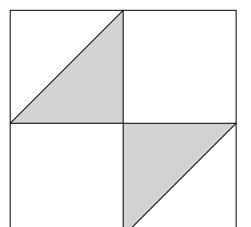
$$2 \int_{\frac{1}{2}}^1 \left( \frac{1}{2x} - \frac{1}{2} \right) dx = \ln 2 - \frac{1}{2}.$$



Подмножество второго квадрата, соответствующие разломам, из которых можно сложить треугольник, строится аналогично.

**(b)** Ответ:  $\frac{1}{4}$ .

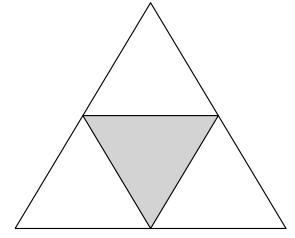
Отождествим палочку с отрезком  $[0; 1]$ . Выбор пары точек  $x, y \in [0; 1]$  задаёт точку в квадрате. Из полученных частей можно сложить треугольник, если  $x < y$  и при этом  $x < \frac{1}{2}$ ,  $y > \frac{1}{2}$  и  $y - x < \frac{1}{2}$ , либо если  $y < x$  и при этом  $x > \frac{1}{2}$ ,  $y < \frac{1}{2}$  и  $x - y < \frac{1}{2}$ . Площадь подмножества, заданного этими неравенствами, равна  $\frac{1}{4}$ .



<sup>1</sup>Вообще говоря, у произвольного подмножества  $A \subset X$  площадь может быть не определена; поэтому можно говорить лишь о вероятности попасть в «достаточно хорошее» подмножество, у которого площадь определена корректно.

(c) Ответ:  $\frac{1}{4}$ .

Вероятностное пространство в этой задаче можно отождествить с конфигурационным пространством из задачи 0. Из частей, полученных в результате разбиения, можно сложить треугольник, если  $x_1 < \frac{1}{2}$ ,  $x_2 < \frac{1}{2}$  и  $x_3 < \frac{1}{2}$ . Площадь этого подмножества составляет четверть площади треугольника.  $\square$

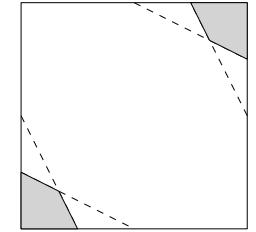


**Решение задачи 3.** Ответ:  $\frac{1}{12}$ .

Отождествим вероятностное пространство с квадратом  $[0; 2\pi] \times [0; 2\pi]$ , где координаты соответствуют величинам углов ломаной, по которой едет марсоход. Помимо границы  $x = 0$  и  $y = 0$  (которая имеет нулевую площадь), марсоход пересечёт свой след, если  $(x, y)$  — пара углов в некоем треугольнике, оба из которых не являются строго наибольшими, либо если  $(2\pi - x, 2\pi - y)$  — пара углов в некоем треугольнике, оба из которых не являются строго наибольшими. Это соответствует системам неравенств

$$\begin{cases} x \leq \pi - x - y, \\ y \leq \pi - x - y \end{cases} \quad \text{и} \quad \begin{cases} (2\pi - x) \leq \pi - (2\pi - x) - (2\pi - y), \\ (2\pi - y) \leq \pi - (2\pi - x) - (2\pi - y). \end{cases}$$

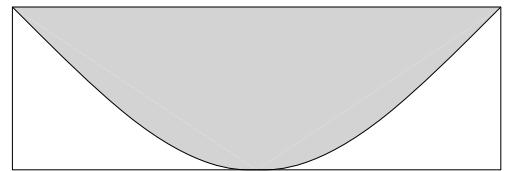
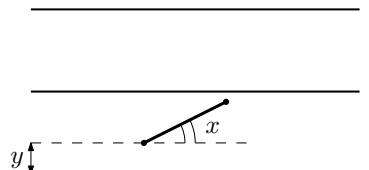
Каждая из них задаёт четырёхугольник, площадь которого составляет  $\frac{1}{24}$  от площади квадрата.  $\square$



**Решение задачи 4.** Ответ:  $\frac{2}{\pi}$ .

Для определённости будем считать прямые горизонтальными. Вероятностное пространство в этой задаче можно отождествить с прямоугольником  $[0; \pi] \times (0; 1]$ , где первая координата задаёт ориентированный угол иголки относительно прямых, а вторая координата показывает расстояние от нижнего конца иголки до ближайшей снизу прямой.

Тогда множество исходов, которые нас интересуют, задаётся неравенством  $1 - y \leq \sin x$ . Это множество имеет площадь  $\int_0^\pi \sin x dx = 2$ .  $\square$



## Пространства конфигураций

**Терминологическое замечание.** Пусть дано подмножество  $X$  евклидова пространства. Если мы отождествляем множество точек  $X$  с множеством расположений чего-либо (например, с множеством прямых на плоскости, или с множеством больших окружностей на сфере, или с множеством расстановок чисел с постоянной суммой), то  $X$  называется *пространством конфигураций*. Этот термин считается общепринятым и более удачным, чем термин «фазовое пространство», хотя по сути они имеют одинаковый смысл.

**Решение задачи 5.** Рассмотрим «решётку» прямых  $x = n$  и  $y = n$  для всевозможных  $n \in \mathbb{Z}$ . Она разбивает плоскость на квадраты. Назовём квадрат с вершинами  $(0, 0)$ ,  $(1, 0)$ ,  $(1, 1)$  и  $(0, 1)$  *базовым*. Очевидно, каждый квадрат получается из базового сдвигом на свой целочисленный вектор. Будем считать, что все квадраты выглядят как  $[0; 1] \times [0; 1]$ , т. е. не включают верхнюю и правую стороны.

Возьмём многоугольник из условия. Решётка разрезает его на конечное число частей. Сдвинем каждую часть на соответствующий целочисленный вектор так, чтобы все они оказались внутри базового квадрата. Фактически, мы построили *множество точек многоугольника, с точностью до целочисленного сдвига*.

Поскольку сумма площадей частей  $> 1$ , они не могут не накладываться внутри базового квадрата. В качестве  $A$  и  $B$  достаточно взять любую пару точек, которые совпадут после сдвига.

□

**Решение задачи 6.** Начертим вокруг каждой точки круг радиуса  $\sqrt{\frac{1000}{\pi}}$ . Закрасим в каждом круге точки многоугольника, которые в нём лежат. Затем при помощи параллельных переносов совместим все круги. Закрашенные точки покроют некоторую область  $P$ . Вектора от точек  $P$  до центра круга — это в точности те вектора, на которые нельзя сдвигать многоугольник.

Каждое закрашенное множество имело площадь  $< 1$ , значит площадь  $P$  составляет  $< 1000$ . Но круг имеет площадь ровно 1000, следовательно, в нём найдётся незакрашенная точка. Вектор между этой точкой и центром круга является искомым.

**Решение задачи 7.** Решение этой задачи использует важную идею, сходную с проективной двойственностью (см., например, [S]). Этот метод позволяет удобно работать с *множеством больших окружностей* на сфере. А именно, пусть сфера имеет центр в точке  $O$ . Любой точке  $A$  на сфере сопоставим большую окружность, лежащую в плоскости, проходящей через  $O$  перпендикулярной  $OA$ .

Это задаёт взаимно-однозначное соответствие между парами диаметрально противоположных точек сферы и большими окружностями. Будем называть это соответствие *двойственностью* и обозначать  $\delta$ . Отметим, что  $\delta(\delta(A)) = \pm A$  для любой точки  $A$  на сфере и  $\delta(\delta(\omega)) = \omega$  для любой большой окружности  $\omega$ . Кроме того, если точка  $A$  лежит на большой окружности  $\omega$ , то большая окружность  $\delta(A)$  содержит пару точек  $\delta(\omega)$ .

(a) Пусть имеется дуга  $\alpha$  большой окружности. Предположим,  $\alpha$  имеет длину  $\pi t$  для  $t \in (0; 1)$ . Возьмём большие окружности  $\delta(A)$  для всех  $A \in \alpha$ . Заметим, что объединение  $\delta(A)$  занимает долю  $t$  от площади сферы.

Ломаная  $\gamma$  из условия имеет длину  $< \pi$ . Поэтому большие окружности, двойственные к точкам  $\gamma$ , не покрывают всей сферы. Возьмём непокрытую точку  $B$ . Тогда большая окружность  $\delta(B)$  не пересекает  $\gamma$ .

(b) Доказательство аналогично. Для каждого ребра  $\gamma$  возьмём объединение больших окружностей, двойственных к его точкам. Мы получим пару «сферических долек». Поскольку длина  $\gamma$  больше  $\pi k$ , то объединение всех таких долек покрывает более  $k$  раз некоторую часть сферы, имеющую ненулевую площадь.

В частности, существует бесконечно много точек сферы, покрытых более чем  $k$  дольками. Отметим точки  $B_1, \dots, B_m$ , двойственные к продолжениям рёбер  $\gamma$ . Мы можем выбрать точку  $C$ , покрытую более чем  $k$  дольками и не совпадающую с  $B_1, \dots, B_m$ . Тогда большая окружность  $\delta(C)$  пересекает более чем  $k$  рёбер  $\gamma$  и не содержит ни одного из них.

**Указание к решению задачи 8.** Впишем каждый тетраэдр в сферу. Применим к ним параллельный перенос и гомотетию, чтобы сферы совпали.

Далее рассмотрите прямые  $l$ , проходящие через центр сферы, такие что проекции тетраэдров на плоскость, перпендикулярную  $l$ , являются треугольниками.

□

**Решение задачи 9.** Возьмём круг  $D$ , содержащий все гвозди. Если любая прямая из некоторого класса эквивалентности пересекает  $D$ , назовём этот класс эквивалентности *ограниченным*. Ясно, что есть ровно один класс, не являющийся ограниченным.

Проведём между гвоздями всевозможные отрезки, так что никакой отрезок не содержит гвоздей кроме концов. Можно отождествить *множество отрезков* с *множеством ограниченных классов эквивалентности прямых*. Для этого нужно поворачивать каждую прямую против часовой стрелки, пока она не упрётся в два гвоздя — эта пара гвоздей и будет концами отрезка, соответствующего классу эквивалентности данной прямой.

(a) Ответ:  $k$ .

Действительно, мы всегда сможем провести  $k - 1$  отрезок. Такое число отрезков реализуется, если все гвозди расположены на одной прямой.

**(б)** Ответ:  $C_k^2 + 1$ .

Число отрезков не больше числа рёбер в полном графе. Эта оценка достигается, если никакие три гвоздя не лежат на одной прямой.  $\square$

**Идея другого решения задачи 9.** Конфигурационное пространство  $X$  всех прямых в  $\mathbb{R}^2$  при помощи проективной двойственности отождествляется с  $\mathbb{RP}^2$  без одной точки. Выкинутая точка соответствует «бесконечно удалённой прямой». См., например, [S].

Множеству прямых, проходящих через точку  $A \in \mathbb{R}^2$ , при этом соответствует прямая в  $\mathbb{RP}^2$ . Таким образом задача сводится к тому, на сколько частей можно разрезать  $\mathbb{RP}^2$  с помощью  $k$  прямых (выкинутая точка на количество частей не влияет).  $\square$

**Решение задачи 10.** Пусть  $S$  — точка старта. Для каждой точки трассы  $A$  обозначим суммарную длину сухих участков от  $S$  до  $A$  через  $x$ , а суммарную длину заболоченных участков пути от  $S$  до  $A$  через  $y$ . Сопоставим точке  $A$  точку  $(x, y)$  на плоскости.

Нарисуем график движения каждой машины в пространстве с координатами  $x, y, t$ . Каждый график является ломаной. Заметим, что каждая такая ломаная лежит в некоторой плоскости  $t = t_0 + \frac{x}{u} + \frac{y}{v}$ ; здесь  $t_0$  — время прохождения точки  $S$ ,  $u$  и  $v$  — скорость машины на сухих и заболоченных участках соответственно. Обозначим эти плоскости  $\alpha_1, \dots, \alpha_8$ .

Нарисуем для судей вертикальные прямые  $l_1, \dots, l_{500}$ . Нам нужно показать, что точки пересечения некоторых двух прямых с плоскостями идут на этих прямых в одинаковом порядке.

Рассмотрим попарные пересечения плоскостей  $\alpha_i \cap \alpha_j$  и спроектируем на горизонтальную плоскость  $\beta$ . Мы получим не более чем  $C_8^2 = 28$  различных прямых. Они разбивают  $\beta$  не более чем на  $1 + C_{29}^2 = 407$  частей. По принципу Дирихле, какие-то две из прямых  $l_1, \dots, l_{500}$  проходят через одну и ту же часть.  $\square$

## Дискретные фазовые пространства

**Решение задачи 11.** Ответ: 12 ходов.

Отождествим каждое двузначное число с клеточкой в таблице  $9 \times 10$  (строки — десятки, столбцы — единицы). Если Вася называет число, оно покрывает квадрат  $3 \times 3$  в этой таблице. Но чтобы покрыть такими квадратами заштрихованные строки (все числа, начинающиеся на 2, на 5 и на 8), необходимо разместить 12 таких квадратов, то есть назвать минимум 12 чисел.

Пример легко построить, глядя на таблицу: пусть Вася назовёт числа 21, 24, 27, 29, 51, 54, 57, 59, 81, 84, 87 и 89.  $\square$

	0	1	2	3	4	5	6	7	8	9
1										
2										
3										
4										
5										
6										
7										
8										
9										

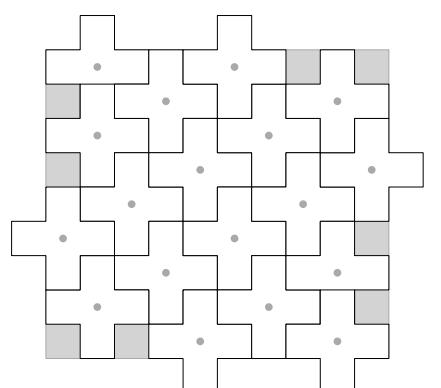
**Решение задачи 12.** Идея решения та же, только теперь нам нужно покрыть клетки прямоугольника  $9 \times 10$  «крестами», состоящими из пяти клеток.

**(а)** Ответ: Нет.

Действительно, если бы 18 крестов хватило, то они покрывали бы прямоугольник без наложений и не выходя за границы. Но это невозможно, например угловую клетку так покрыть не получится.

**(с)** Ответ: Да.

Разместим 18 крестов как на рисунке (для большей понятности отмечен центр каждого креста), а восемь непокрытых клеток покроем оставшимися 4 крестами.  $\square$



**Решение задачи 13. (а)** Текущее состояние описанной в задаче системы определяется количеством шариков в каждой коробочке и указанием коробочки, с которой нужно начинать раскладывать шарики в следующий раз. Поэтому возможных состояний системы конечное число.

Из каждого состояния можно, раскладывая шарики, перейти в другое состояние системы, которое определено однозначно. Наоборот, зная состояние системы в настоящий момент, можно однозначно определить состояние системы перед последним раскладыванием шариков. Действительно, последнее раскладывание должно было закончиться на выделенной коробочке; поэтому, чтобы восстановить предыдущее состояние, нужно взять один шарик из выделенной коробочки и далее, идя против часовой стрелки, брать по шарику из каждой коробочки, пока это возможно. Когда же мы встретим пустую коробочку, мы положим в неё все собранные шарики и объявим её отмеченной.

Построим *ориентированный граф состояний* системы. Для этого обозначим состояния системы точками, а возможность перехода из одного состояния в другое — стрелкой, соединяющей соответствующие точки. Из каждой точки будет выходить ровно одна стрелка и в каждую точку будет входить ровно одна стрелка.

Начнём двигаться по стрелкам, начиная с заданного состояния  $A_1$ . Получаем последовательность состояний  $A_2, A_3, \dots$ . Поскольку число состояний конечно, в некоторый момент в последовательности  $\{A_i\}$  возникнет повторение. Пусть, например,  $A_k = A_l$ , где  $k < l$ . Поскольку в точку  $A_k$  входит ровно одна стрелка, из равенства  $A_k = A_l$  следует  $A_{k-1} = A_{l-1}, \dots, A_1 = A_{l-k+1}$ . Тем самым, через  $l - k$  ходов мы вернулись в состояние  $A_1$ .

**(б)** В отличие от пункта (а) теперь состояние системы определяется лишь тем, как разложены шарики по коробочкам. Заметим, что если ход ведёт из состояния  $A$  в состояние  $B$ , то, согласно (а), мы можем (за несколько ходов) вернуться из  $B$  в  $A$ . Если мы можем попасть из состояния  $A$  в состояние  $C$  за несколько ходов, то мы можем вернуться из  $C$  в  $A$ , «откатывая» ходы по одному.

Таким образом, если мы научимся попадать из любого состояния в некоторое фиксированное состояние  $M$ , то сможем «путешествовать» между любыми состояниями, «проезжая» через  $M$ . Обозначим через  $M$  состояние, когда все шарики собраны в фиксированной коробочке  $m$ . Будем при каждой операции брать шарики из ближайшей (против часовой стрелки) к  $m$  непустой коробочки. Тогда либо число шариков в  $m$  увеличится, либо ближайшая к  $m$  непустая коробочка станет ещё ближе. Рано или поздно все шарики соберутся в  $m$ .  $\square$

**Указание к решению задачи 14.** Фазовое пространство в этой задаче — множество всевозможных пар  $(x, v)$ , где  $x$  — начальное положение корабля, а  $v$  — вектор, на который корабль сдвигается за один ход. Легко показать, что фазовое пространство счётно, а этого достаточно для построения алгоритма стрельбы.  $\square$

## Избранные задачи

**Указание к решению задачи 15.** Постройте конфигурационное пространство воды в сосудах, как в задаче 0, и рассмотрите изменение состояния при переливаниях. Подробное обсуждение см. в [CG, Гл. 4, §6].  $\square$

**Решение задачи 16.** Ответ: нет, невозможно.

Конфигурационное пространство количества воды в трёх бассейнах — подмножество  $X \subset \mathbb{R}^3$ , состоящее из точек с неотрицательными координатами. Точка, соответствующая текущему положению системы, движется по отрезку  $I$ , соединяющему начальное и конечное положение.

Пересечение плоскостей  $x+y = z$ ,  $y+z = x$  и  $z+x = y$  с  $X$  является границей бесконечного треугольного конуса. Поскольку конус выпуклый, отрезок  $I$  пересекает его границу не более чем в двух точках. Но по условию отрезок  $I$  содержит хотя бы по одной точке каждой грани. Следовательно,  $I$  проходит хотя бы через одно ребро конуса. Наконец, заметим, что рёбра конуса лежат на плоскостях  $x = 0$ ,  $y = 0$  и  $z = 0$ .  $\square$

**Решение задачи 17.** Конфигурационное пространство количества зайцев и волков — первый квадрант плоскости  $\mathbb{R}^2$ . Обозначим его  $X$ . Положение системы меняется со временем, точка с положительными координатами  $(x, y)$  движется с вектором скорости  $(a_0 - a_1 y, -b_0 + b_1 x)$ .

Заметим, что в точке  $(\frac{b_0}{b_1}, \frac{a_0}{a_1})$  вектор скорости нулевой. Сдвинем начало координат в эту точку. Тогда сопоставление каждой точке её вектора скорости будет линейным отображением  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ . Заметим, что это линейное отображение переводит ось  $x$  в ось  $-y$ , а ось  $y$  — в ось  $x$ . Растворив оси в нужное количество раз, можно сделать его композицией поворота на  $90^\circ$  и гомотии.

А именно, сделаем линейную замену переменных, положив

$$\tilde{x} = \frac{-b_0 + b_1 x}{\sqrt{b_1}} \quad \text{и} \quad \tilde{y} = \frac{-a_0 + a_1 y}{\sqrt{a_1}}.$$

В этих координатах вектор скорости точки  $(\tilde{x}, \tilde{y})$ , не лежащей на границе  $X$ , записывается как  $\sqrt{a_1 b_1} \cdot (-\tilde{y}, \tilde{x})$ . Это значит, что все такие точки движутся по окружностям с центром в начале координат.

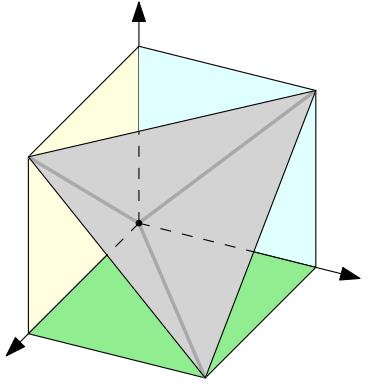
Таким образом, движение всех точек, чьи окружности не пересекают границу  $X$ , периодично. Если точка попадает на границу  $X$ , то дальше она движется по ней с постоянной скоростью. То есть, не периодично движение точек, для которых

$$\tilde{x}^2 + \tilde{y}^2 \leq \min \left( \frac{b_0^2}{b_1}, \frac{a_0^2}{a_1} \right),$$

то есть расстояние до начала координат (в новых координатах) не больше расстояния до хотя бы одной из прямых  $x = 0$  и  $y = 0$ .  $\square$

**Решение задачи 18. (а)** Будем следить лишь за *скоростями* шариков. В пространстве с координатами  $v_1, v_2$  закон сохранения энергии  $m_1 v_1^2 + m_2 v_2^2 = \text{const}$  задаёт эллипс. Для удобства можно умножить координаты на положительные числа так, чтобы этот эллипс стал окружностью.

А именно, положим  $x = \sqrt{m_1} \cdot v_1$  и  $y = \sqrt{m_2} \cdot v_2$ . (Первый шарик — дальний от стенки, скорость считается положительной, если она направлена к стенке.) Из закона сохранения энергии, точки, соответствующие положениям системы, лежат на окружности  $x^2 + y^2 = \text{const}$ . Эта окружность будет нашим фазовым пространством, обозначим её  $X$ .



При соударении между шариком и стенкой в фазовом пространстве происходит преобразование  $(x, y) \mapsto (x, -y)$ , т. е. отражение относительно прямой  $l$ , заданной как  $y = 0$ . Отметим, что соударение может произойти только если  $v_2 > 0$ , т. е.  $y > 0$ .

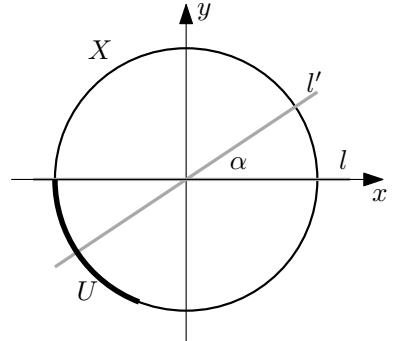
При каждом соударении между шариками в фазовом пространстве происходит отражение относительно прямой, проходящей через начало координат и точку  $(\sqrt{m_1}, \sqrt{m_2})$ . Это следует из закона сохранения импульса. Назовём эту прямую  $l'$ , она задаётся как  $\frac{x}{\sqrt{m_1}} = \frac{y}{\sqrt{m_2}}$ . Отметим, что соударение может произойти только если  $v_1 > v_2$ , т. е.  $\frac{x}{\sqrt{m_1}} > \frac{y}{\sqrt{m_2}}$ .

Обозначим угол между  $l$  и  $l'$  через  $\alpha$ . Нам известно, что  $\alpha = \operatorname{arctg} \frac{\sqrt{m_2}}{\sqrt{m_1}}$ . Очевидно, композиция двух описанных преобразований  $X$  является поворотом на угол  $-2\alpha$ .

Отметим на окружности дугу  $[\pi; \pi + 2\alpha]$ , обозначим её  $U$ . Рано или поздно любая точка попадёт в область  $U$ . В таком положении системы не произойдёт ни одного соударения со стенкой.

**(b)** Пусть  $(x_0, y_0)$  — начальное положение системы. Из условия,  $y_0 < 0$ . Определим  $\beta$  как угол вектора  $(x_0, y_0)$ . Формально,  $\beta = \operatorname{arctg} \frac{x_0}{y_0} - \pi$ . Тогда число соударений между шариками равно  $\lceil \frac{\pi + \beta - \alpha}{2\alpha} \rceil$ , а число соударений между вторым шариком и стенкой равно  $\lceil \frac{\pi + \beta - 2\alpha}{2\alpha} \rceil$ .

К этой задаче мы можем посоветовать дополнительные материалы на YouTube: обзорное видео [1], где говорится о связи этой задачи со знаками в десятичной записи числа  $\pi$ , видео [2] с решением в пространстве скоростей, а также видео [3] с решением через бильярды в пространстве координат.  $\square$



# Задачи после промежуточного финиша

Задачи здесь разделены на два независимых сюжета. В разделе 2 мы изучаем различные топологические свойства фазовых пространств, возникающих в задачах с довольно простыми формулировками. В разделе 3 мы сталкиваемся с геометрией фазовых пространств, а именно — с преобразованиями, сохраняющими объём. *По причине обширности этих сюжетов участникам предлагается сосредоточить свои усилия лишь на одном из них.*

Основными результатами §2 являются задачи 20<sup>m</sup> и 22<sup>m</sup>, основными результатами §3 — задачи 42<sup>m</sup> и 51<sup>m</sup>. Задачи, отмеченные звёздочками, требуют некоторой техники (такой как непрерывные отображения); если вы не знаете соответствующих формальных определений, то решать эти задачи не нужно.

Иногда в качестве подсказок к сложным задачам мы формулируем леммы. Эти леммы говорят многое о природе рассматриваемых объектов, и поэтому могут быть интересны сами по себе. Доказательства этих лемм, в свою очередь, разбиваются на задачи, которые размещаются после их формулировки.

Также для справки мы приводим формулировки некоторых теорем; их доказательства сдавать не нужно.

## 2 Топология фазовых пространств

### 2.1 Задача про возы

**Задача 19.** В 9:00 турист вышел из дома, он шёл весь день и к 21:00 пришёл на место стоянки. Переночевав, на следующий день турист с 9:00 до 21:00 шёл обратно по той же дороге. Он идёт с непостоянной скоростью, может иногда останавливаться или даже возвращаться назад. Докажите, что в некотором месте дороги турист в разные дни находился в одно и то же время.

**Задача 20<sup>m</sup>** (Н. Н. Константинов). Из города  $A$  в город  $B$  ведут две непересекающиеся дороги. Известно, что две машины, связанные веревкой длины 10 метров, смогли проехать из  $A$  в  $B$  по разным дорогам, не порвав веревки. Могут ли разминуться, не коснувшись, два круглых воза с сеном, имеющие радиус 6 метров и движущиеся по разным дорогам навстречу друг другу?

Ниже мы наметим путь *формального* решения задачи 20<sup>m</sup> для *кусочно-линейного* движения машин и возов. Это значит, что временной отрезок должен быть разбит на конечное число частей, скорости машин и возов на каждой из которых постоянны. Тогда для решения задачи 20<sup>m</sup> можно доказать следующее вспомогательное утверждение.

**Лемма 1.** В квадрате  $ABCD$  нарисованы две ломаные  $\alpha$  и  $\beta$ . Ломаная  $\alpha$  соединяет вершины  $A$  и  $C$ , а ломаная  $\beta$  — вершины  $B$  и  $D$ . Тогда  $\alpha \cap \beta \neq \emptyset$ .

Ломаные могут самопересекаться, если не оговорено противное.

Почему мы не рассматриваем *непрерывные* кривые вместо ломаных? Разницу в обращении с ними иллюстрирует следующая задача (ответы в пунктах (a) и (b) разные).

**Задача 21.** Среди ровной степи стоит гора. На вершину ведут две тропы, не опускающиеся ниже уровня степи. Два альпиниста одновременно начали подъём по разным тропам, соблюдая условие: в каждый момент времени быть на одинаковой высоте. Смогут ли альпинисты достичь вершины, двигаясь непрерывно, если (a) тропы являются ломаными; (b\*) тропы могут быть произвольными графиками непрерывных функций?

(c) Решите аналог пункта (a) для произвольного числа альпинистов.

Лемма 1 кажется очевидной, но строго доказать её оказывается не так просто. Указания к доказательству см. в §2.3.1.

## 2.2 Прямоугольник, вписанный в кривую

**Задача 22<sup>m</sup>.** Данна замкнутая несамопересекающаяся кривая на плоскости. Докажите, что существует прямоугольник, вершины которого лежат на этой кривой.

Возьмём на плоскости точки  $A = (0, 0)$ ,  $B = (1, 0)$ ,  $C = (1, 1)$  и  $D = (0, 1)$ . Можно определить ленту Мёбиуса как квадрат  $ABCD$  (с внутренностью), в котором стороны  $AD$  и  $CB$  отождествлены посредством отображения  $(0, t) \mapsto (1, 1-t)$ . Будем обозначать ленту Мёбиуса  $M$ .

Для доказательства задачи 22<sup>m</sup> будут полезны следующие два утверждения.

**Задача 23.** Отождествите с  $M$  конфигурационное пространство пар точек на окружности.

**Лемма 2.** Не существует непрерывного вложения  $M \rightarrow \mathbb{R}^3$ , такого что граница  $M$  лежит в плоскости  $z = 0$ , а все остальные точки — в полупространстве  $z > 0$ .

(Под “вложением” здесь понимается отображение, при котором разные точки  $M$  переходят в разные точки  $\mathbb{R}^3$ .)

Вообще говоря, Лемма 2 использует понятие непрерывности, аккуратное обращение с которым выходит далеко за рамки проекта. Тем не менее, мы можем строго доказать кусочно-линейную версию Леммы 2. Пояснения и указания к доказательству см. в §2.3.2.

## 2.3 Топологические леммы

### 2.3.1 Замкнутые кривые на плоскости

Основной целью этого раздела является доказательство Леммы 1.

**Определение.** Набор точек плоскости называется *набором общего положения*, если

- (1) никакие три из них не лежат на одной прямой и
- (2) никакие 6 из них нельзя покрыть тройкой прямых, проходящих через одну точку (не обязательно принадлежащую набору).

**Задача 24.** Верно ли, что если набор точек плоскости содержит хотя бы 6 точек, то условие (1) из определения выше следует из условия (2)?

**Задача 25.** Покажите, что любой конечный набор точек плоскости можно сделать набором общего положения посредством сколь угодно малого шевеления (то есть, сдвинув каждую точку не более чем на заранее указанное расстояние).

**Задача 26.** Дан квадрат  $ABCD$  и ломаные  $\alpha = A_0A_1\dots A_m$  и  $\beta = B_0B_1\dots B_n$ , где  $A_0 = A$ ,  $B_0 = B$ ,  $A_m = C$ ,  $B_n = D$  и остальные вершины лежат внутри квадрата. Предположим, множество всех вершин ломаных находится в общем положении. Тогда число точек пересечения  $\alpha$  и  $\beta$  нечётно. (Указание: используйте индукцию по  $m$  и  $n$ .)

**Задача 27.** Верно ли утверждение задачи 26, если для множество вершин  $\alpha$  и  $\beta$  (a) условие (1) из определения набора общего положения не выполняется, или (b) условие (1) выполняется, а условие (2) не выполняется?

**Задача 28. (a)** Докажите Лемму 1. **(b\*)** Докажите аналог Леммы 1 для непрерывных кривых.

Аналогичным образом, из задачи 26 можно вывести следующее утверждение.

**Теорема Жордана.** Будем говорить, что подмножество плоскости  $A$  *связно*, если между любыми двумя его точками существует ломаная, целиком лежащая внутри  $A$ . Тогда (a) любая замкнутая несамопересекающаяся ломаная разбивает плоскость на части (т. е. дополнение плоскости до этой ломаной не является связным); (b) более того, этих частей ровно две.

### 2.3.2 Зацепленность замкнутых кривых в пространстве

Основной целью этого раздела является доказательство Леммы 2.

**Определение.** Набор точек пространства называется *набором общего положения*, если  
 (1) никакие три точки не лежат на одной прямой,  
 (2) никакие четыре точки не лежат в одной плоскости и  
 (3) никакие 8 из них нельзя покрыть парой плоскостей и прямой, проходящими через одну точку (не обязательно принадлежащую набору).

Говорят, что ломаные в пространстве *находятся в общем положении*, если множество их вершин — набор точек общего положения.

**Задача 29.** Покажите, что любой конечный набор точек в пространстве можно сделать набором общего положения посредством сколь угодно малого шевеления.

**Задача 30.** Покажите, что если объединение множества вершин замкнутой ломаной в пространстве и вершин произвольного тетраэдра является набором общего положения, то количество точек пересечения ломаной с поверхностью тетраэдра чётно.

**Определение.** Пусть  $\alpha, \beta \subset \mathbb{R}^3$  — две замкнутые ломаные в общем положении. Возьмём точку  $O \in \mathbb{R}^3$  в общем положении с их вершинами. Пусть  $A_0, A_1, \dots, A_n = A_0$  — вершины  $\alpha$ . Для  $i = 0, \dots, n - 1$  посчитаем остаток по модулю 2 для числа точек пересечения треугольника  $OA_iA_{i+1}$  и ломаной  $\beta$ . Сумма  $n$  полученных остатков называется *коэффициентом зацепления*  $\alpha$  и  $\beta$  по модулю 2. Обозначение:  $\text{lk}(\alpha, \beta)$ .

**Задача 31. (а)** Покажите, что  $\text{lk}(\alpha, \beta)$  не зависит от выбора точки  $O$ . (Указание: возьмите точку  $O'$  и рассмотрите пересечение тетраэдров  $OO'A_iA_{i+1}$  и ломаной  $\beta$ .)

**(б)** Покажите, что  $\text{lk}(\alpha, \beta) \equiv \text{lk}(\beta, \alpha)$ . (Символом  $\equiv$  мы обозначаем сравнимость по модулю 2.)

**Задача 32.** Пусть  $\alpha, \beta \subset \mathbb{R}^3$  — пара непересекающихся и несамопересекающихся замкнутых ломаных.

**(а)** Докажите, что существует  $\varepsilon > 0$ , такое что при любом сдвиге каждой вершины  $\alpha$  и  $\beta$  меньше чем на  $\varepsilon$  ломаные останутся непересекающимися и несамопересекающимися.

**(б)** Пошевелив вершины  $\alpha, \beta$  меньше чем на  $\varepsilon$ , можно получить пару ломаных общего положения  $\alpha', \beta'$ . Докажите, что,  $\text{lk}(\alpha', \beta')$  корректно определён, т. е. не зависит от этого сдвига.

Задача 32 позволяет определить коэффициент зацепления по модулю 2 для *произвольной* пары непересекающихся и несамопересекающихся замкнутых ломаных  $\alpha, \beta \subset \mathbb{R}^2$ . Будем говорить, что  $\alpha$  и  $\beta$  *зацеплены по модулю 2*, если  $\text{lk}(\alpha, \beta) \equiv 1$ .

Для простого доказательства Леммы 2 удобно использовать следующее свойство графа  $K_6$  (полного графа на 6 вершинах). Отображение  $K_6 \rightarrow \mathbb{R}^3$  будем называть *кусочно-линейным*, если образы всех рёбер являются ломаными.

**Лемма 3.** Для любого кусочно-линейного вложения  $K_6 \rightarrow \mathbb{R}^3$  найдётся пара непересекающихся циклов, зацепленных по модулю 2.

**Задача 33.** Для кусочно-линейного вложения  $\gamma : K_6 \rightarrow \mathbb{R}^3$  обозначим  $\text{slk}(\gamma)$  сумму коэффициентов зацепления по модулю 2 для всех пар непересекающихся циклов. Постройте какое-нибудь вложение  $\gamma_0 : K_6 \rightarrow \mathbb{R}^3$  и убедитесь, что  $\text{slk}(\gamma_0) \equiv 1$ .

**Задача 34.** Пусть кусочно-линейные вложения  $\gamma_1, \gamma_2 : K_6 \rightarrow \mathbb{R}^3$  совпадают на всех рёбрах, кроме одного. Докажите, что  $\text{slk}(\gamma_1) \equiv \text{slk}(\gamma_2)$ .

**Задача 35.** Выполните Лемму 3.

### 2.3.3 Вложения ленты Мёбиуса в пространство

Триангуляцией ленты Мёбиуса  $M$  называется граф  $\Gamma \subset M$ , все грани которого — треугольники. Отметим, что при этом граница  $M$  целиком состоит из рёбер. Отображение  $f : M \rightarrow \mathbb{R}^3$  называется *кусочно-линейным*, если для некоторой триангуляции  $M$  отображение  $f$  переводит её грани в треугольники в  $\mathbb{R}^3$ .

**Задача 36.** (a) Вложите  $K_6$  в  $M$  так, чтобы одним из циклов была граница  $M$ , а другим циклом была средняя линия  $M$ . Назовём эти циклы  $\alpha$  и  $\beta$ .

(b) Покажите, что если задано вложение  $f : M \rightarrow \mathbb{R}^3$ , то никакие циклы в  $f(K_6)$ , кроме  $f(\alpha)$  и  $f(\beta)$ , не будут зацеплены.

**Задача 37.** Пусть задано кусочно-линейное вложение  $f : M \rightarrow \mathbb{R}^3$ . Обозначим  $\alpha$  границу  $M$ , а  $\beta$  — среднюю линию  $M$ . Докажите, что  $f(\alpha)$  и  $f(\beta)$  — зацепленные ломаные в  $\mathbb{R}^3$ .

**Задача 38.** Выведите из задачи 37 Лемму 2 для кусочно-линейного вложения  $M \rightarrow \mathbb{R}^3$ .

**Задача 39\*.** Докажите Лемму 2 для непрерывного вложения  $M \rightarrow \mathbb{R}^3$ .

## 3 Зеркала и билльярды

### 3.1 Невидимая система зеркал

В этом разделе мы рассматриваем *системы зеркал* — наборы кривых на плоскости. Для лучей выполняется закон “угол падения равен углу отражения”; зеркала могут быть искривлёнными, тогда этот закон применяется к касательной к зеркалу в точке падения луча. Лучами, попадающими в края зеркал, можно пренебречь. Система зеркал должна быть ограниченной. Все зеркала не могут быть параллельными отрезками.

**Задача 40.** Постройте систему зеркал, (a) невидимую в каком-нибудь направлении; (b) невидимую в каких-нибудь двух направлениях.

*Невидимость в направлении* прямой  $l$  означает, что каждый луч, параллельный  $l$  и начинавшийся достаточно далеко, несколько отражений спустя продолжает идти по той же прямой, как если бы он ни от чего не отражался.

**Задача 41.** (a) Предположим, все зеркала системы являются отрезками и расположены под углами  $0^\circ$  и  $90^\circ$ . Докажите, что такая система зеркал не может быть невидимой с направлений  $45^\circ$  и  $135^\circ$ . Углы измеряются по отношению к оси  $x$ .

(b) Предположим, все зеркала системы являются отрезками и расположены только под углами  $0, \frac{\pi}{n}, \frac{2\pi}{n}, \dots, \frac{(n-1)\pi}{n}$  для некоторого натурального  $n$ . Назовём такие направления *допустимыми*.

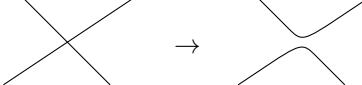
Пусть задано конечное множество прямых  $l_1, \dots, l_k$ , такое что при отражении любой прямой  $l_i$  относительно прямой, идущей в допустимом направлении, полученная прямая будет параллельна некоторой  $l_j$ . Докажите, что такая система зеркал не может быть невидимой с направлений  $l_1, \dots, l_k$ .

**Задача 42<sup>m</sup>.** Докажите, что не существует системы зеркал, невидимой во всех направлениях.

Для решения задачи 42<sup>m</sup> можно рассмотреть преобразование фазового пространства, сохраняющее объём. Такие преобразования рассматриваются далее на более простых примерах в задачах 46 и 50. Другой приём, который понадобится в решении задачи 42<sup>m</sup>, проиллюстрирован на следующем дискретном примере.

**Задача 43.** Некоторый остров имеет форму круга  $D$ . На границе  $D$  находятся  $2n$  транспортных узлов, принадлежащих  $n$  компаниям. Каждой компании принадлежит 2 узла, их соединяет прямая железная дорога, по которой поезда ездят из конца в конец. На пересечении железных дорог установлены мосты, так что любой поезд движется по прямой и не может сворачивать.

Министр путей сообщения захотел уменьшить число мостов, заменив их на повороты, как на рисунке.



При этом требуется, чтобы каждый поезд продолжал ездить между транспортными узлами одной и той же компании. Докажите, что министру не удастся это сделать.

### 3.2 Внешние бильярды

Пусть  $T$  — выпуклая ограниченная фигура на плоскости  $\mathbb{R}^2$ . Возьмём точку  $x_0$  вне  $T$ . Из  $x_0$  существует две опорные (касательные) прямые к  $T$ . Выберем правую из этих прямых, если смотреть из  $x_0$ , обозначим её  $l$ . Если  $l$  пересекает  $T$  в одной точке  $y_1$ , обозначим через  $x_1$  образ точки  $x_0$  при отражении относительно  $y_1$ .

Аналогичным образом, по точке  $x_1$  строится (при условии, что правая опорная прямая из  $x_1$  пересекает  $T$  в единственной точке) следующая точка  $x_2$ , и т. д. Отображение  $R$ , переводящее точку на плоскости в её образ, называется *отображением внешнего бильярда*, а последовательность  $x_0, x_1, x_2, \dots$  называется *орбитой точки*  $x_0$ .

Если на каком-то шаге очередная опорная прямая пересекает границу  $T$  не в одной точке, а по отрезку, будем считать, что орбита  $x_0$  не определена.

**Задача 44.** Пусть  $T$  — квадрат на плоскости. **(а)** Нарисуйте множество точек, для которых определены орбиты. **(б)** Докажите, что все орбиты для этого бильярда конечны. **(с)** Как по точке  $\mathbb{R}^2$  определить длину её орбиты?

**Задача 45.** Решите ту же задачу, если  $T$  — произвольный треугольник на плоскости.

**Задача 46.** Докажите, что отображение  $R$  сохраняет площадь (т. е. для любой фигуры  $A$ , не пересекающей  $T$ , площади  $A$  и  $R(A)$  равны), **(а)** если  $T$  — выпуклый многоугольник; **(б)** если  $T$  — произвольная строго выпуклая ограниченная фигура.

Назовём орбиту  $x_0, x_1, x_2, \dots$  *почти периодической*, если для любого  $\varepsilon > 0$  существует натуральное  $n$ , такое что расстояние между  $x_0$  и  $x_n$  меньше  $\varepsilon$ .

**Задача 47\*.** Верно ли, что любая орбита внешнего бильярда  $T$  почти периодична, если

- (а)**  $T$  — выпуклый многоугольник с рациональными вершинами;
- (б)**  $T$  — произвольный выпуклый многоугольник;
- (с)**  $T$  — строго выпуклая ограниченная фигура;
- (д)**  $T$  — произвольная выпуклая ограниченная фигура?

Простое решение этой задачи нам не известно. Однако ответ на аналогичный вопрос для внутренних бильярдов куда более прост, как мы увидим в следующем разделе.

### 3.3 Внутренние бильярды

Пусть  $T$  — выпуклая ограниченная фигура на плоскости. Возьмём точку  $x$  внутри  $T$  и зададим отложенный от  $x$  единичный вектор скорости. Это определяет движение точки  $x$  в зависимости от времени: внутри  $T$  точка  $x$  движется по прямой, а на границе происходит отражение по закону “угол падения равен углу отражения” (углы меряются с касательной к границе  $T$  в точке соударения).

Если в какой-то момент  $x$  попадает в точку на границе  $T$ , в которой не существует касательной, будем считать, что орбита  $x$  не определена. Орбита точки  $x$  называется *периодической*, если через некоторое время  $x$  оказывается на изначальном месте и имеет изначальную скорость.

**Задача 48.** Пусть  $T$  — квадрат. **(а)** Для каких начальных точек и векторов скорости орбиты будут периодическими? **(б)** Покажите, что любая периодическая орбита в  $T$  имеет чётное число отражений относительно границы.

Далее  $T$  можно считать либо выпуклым многоугольником, либо произвольной выпуклой ограниченной фигуруй с гладкой границей.

**Задача 49.** Зададим для всех точек равные вектора скорости. Обозначим положение точки  $x$  спустя время  $t$  через  $f_t(x)$ . Покажите, что для фигуры  $A \subset T$  образ  $f_t(A)$  не обязательно имеет такую же площадь. (Образ берётся только для тех точек, орбиты в которых определены.)

**Задача 50.** Для точки  $x$ , вектора  $v$  и числа  $t$  посмотрим на положение  $x$  и направление её вектора скорости спустя время  $t$ . Это задаёт отображение  $F_t : T \times [0; 2\pi) \rightarrow T \times [0; 2\pi)$ .

**(а)** Докажите, что если  $T$  — многоугольник, то множество точек, где  $F_t$  не определено, имеет в  $T \times [0; 2\pi)$  нулевой объём.

**(б)** Докажите, что для любого  $t$  отображение  $F_t$  сохраняет объём.

Орбита точки  $x$  с заданным вектором скорости называется *почти периодической*, если для любых  $\varepsilon_1, \varepsilon_2 > 0$  найдётся  $t > 0$ , такое что расстояние между  $x$  и  $f_t(x)$  меньше  $\varepsilon_1$ , а угол между векторами скорости  $x$  и  $f_t(x)$  меньше  $\varepsilon_2$ .

**Задача 51<sup>m</sup>.** Докажите, что почти любые начальные условия  $(x, \varphi) \in T \times [0; 2\pi)$  задают почти периодическую траекторию. Здесь “почти любые” означает “все, кроме некоторого множества в  $T \times [0; 2\pi)$ , имеющего нулевой объём”.

Неформально можно сформулировать задачу так: докажите, что, посетив из случайного места в зеркальной комнате фонариком в случайном направлении, мы с вероятностью 1 попадём себе в затылок с любой наперёд заданной точностью.

Свойство преобразований, сохраняющих объём, которое предлагается доказать в задаче 51<sup>m</sup>, можно сформулировать в общем случае следующим образом:

**Теорема Пуанкаре о возвращении.** Пусть  $U \subset \mathbb{R}^3$  — ограниченная область,  $f : U \rightarrow U$  — отображение, сохраняющее объём. Возьмём меньшую область  $A \subset U$ . Для точки  $x \in A$  построим последовательность  $f(x), f(f(x)), f(f(f(x))), \dots$  Определим  $Z \subset A$  как множество точек, для которых эта последовательность целиком лежит вне  $A$ . Тогда  $Z$  имеет нулевой объём.

Чтобы эта теорема имела строгий смысл, необходимо сделать оговорки о том, какие “области” мы рассматриваем, а также уточнить, для каких подмножеств множества  $U$  отображение  $f$  “сохраняет объём”. (Известные парадоксы [Ya, стр. 12, 18] показывают, что *нельзя* корректно определить объём для всех подмножеств. Необходимую теорию см., напр., в [AMK] или [Ox].)

# Указания и решения к задачам после пром. финиша

Мы изложим решения задач после промежуточного финиша в таком порядке, в котором они ведут к главным задачам.

## Топология. Задача про возы

### Замкнутые кривые на плоскости

**Решение задачи 24.** Нет, условие (1) не следует из условия (2).

Возьмём две параллельные прямые  $l, m$ . Мы выберем три точки на каждой из них:  $A_1, A_2, A_3 \in l$  и  $B_1, B_2, B_3 \in m$ . Если никакая тройка прямых  $A_1B_i, A_2B_j, A_3B_k$  (где  $\{i, j, k\} = \{1, 2, 3\}$ ) не пересекается в одной точке, то условие (2) будет выполнено, в то время как условие (1) не выполнено по построению.

Докажем, что такие шесть точек существуют. Выберем точки  $A_1, A_2, A_3 \in l$  и  $B_1, B_2 \in m$  произвольно. Тогда для точки  $B_3$  существует лишь конечное число — не более трёх — запрещённых положений. (Например, если обозначить пересечение  $A_1B_1 \cap A_2B_2$  через  $C$ , то  $B_3$  не может лежать на пересечении  $A_3C$  и  $m$ .)  $\square$

**Решение задачи 25.** Пусть даны произвольные точки  $A_1, \dots, A_n \in \mathbb{R}^2$ . Сколь угодно малым сдвигом можно добиться того, чтобы они не совпадали. Поэтому будем считать точки различными. Далее мы будем двигать их по одной, приводя каждую в общее положение со всеми предыдущими.

Пусть точки  $A_1, \dots, A_{k-1}$  уже в общем положении. Посмотрим на множество положений, запрещённых для  $A_k$ . Во-первых, оно включает все прямые  $A_iA_j$  для всевозможных пар индексов  $i, j < k$ . Во-вторых, оно включает все прямые  $A_jC$ , где  $C$  — точка пересечения  $A_{i_1}A_{i_2} \cap A_{i_3}A_{i_4}$ , для всевозможных пятёрок индексов  $i_1, i_2, i_3, i_4, j < k$ .

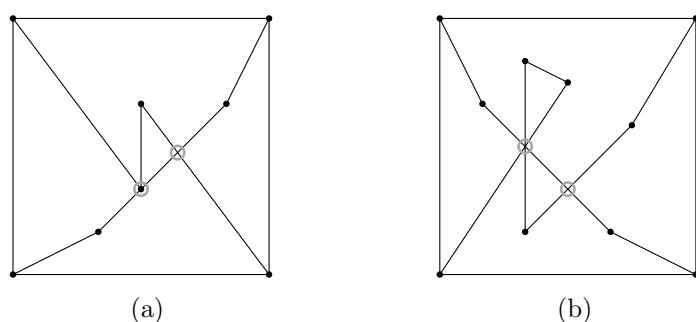
Мы видим, что запрещённые положения для  $A_k$  образуют конечное объединение прямых. Поэтому можно сдвинуть  $A_k$  сколь угодно мало, так что она не будет лежать в этом множестве.  $\square$

**Решение задачи 26.** База индукции очевидна: если  $m = n = 1$ , то утверждение заключается в том, что диагонали квадрата пересекаются в нечётном числе точек.

Докажем шаг индукции. Пусть  $m > 1$ . Заменим звенья  $A_{m-2}A_{m-1}$  и  $A_{m-1}A_m$  ломаной  $\alpha$  на одно звено  $A_{m-2}A_m$ . Чтобы показать, что чётность числа точек пересечения  $\alpha$  и  $\beta$  не изменилась, докажем, что  $\beta$  пересекает границу треугольника  $A_{m-2}A_{m-1}A_m$  в чётном числе точек.

Действительно, если вершины  $B_k, B_{k+1}$  лежат *по разные стороны* от границы  $A_{m-2}A_{m-1}A_m$  (т. е. одна внутри треугольника, а другая снаружи), то пересечение отрезка  $B_kB_{k+1}$  с границей  $A_{m-2}A_{m-1}A_m$  состоит из нечётного числа точек, а если *по одну* — то из чётного. Поскольку  $A_0$  и  $A_n$  лежат по одну сторону (обе снаружи), всего точек пересечения будет чётное число.  $\square$

**Решение задачи 27.** Ответ: (a) нет; (b) нет. Примеры показаны на рисунках.



*Комментарий.* В нашем примере к пункту (а) для множества вершин ломаных не выполняется также и условие (2). Примера для пункта (а), в котором условие (2) выполняется, не существует.

Если требовать, чтобы ломаные не самопересекались, то для пункта (б) можно доказать, что число точек пересечения всегда нечётно. Для этого можно при приведении вершин ломаных в общее положение проследить за точками пересечения, как в доказательстве Леммы 1.  $\square$

**Решение задачи 28.** (а) Предположим,  $\alpha \cap \beta = \emptyset$ . Возьмём число  $\varepsilon > 0$ , такое что расстояние между любой точкой на  $\alpha$  и любой точкой на  $\beta$  меньше  $\varepsilon$ . Тогда, если мы сдвинем вершины  $\alpha$  и  $\beta$  не более чем на  $\frac{\varepsilon}{2}$ , точек пересечения у них не появится, поскольку любая точка на ребре также сдвинется не более чем на  $\frac{\varepsilon}{2}$ . Согласно же задаче 25, мы можем привести  $\alpha$  и  $\beta$  в общее положение, сдвинув каждую вершину не более чем на  $\frac{\varepsilon}{2}$ . Это завершает доказательство.

Отметим, что  $\varepsilon$  может быть меньше, чем минимум расстояний между вершинами  $\alpha$  и  $\beta$ . Число  $\varepsilon$  можно вычислить так: возьмём вершину одной ломаной и ребро другой, померим расстояние между ними; сделаем это для всевозможных комбинаций вершины одной ломаной и ребра другой; тогда достаточно взять  $\varepsilon$  меньше всех найденных чисел.

(б) *Набросок решения.* Любую непрерывную кривую можно аппроксимировать ломаной с точностью до любого  $\varepsilon > 0$ . Это значит, что мы последовательно отмечаем на кривой точки, так что участок кривой между соседними точками находится от соединяющего их отрезка не дальше, чем на  $\varepsilon$ . Нужно построить такие аппроксимации для  $\varepsilon = \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots$  и найти у пары ломаных на каждом шаге произвольную точку пересечения  $P_i$ . Для каждой  $P_i$  найдутся точки  $A_i$  и  $B_i$ , лежащие на кривых, причём расстояние между  $A_i$  и  $B_i$  не превосходит  $\frac{1}{2^{i-1}}$ . Остаётся, воспользовавшись компактностью, выбрать из  $A_i$  и  $B_i$  сходящиеся подпоследовательности с одинаковыми индексами. Их пределы будут равны — это и есть искомая общая точка наших кривых.  $\square$

## Задача про возы

**Решение задачи 19.** Отождествим дорогу с отрезком  $[0; 1]$ , а время — с отрезком  $[9; 21]$ . Зависимости точки, где находится турист, от времени являются непрерывными функциями  $[9; 21] \rightarrow [0; 1]$ . Обозначим их  $f$  и  $g$ , соответственно. При этом  $f(9) = g(21) = 0$  и  $f(21) = g(9) = 1$ .

Для разности  $h = f - g$  значение в точке 9 отрицательно, а в точке 1 положительно. По теореме о промежуточном значении, существует  $t \in [9; 21]$ , для которого  $h(t) = 0$ . Значит местоположение туриста в момент времени  $t$  в первый и во второй дни совпадает.  $\square$

**Решение задачи 20<sup>m</sup>.** Отождествим каждую дорогу с отрезком  $[0; 1]$ . Тогда фазовое пространство положений двух транспортных средств на дорогах — квадрат  $[0; 1] \times [0; 1]$ .

Кусочно-линейное движение машин задаёт ломаную внутри квадрата, ведущую из вершины  $(0, 0)$  в вершину  $(1, 1)$ . Кусочно-линейное движение возов задаёт ломаную внутри квадрата, ведущую из вершины  $(0, 1)$  в вершину  $(1, 0)$ . По Лемме 1 эти ломаные имеют общую точку. Значит, в какой-то момент положение машин совпадает с положением возов, но это невозможно из условия.  $\square$

**Решение задачи 21. (а)** Ответ: да.

Будем считать, что никакой участок горы не горизонтален. Отождествим каждую тропу с отрезком  $[0; 1]$ . Тогда множество возможных положений альпинистов (на одной высоте) будет подмножеством  $M$  квадрата  $[0; 1] \times [0; 1]$ , содержащим вершины  $(0, 0)$  и  $(1, 1)$ .

Заметим, что  $M$  состоит из отрезков. Введём на нём структуру графа: его вершины — состояния, когда хотя бы один из альпинистов находится в вершине ломаной-склона. Можно показать, что степень каждой вершины, за исключением  $(0, 0)$  и  $(1, 1)$ , чётна. Из этого следует, что существует путь из  $(0, 0)$  в  $(1, 1)$ .

Если же некоторые участки горы горизонтальны, “схлопнем” эти участки и назовём полученные точки на тропах *особыми*. Для новой горы алгоритм подъёма существует по доказанному

выше. Когда хотя бы один из альпинистов проходит через особую точку, пусть они задержатся там на минуту. Это добавит конечное число минут ко времени подъёма. Из такого алгоритма легко получить алгоритм подъёма на исходную гору.

Отдельно отметим, что если никакие две вершины ломаной-склона не лежат на одной высоте, то для альпинистов существует единственный способ движения, при котором они проходят каждое положение не более одного раза.

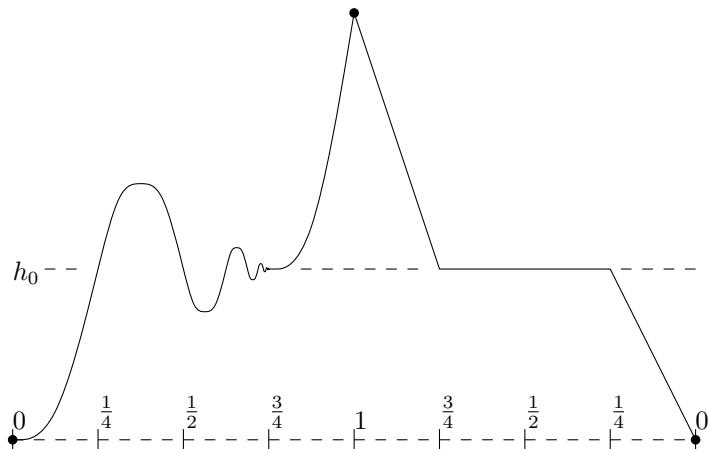
**(с)** Ответ: да. Докажем утверждение по индукции. Для одного альпиниста утверждение trivialно. Опишем шаг.

Возьмём первых двух альпинистов и алгоритм их подъёма на гору из пункта (а). Их высота зависит от времени кусочно-линейно. Нарисуем график этой зависимости и скажем, что это новый склон горы. Тогда мы можем заменить первых двух альпинистов на одного, ползущего по новому склону. Так  $k$  альпинистов заменяются на  $k - 1$ .

**(б)** Ответ: нет.

Пример того, как могут быть устроены склоны, показан на рисунке. Один из них в любой окрестности точки  $\frac{3}{4}$  имеет монотонно возрастающий участок и монотонно убывающий участок, каждый из которых проходит высоту  $h_0$ .

Чтобы альпинисты влезли на вершину, находясь на одной высоте, второму пришлось бы бесконечное количество раз по очереди побывать в точках  $\frac{1}{4}$  и  $\frac{3}{4}$ . С таким условием зависимость положения второго альпиниста от времени не может быть непрерывной. Доказательство последнего утверждения — хорошее упражнение про непрерывные функции.



Мы рекомендуем участникам нарисовать для этой горы множество  $M \subset [0; 1] \times [0; 1]$ , определённое как в пункте (а), и показать, что внутри него не существует непрерывного пути из точки  $(0, 0)$  в точку  $(1, 1)$ .  $\square$

## Топология. Прямоугольник, вписанный в кривую

Предлагаемый нами путь к решению задачи 22<sup>м</sup> во многом схож с подходом, изложенным в статье [Pr]. В этой статье, однако, приводится другое определение коэффициента зацепления замкнутых кривых в пространстве. Мы рекомендуем участникам ознакомиться с этой статьёй в качестве дополнительного материала.

## Зацепленность замкнутых кривых в пространстве

**Решение задачи 29.** Решение этой задачи аналогично решению задачи 25. Будем двигать точки по одной, приводя в общее положение. Первые три точки сдвинем так, чтобы они не лежали на одной прямой. На  $k$ -м шаге при  $k \geq 4$  множество, куда запрещено ставить  $A_k$ , будет состоять из конечного числа плоскостей. Его можно избежать путём сколь угодно малого сдвига  $A_k$ .  $\square$

**Решение задачи 30.** Поскольку множество всех вершин является набором общего положения, никакая из вершин ломаной не лежит на поверхности тетраэдра, а любое звено ломаной может пересекать поверхность тетраэдра лишь во внутренних точках граней.

Обозначим вершины ломаной  $A_0, A_1, \dots, A_n = A_0$ . Покрасим  $A_i$  в красный цвет, если она лежит внутри тетраэдра, и в синий, если снаружи. Тогда звено ломаной  $A_i A_{i+1}$  пересекает поверхность тетраэдра в нечётном числе точек если и только если  $A_i$  и  $A_{i+1}$  покрашены в разные цвета. Таких звеньев чётное число.  $\square$

**Решение задачи 31. (а)** Обозначим вершины  $\alpha$  и  $\beta$  через  $A_1, \dots, A_n$  и  $B_1, \dots, B_m$  соответственно.

Предположим,  $\{A_1, \dots, A_n, B_1, \dots, B_m, O, O'\}$  является набором общего положения. Тогда по задаче 30 пересечение поверхности каждого тетраэдра  $OO'A_i A_{i+1}$  с ломаной  $\beta$  состоит из чётного числа точек. Суммируя по всем тетраэдром, получаем требуемое.

Единственная трудность может состоять в том, что  $\{A_1, \dots, A_n, B_1, \dots, B_m, O, O'\}$  не будет набором общего положения. Однако, по условию множества  $\{A_1, \dots, A_n, B_1, \dots, B_m, O\}$  и  $\{A_1, \dots, A_n, B_1, \dots, B_m, O'\}$  являются наборами общего положения. Выберем точку  $O'' \in \mathbb{R}^3$ , при добавлении которой к любому из них полученное множество останется в общем положении. Остается воспользоваться предыдущим рассуждением, перейдя от  $O$  к  $O''$ , и затем от  $O''$  к  $O'$ .

**(б) Указание.** Возьмём пару параллельных плоскостей в  $\mathbb{R}^3$ , между которыми заключены  $\alpha$  и  $\beta$ . Выберем точку  $O$  на одной из этих плоскостей. Будем вычислять  $\text{lk}(\alpha, \beta)$  и  $\text{lk}(\beta, \alpha)$  с помощью выбранной точки  $O$ .

Спроектируем  $\alpha$  и  $\beta$  на вторую плоскость из точки  $O$ . Обозначим полученные плоские ломаные  $\tilde{\alpha}$  и  $\tilde{\beta}$ . Чтобы показать, что  $\text{lk}(\alpha, \beta) \equiv \text{lk}(\beta, \alpha)$ , достаточно проверить, что  $\tilde{\alpha}$  и  $\tilde{\beta}$  пересекаются в чётном числе точек. Это доказывается аналогично задаче 26.  $\square$

**Решение задачи 32. (а)** Решение этой задачи аналогично решению задачи 28. Возьмём число  $\varepsilon > 0$ , такое что расстояние между любой точкой на  $\alpha$  и любой точкой на  $\beta$  меньше  $\varepsilon$ , а также расстояние между любой парой несоседних рёбер  $\alpha$  и между любой парой несоседних рёбер  $\beta$  меньше  $\varepsilon$ . Тогда, если мы сдвинем вершины  $\alpha$  и  $\beta$  не более чем на  $\frac{\varepsilon}{2}$ , точек пересечения у них не появится, поскольку любая точка на ребре также сдвинется не более чем на  $\frac{\varepsilon}{2}$ . Согласно же задаче 29, мы можем привести  $\alpha$  и  $\beta$  в общее положение, сдвинув каждую вершину не более чем на  $\frac{\varepsilon}{2}$ .

**(б)** Докажем требуемое утверждение для сдвига одной из вершин.

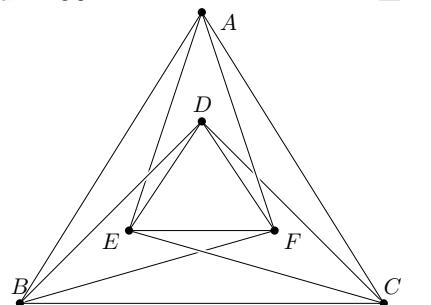
А именно, пусть ломаные  $\alpha'$  и  $\beta'$  находятся в общем положении. Сдвинем одну из вершин  $A'_i$  ломаной  $\alpha'$  так, что в процессе сдвига (по прямой) звенья  $A'_{i-1} A'_i$  и  $A'_i A'_{i+1}$  не пересекли других звеньев  $\alpha'$  и  $\beta'$ . Обозначим полученную вершину  $A''_i$ , а полученную ломаную  $\alpha''$ . Далее мы покажем, что  $\text{lk}(\alpha', \beta') \equiv \text{lk}(\alpha'', \beta')$ .

Возьмём точку  $O$  в общем положении со всеми вершинами  $\alpha'$  и  $\beta'$ , включая  $A''_i$ . Рассмотрим пересечение тетраэдров  $OA'_{i-1} A'_i A''_i$  и  $OA'_i A''_i A'_{i+1}$  с ломаной  $\beta'$ . По построению, грани  $A'_{i-1} A'_i A''_i$  и  $A'_i A''_i A'_{i+1}$  не пересекаются с  $\beta'$ . Тогда  $\text{lk}(\alpha', \beta') \equiv \text{lk}(\alpha'', \beta')$  из задачи 30.  $\square$

**Решение задачи 33.** Возьмём вложение  $\gamma_0 : K_6 \rightarrow \mathbb{R}^3$ , изображённое на рисунке.

Для него цикл  $AEF$  зацеплен по модулю 2 с циклом  $DBC$ , цикл  $BFD$  зацеплен по модулю 2 с циклом  $ECA$ , а цикл  $CDE$  зацеплен по модулю 2 с циклом  $FAB$ .

Других пар циклов, зацепленных по модулю 2, для построенного вложения  $K_6 \rightarrow \mathbb{R}^3$  нет. Поэтому  $\text{slk}(\gamma_0) \equiv 1$ .  $\square$



**Решение задачи 34.** Пусть вложения  $\gamma_1, \gamma_2 : K_6 \rightarrow \mathbb{R}^3$  различаются только на ребре  $AB$ .

Рассмотрим пару циклов  $ABC$  и  $DEF$ . Обозначим ломаную  $\gamma_1(ABC)$  через  $\alpha$ , ломаную  $\gamma_2(ABC)$  через  $\alpha'$ , ломаную  $\gamma_1(DEF)$  через  $\beta$ , а объединение  $\gamma_1(AB) \cup \gamma_2(AB)$ , тоже являющееся замкнутой ломаной, через  $\alpha''$ . Тогда можно показать, что

$$\text{lk}(\alpha, \beta) - \text{lk}(\alpha', \beta) \equiv \text{lk}(\alpha'', \beta).$$

Всего имеется 4 пары циклов в  $K_6$ , таких что один из них содержит ребро  $AB$ . Суммируя для них соотношения, аналогичные показанному выше, мы получим

$$\text{slk}(\gamma_1) - \text{slk}(\gamma_2) \equiv \text{lk}(\alpha'', \gamma_1(DEF)) + \text{lk}(\alpha'', \gamma_1(CEF)) + \text{lk}(\alpha'', \gamma_1(CDF)) + \text{lk}(\alpha'', \gamma_1(CDE)).$$

Нам остаётся доказать, что сумма четырёх слагаемых в правой части равенства равна нулю. По сути это утверждение аналогично утверждению задачи 30. Отличие в том, что вместо тетраэдра в  $\mathbb{R}^3$  нам дано кусочно-линейное вложение графа  $K_4 = CDEF$ , а вместо пересечения  $\alpha''$  с поверхностью мы считаем коэффициенты зацепления.

Выберем точку  $O$  в общем положении с вершинами всех этих ломанных. Тогда равенство правой части нулю по модулю 2 следует прямо из определения коэффициента зацепления.  $\square$

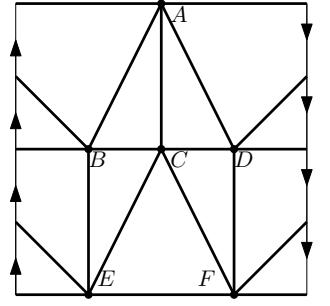
**Решение задачи 35.** Согласно задаче 34, сумма  $\text{slk}(\gamma)$  по модулю 2 не зависит от выбора вложения  $\gamma : K_6 \rightarrow \mathbb{R}^3$ . Тогда из задачи 33 следует, что для всех вложений  $K_6 \rightarrow \mathbb{R}^3$  имеем  $\text{slk} \equiv 1$ . Следовательно, для любого наперёд заданного вложения  $K_6 \rightarrow \mathbb{R}^3$  найдётся пара непересекающихся циклов, образы которых зацеплены.  $\square$

## Вложения ленты Мёбиуса в пространство

**Решение задачи 36. (a)** Вложение показано на рисунке.

(b) Если цикл  $K_6$  ограничивает в  $M$  многоугольник, то образ такого цикла при  $f$  не может быть зацеплен с образом никакого другого цикла.

Перечислим циклы длины 3, не ограничивающие многоугольник:  $ABD$ ,  $AEF$ ,  $BCD$ ,  $BED$ . Из них можно выбрать лишь одну непересекающуюся пару —  $AEF$  и  $BCD$ . Это как раз есть циклы  $\alpha$  и  $\beta$ . Поскольку  $\text{slk}(f(K_6)) \equiv 1$ , мы получаем  $\text{lk}(\alpha, \beta) \equiv 1$ .  $\square$



**Решение задачи 37.** Если вложить  $K_6$  в  $M$  как в задаче 36 (a), то  $f$  задаст кусочно-линейное вложение  $K_6 \rightarrow \mathbb{R}^3$ . Воспользуемся для него утверждением задачи 36 (b) и Леммы 3.  $\square$

**Решение задачи 38.** Пусть такое вложение существует. Как мы показали в задаче 37, образ границы  $M$  обязательно зацеплен с образом средней линии  $M$ . Но если образ границы лежит в некоторой плоскости, а образ средней линии — в одной из полуплоскостей, то они не могут быть зацеплены.  $\square$

**Решение задачи 39\*.** Можно пытаться свести непрерывную задачу к кусочно-линейной, аналогично тому, как мы это сделали в задаче 28 (b). Сложность такого пути в том, что кусочно-линейные отображения  $M \rightarrow \mathbb{R}^3$ , которыми мы приближаем заданное непрерывное вложение, тоже должны быть *вложениями*. Данная техническая сложность хотя и преодолевается, но крайне тяжело.

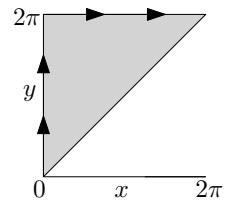
Более простой способ — определить коэффициент зацепления по модулю 2 для пары замкнутых непрерывных кривых в  $\mathbb{R}^3$ . Для этого надо приближать кривые ломаными. Можно показать, что для достаточно близких приближений полученный коэффициент зацепления по модулю 2 не зависит от выбора приближения. Далее для решения задачи нужно показать, что если одна из кривых затягивается диском (непрерывно вложенным в  $\mathbb{R}^3$ ), не пересекающим вторую кривую, то коэффициент зацепления равен нулю.

О других более концептуальных способах определить коэффициент зацепления для замкнутых непрерывных кривых в  $\mathbb{R}^3$  см. [H, §1.2] или [FF, 17.6].  $\square$

## Прямоугольник, вписанный в кривую

**Решение задачи 23.** Каждой неупорядоченной паре точек на окружности сопоставим упорядоченную пару точек  $x \leq y$  на отрезке  $[0; 2\pi]$ .

При этом пары  $(0, a)$  и  $(a, 2\pi)$  точек отрезка соответствуют одной паре точек на окружности. Таким образом, конфигурационное пространство пар точек на окружности получается склейкой двух сторон треугольника на рисунке справа. Предлагаем участникам самостоятельно убедиться, что такая склейка даёт ленту Мёбиуса.



Отметим, что граница  $M$  соответствует множеству пар совпадающих точек окружности.  $\square$

**Решение задачи 22<sup>m</sup>.** Обозначим окружность  $S^1$ . Пусть задано непрерывное отображение  $\gamma : S^1 \rightarrow \mathbb{R}^2$ . Отождествим  $\mathbb{R}^2$  с плоскостью  $z = 0$  в  $\mathbb{R}^3$ .

Зададим отображение из конфигурационного пространства пар точек окружности в  $\mathbb{R}^3$  следующим образом. Неупорядоченной паре  $(a, b)$  сопоставим точку  $(\frac{\gamma(a)+\gamma(b)}{2}, |\gamma(a) - \gamma(b)|)$ . Здесь  $\frac{\gamma(a)+\gamma(b)}{2}$  — середина отрезка между точками  $\gamma(a)$  и  $\gamma(b)$  в  $\mathbb{R}^2$ .

Мы получили отображение  $M \rightarrow \mathbb{R}^3$ . Заметим, что образ границы  $M$  совпадает с кривой  $\gamma$ . Согласно Лемме 2, это отображение не может быть вложением. Следовательно, существуют две различные пары точек  $\gamma$ , такие что отрезки, соединяющие их, имеют одинаковую середину и одинаковую длину. Эти четыре точки являются вершинами искомого прямоугольника.

Это доказательство наглядно изложено в видео [4] на YouTube.  $\square$

## Литература и дополнительные материалы

- [AMK] П. С. Александров, А. И. Маркушевич, А. Я. Хинчин, *Энциклопедия элементарной математики. Книга 5, геометрия*, М., Наука, 1966.
- [CG] Г. С. М. Коксетер, С. П. Грейтцер, *Новые встречи с геометрией*, М.: Наука, 1978.
- [Ox] Дж. Окстоби, *Мера и категория*, Мир, 1974.
- [Pr] В. В. Прасолов, *Прямоугольники на кривой и вложения листа Мёбиуса*, Математическое Просвещение, Выпуск 8, 2004.
- [S] А. Б. Сосинский, *Геометрия*, МЦНМО, 2017.
- [FF] А. Т. Фоменко, Д. Б. Фукс, *Курс гомотопической топологии*, Наука, 1989.
- [H] А. Хатчер, *Алгебраическая топология*, МЦНМО, 2011.
- [Sh] А. Н. Ширяев, *Вероятность-1*, МЦНМО, 2011.
- [Ya] И. В. Ященко, *Парadoxы теории множеств*, Библиотека «Математическое просвещение», МЦНМО, 2002.
- [1] <https://www.youtube.com/watch?v=HEfHFsfGXjs>
- [2] <https://www.youtube.com/watch?v=jsYwFizhncE>
- [3] <https://www.youtube.com/watch?v=brU5yLm9DZM>
- [4] <https://www.youtube.com/watch?v=AmgkSdhK4K8>

# Phase spaces

presented by Anastasiya Enne, Evgeny Khinko,  
Andrey Ploskonosov and Andrey Ryabichev

## Abstract

We offer participants a number of problems to solve, for which it is useful to consider phase spaces. In the section before the semifinal we show a variety of problems illustrating this principle. In the section after the semifinal we introduce a couple of challenging ideas. These ideas will require the participants to explore geometrical and topological properties of the phase spaces.

## 1 Problems before the semifinal

### 1.1 Introduction

It is convenient to consider a “set of all possible states” of a system for solving many mathematical problems. Such a set is usually called *a phase space* of the system. Information about the state of the system may include not only points’ coordinates, but also, as is common in mechanics, points’ velocities.

A phase space for some problem should be viewed not just as a set of points: usually it is useful to consider an additional structure. For example, geometric structure (as on a set of points in the plane); function of distance between points; notion of area/volume for subsets of a phase space; incidence relation (if a phase space is a set of graph vertices). The right choice of such a structure can simplify a statement of a problem, then the problem itself becomes trivial.

Let us consider the following example.

**Problem 0.** Three kids sit around a table, and each of them has a plate of porridge. Every minute they simultaneously do the following: each kid divides his or her porridge into 2 equal parts and puts these parts to each of the other kids’ plates. Prove that after several minutes all porridge will be spread evenly between the kids with an accuracy of 1%.

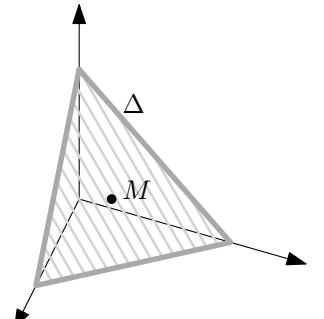
*Solution.* Suppose that the total amount of the porridge is equal to 1. By  $(x_1, x_2, x_3)$  denote a set of numbers, where  $x_i$  corresponds to an amount of porridge in  $i$ -th kid’s plate. All possible states of our system lie in the plane  $x_1 + x_2 + x_3 = 1$ , and  $x_1 \geq 0, x_2 \geq 0, x_3 \geq 0$ . Hence, *our phase space is a regular triangle  $\Delta$  with vertices  $(1, 0, 0)$ ,  $(0, 1, 0)$ , and  $(0, 0, 1)$ .*

Note that the transformation

$$(x_1, x_2, x_3) \mapsto (y_1, y_2, y_3) = \left( \frac{x_2+x_3}{2}, \frac{x_1+x_3}{2}, \frac{x_1+x_2}{2} \right)$$

is a homothetic transformation of the triangle  $\Delta$  with ratio  $-\frac{1}{2}$  and origin  $M = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$  — the intersection point of the medians. Try to prove that yourself.

Let us mark all the system’s states, where the porridge is spread evenly between the kids with an accuracy of 1%. This subset of the triangle  $\Delta$  contains a small disk of centre  $M$ . Then, after a sufficiently large number of iterations all the points of  $\Delta$  will be inside the disk. This implies the required statement of the problem.  $\square$



## 1.2 Geometric probability

In each of the following problems a notion of probability needs to be defined. Then, you should use your definition to find the answer.

**Problem 1.** Two friends agreed to meet near a huge oak between midday and 1 p.m., but they didn't decide on the exact time of the meeting. They arrive there randomly at that time interval. They are willing to wait for each another for 10 minutes, after which they go away. What is the probability of their meeting?

**Problem 2.** What is the probability that a stick randomly broken in two points can form a triangle? Compare the answers for the following ways *to break it randomly*:

- (a) the first point we choose randomly; after breaking the stick we select one of two parts with equal probability; then we choose the second point randomly on the selected part;
- (b) we choose the two points randomly and independently;
- (c) we choose a random representation of the stick's length  $l$  as a sum of the three ordered summands  $l = x_1 + x_2 + x_3$  (cf. problem 0).

**Problem 3.** A Mars rover travels around an even surface of an inhospitable planet (the surface can be considered flat). The rover chooses a random direction and moves one kilometer this way. What is the probability that after making three iterations and covering three kilometers the rover will cross its own trail?

**Problem 4** (Buffon's needle). A plane is ruled with parallel lines 1 cm apart. A needle of length 1 cm is dropped on the plane. What is the probability that the needle crosses a line?

## 1.3 Configuration spaces

**Problem 5.** A polygon of area  $> 1$  is drawn on a coordinate plane. Prove that there exist two points  $A$  and  $B$  in its interior such that both coordinates of the vector  $AB$  are integer.

**Problem 6.** A polygon of area  $< 1$  and 1000 points are drawn on a plane. Prove that the polygon can be moved in a vector of length  $< \sqrt{\frac{1000}{\pi}}$  in such a way that the polygon will not cover any of the given points.

**Problem 7.** A unit sphere is given. A *great circle* is a circle with radius 1 laying on the sphere. We call a curve on the sphere *polygonal* if it consists of arcs of great circles.

- (a) There is a polygonal curve  $\gamma$  of length  $< \pi$  on the unit sphere. Prove that there exists a great circle that does not intersect  $\gamma$ .
- (b) There is a non-self-intersecting polygonal curve  $\gamma$  of length  $> \pi k$  on the unit sphere. Prove that there exists a great circle intersecting  $\gamma$  in more than  $k$  points such that it does not contain any edges of  $\gamma$ .

**Problem 8.** There are two tetrahedrons in space. For every plane the following statement holds: the projections of these tetrahedrons on the plane are both either triangles or quadrilaterals. Prove that the tetrahedrons are similar.

**Problem 9.** There are  $k$  nails hammered into a plane. Consider all lines in the plane such that none of the nails lies on these lines. We call two lines equivalent if one of them can be moved onto another without touching any nails. Then, the set of all considered lines is divided into disjoint equivalence classes, where each class consists of the lines equivalent to each other. Find the (a) minimal (b) maximal number of the equivalence classes for a given  $k$ .

**Problem 10.** Eight cars entered a cross-country race. A route is a straight road with several swampy sections. Every car moves at a constant speed on a dry section of the road (each one with its own), and at a different constant speed on a swampy section of the road (each one also with its own). All the cars start the race from the same point, but at a different time (start times may be not equally distributed). There are 500 judges on the route.

Each judge noticed the order of the cars passed by, and there was no overtaking right in front of the judges. Prove that there exist two judges such that the cars passed by them in the same order.

## 1.4 Descrete phase spaces

**Problem 11.** Alice picked a two-digit number. Bob suggests two-digit numbers and his goal is to find a number which differs from Alice's number no more than by 1 in every digit. What is the minimum number of attempts required?

**Problem 12.** Alice picked a two-digit number. Now, Bob's goal is to find a number which equals Alice's number in one digit and differs from it no more than by 1 in the other digit. Is it enough for him to do (a) 18 attempts; (b) 20 attempts; (c) 22 attempts?

**Problem 13.** Several boxes are arranged in a circle with some beads placed inside the boxes. For each move it is allowed to take all the beads from any box and place them one by one to the next boxes in a clockwise order.

(a) Prove that if for each move the beads are taken from a box to which the last bead was placed in the previous move, then after some number of moves the placement of beads from the start appears again.

(b) Prove that it is possible to get any desired bead's placement form any starting placement for several moves.

**Problem 14.** (a) An invisible ship is placed on some cell of a cellular strip infinite in both directions. For each turn a player can shoot at one square and after each shot the ship moves by some number of cells (the number of cells and the direction of the move is the same for every turn, but player does not know neither of them). Find a strategy to shoot the ship.

(b) The same problem can be stated for a cellular plane: the ship is placed on some cell and after each shot it moves in a vector with integer coordinates (this vector is the same for every move). A player can shoot at one square for each turn.

## 1.5 Selected problems

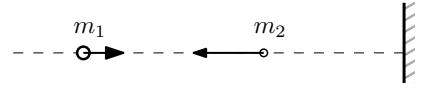
**Problem 15.** You have 6-liter, 7-liter, and 12-liter jugs. The two smaller jugs are filled with water. Is it possible to measure exactly 9 liters of water if you are allowed just to pour water from one jug to another?

**Problem 16.** There are three water tanks. Water is running out of the first tank with a constant speed, and running in the second and the third tank (also with a constant speed). In the beginning, the first tank was filled with the same amount of water as two other tanks together; after some period of time the second tank had the same amount of water as two other tanks together; in the end the third tank had the same amount of water as two other tanks together. Is it possible that neither in the beginning nor in the end none of the tanks was empty?

**Problem 17** (Simplified “predator-pray” model). There are  $x$  rabbits and  $y$  wolves living in a forest. Without wolves the rabbit population grows with constant rate  $a_0$ . But if there are  $y > 0$  wolves living in a forest, then these wolves eat  $a_1 y$  rabbits per a unit of time (i.e.,  $x'(t) = a_0 - a_1 y$ ). Also, without rabbits the wolves population decrease with constant rate  $b_0$ , but if there are  $x > 0$  rabbits

then the wolves population grows with rate  $b_1x$  (i.e.,  $y'(t) = -b_0 + b_1x$ ). Find the time dependence for an amount of rabbits and wolves. For what values  $a_0$ ,  $a_1$ ,  $b_0$ , and  $b_1$  do these amounts change periodically?

**Problem 18.** Two balls of masses  $m_1$  and  $m_2$  are moving along a straight line as it is shown in the figure. Elastic collisions occur between the balls and between the balls and the wall.



- (a) Prove that there will be a finite number of collisions between the balls.
- (b) How does the number of collisions depend on a ratio of the balls' masses and initial velocities?

The law of conservation of momentum ( $\sum m_i v_i = \text{const}$ ) and the law of conservation of energy ( $\sum m_i v_i^2 = \text{const}$ ) apply to the balls' collisions. Collisions with the wall are absolutely elastic (with the conservation of velocity). Assume that a ball which is the closest to the wall moves away from it initially.

# Hints and solutions for problems before the semifinal

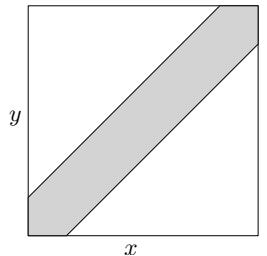
## Geometric probability

To solve these problems we need to define a notion of probability. Let  $X$  be a rectangle such that its points correspond to the set of outcomes in our problem. Let  $A \subset X$  be some subset of  $X$ . We say that *the probability that a point is inside  $A$*  is equal to the relation of the area<sup>1</sup> of  $A$  to the area of  $X$ . In such a case we call  $X$  a *sample space* and we call its subsets *events*. More detailed introduction to probability theory see e.g in [Sh].

**Solution for problem 1.** Answer:  $\frac{11}{36}$ .

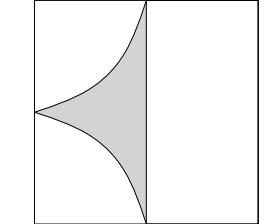
Let us identify the time interval for friend's arrival to the oak with the segment  $[0; 1]$ . Then a possible time of two friends' arrival to the oak is identified with the square  $[0; 1] \times [0; 1]$ . Namely a point  $(x, y)$  is identified with a situation when the first friend comes at the time  $x$ , and the second friend, at the time  $y$ .

Let us colour the points corresponding to the situations when the friends meet. These points form a strip with area  $\frac{11}{36}$ .  $\square$



**Solution for problem 2. (a)** Answer:  $\ln 2 - \frac{1}{2}$ .

Suppose we choose the first point randomly from the line segment  $[0; 1]$ . Then identify each of the resulting parts with its own copy of the line segment  $[0; 1]$ . Hence our sample space consists of two squares (a coordinate of the first choice is marked in each of the squares on the horizontal axis and a coordinate of the second choice is marked on the vertical axis).



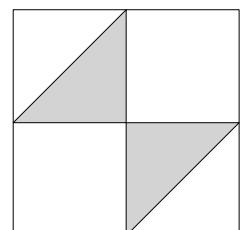
Let us colour the points of  $X$  corresponding to the situations when the broken stick can form a triangle. Suppose the first place where the stick is broken is in the point  $x \in [0; 1]$ . Then suppose that we choose the first part and identify it with  $[0; 1]$ , and then choose a point  $y$  in it. It is possible to form a triangle if  $x > \frac{1}{2}$ ,  $xy < \frac{1}{2}$ , and  $x(1-y) < \frac{1}{2}$ . This subset has area

$$2 \int_{\frac{1}{2}}^1 \left( \frac{1}{2x} - \frac{1}{2} \right) dx = \ln 2 - \frac{1}{2}.$$

The subset of the second square corresponding to the situations where a triangle can be formed can be constructed similarly.

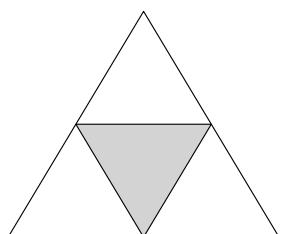
**(b)** Answer:  $\frac{1}{4}$ .

Identify the stick with the line segment  $[0; 1]$ . A choice of two points  $x, y \in [0; 1]$  is identified with a point in the square. It is possible to form a triangle if  $x < y$  and also  $x < \frac{1}{2}$ ,  $y > \frac{1}{2}$ , and  $y - x < \frac{1}{2}$ , or if  $y < x$  and also  $x < \frac{1}{2}$ ,  $y > \frac{1}{2}$ , and  $y - x < \frac{1}{2}$ . This subset has area  $\frac{1}{4}$ .



**(c)** Answer:  $\frac{1}{4}$ .

A sample space for this problem can be identified with the phase space in problem 0. It is possible to form a triangle if  $x_1 < \frac{1}{2}$ ,  $x_2 < \frac{1}{2}$ , and  $x_3 < \frac{1}{2}$ . This subset has area of a quarter of the triangle's area.  $\square$



<sup>1</sup>Generally speaking, for some subsets  $A \subset X$  area may not be defined; therefore we can consider only the probability that a point is inside a "sufficiently good" subset such that its area is well-defined.

**Solution for problem 3.** Answer:  $\frac{1}{12}$ .

Let us identify the sample space with the square  $[0; 2\pi) \times [0; 2\pi)$  where coordinates correspond to the values of angles of the polygonal curve for rover's trail. Besides the boundary  $x = 0$  and  $y = 0$  (that have area 0), the rover will cross its trail if either  $(x, y)$  is a pair of angles in some triangle such that both angles are strictly not the greatest ones, or  $(2\pi - x, 2\pi - y)$  is a pair of angles in some triangle such that both angles are strictly not the greatest ones. These situations correspond to the following systems of inequations

$$\begin{cases} x \leq \pi - x - y, \\ y \leq \pi - x - y \end{cases} \quad \text{and} \quad \begin{cases} (2\pi - x) \leq \pi - (2\pi - x) - (2\pi - y), \\ (2\pi - y) \leq \pi - (2\pi - x) - (2\pi - y). \end{cases}$$

Each of the systems corresponds to a quadrilateral with area equal to the square's area divided by 24.  $\square$

**Solution for problem 4.** Answer:  $\frac{2}{\pi}$ .

For the sake of argument suppose that the lines are horizontal. A sample space for the problem can be identified with the rectangle  $[0; \pi) \times (0; 1]$  where the first coordinate is for the orientated angle of the needle with respect to the lines and the second coordinate is for the distance between the bottom end of the needle and the closest line from below.

Then the set of the outcomes we are interested in is described by inequality  $1 - y \leq \sin x$ . The set has area  $\int_0^\pi \sin x dx = 2$ .  $\square$

## Configuration spaces

**Note about terminology.** Suppose we have a subset  $X$  of Euclidean space. If we identify the set of *points*  $X$  with the set of *positions* of some objects (for example, with a set of lines in a plane or with a set of great circles on a sphere or with a set of  $n$ -tuples of numbers with a fixed sum), then  $X$  is called *configuration space*. This term is considered commonly-accepted and more accurate than the term "phase space", although these terms have the equivalent meaning.

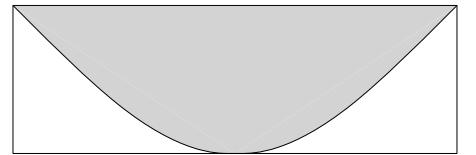
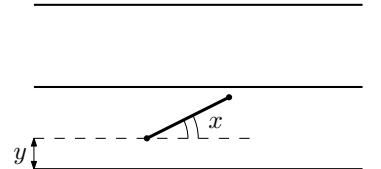
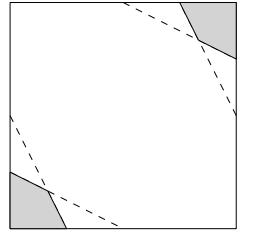
**Solution for problem 5.** Let us consider a "grid" consisting of lines  $x = n$  and  $y = n$  for all possible  $n \in \mathbb{Z}$ . It divides the plane into squares. Let us call the square with vertices  $(0, 0)$ ,  $(1, 0)$ ,  $(1, 1)$ , and  $(0, 1)$  a *base square*. It is clear that each square is obtained from the base square using translation by some integer vector. Suppose that all the squares look like  $[0; 1) \times [0; 1)$  that is the base square without its upper and right edges.

Let us consider the rectangle from the statement of the problem. The grid divides it into a finite number of parts. Let us translate each part by a corresponding integer vector such that all these parts are inside the base square. In fact, we constructed a *set of points of the polygon up to an integer translation*.

Since the sum of the areas of the parts is  $> 1$ , the parts will definitely overlap. As points  $A$  and  $B$  it is sufficient to take any pair of points such that these points become the same point after the move.  $\square$

**Solution for problem 6.** Let us draw disks of radius  $\sqrt{\frac{1000}{\pi}}$  and centre in each of the points. Let us colour the points of the polygon inside each disk. Then let us stack all the disks using translations. Coloured points will cover some set  $P$ . Vectors starting at points of  $P$  and ending at the centre of the disk are *such vectors that the polygon cannot be moved in those directions*.

Each coloured subset has area  $< 1$ , therefore the area of  $P$  is  $< 1000$ . But the area of the disk is exactly 1000 thus there exists a point inside it that is not coloured. The vector starting at that point and ending at the centre of the disk is the required vector for our problem.  $\square$



**Solution for problem 7.** An idea used in this solution is very similar to projective duality (see e. g. [S]). This method allows us to work conveniently with *the set of great circles* on a sphere. Namely suppose we have a sphere of centre  $O$ . Identify each point  $A$  on the sphere with a great circle in the plane passing through  $O$  and perpendicular to  $OA$ .

This determines a one-to-one correspondence between pairs of diametrically opposite points on a sphere and great circles. We call such correspondence *duality* and denote it by  $\delta$ . Note that  $\delta(\delta(A)) = \pm A$  for any point  $A$  on the sphere and  $\delta(\delta(\omega)) = \omega$  for any great circle  $\omega$ . Moreover, if the point  $A$  is on a great circle  $\omega$ , then the great circle  $\delta(A)$  passes through the pair of points  $\delta(\omega)$ .

(a) Suppose we have an ark  $\alpha$  of a great circle. Suppose  $\alpha$  is of length  $\pi t$  for  $t \in (0; 1)$ . Let us consider the great circles  $\delta(A)$  for all  $A \in \alpha$ . Note that area of the union of  $\delta(A)$  is a fraction  $t$  of the area of the sphere.

The polygonal curve  $\gamma$  from the statement of the problem is of length  $< \pi$ . Hence, the great circles dual to the points of  $\gamma$  cannot cover the whole of sphere. Let us consider a point  $B$  such that it is not covered. Then, the great circle  $\delta(B)$  does not intersect  $\gamma$ .

(b) The proof is analogous to the previous one. For each of the edges  $\gamma$  take the union of the great circles that are dual to the points of the edge. We will get a pair of “spherical segments”. Since the length of  $\gamma$  is greater than  $\pi k$ , the union of such segments covers some part of the sphere with non-zero area more than  $k$  times.

In particular there exist infinitely many points on the sphere covered by more than  $k$  segments. Let us mark points  $B_1, \dots, B_m$  which are dual to the extensions of the edges of  $\gamma$ . We can choose a point  $C$  such that it is covered by more than  $k$  segments and is not equal to  $B_1, \dots, B_m$ . Then a big circle  $\delta(C)$  intersects more than  $k$  edges of  $\gamma$  and does not contain any edges.  $\square$

**Hint for problem 8.** Let us inscribe each tetrahedron into a sphere. Let us apply translation and homothetic transformation so that the spheres take the same place.

Then consider lines  $l$  passing through the centre of the sphere such that projections of the tetrahedrons on the plane perpendicular to  $l$  are triangles.  $\square$

**Solution for problem 9.** Let us consider a disk  $D$  such that all the nails are inside it. If a line from some equivalence class intersects  $D$ , then we call such equivalence class *restricted*. It is clear that there exists exactly one class which is not restricted.

Let us draw all possible line segments between the nails such that every segment does not pass through any nails except its ends. One can construct a correspondence between *the set of the segments* and *the set of restricted equivalence classes of the lines*. To do this we should rotate each line counterclockwise until it touches two nails, this pair of nails is the ends of the segment corresponding to the equivalence class of this line

(a) Answer:  $k$ .

Indeed, we can always draw  $k - 1$  line segments. This number of segments is possible when all the nails lie on the same line.

(b) Answer:  $C_k^2 + 1$ .

The number of the segments is not greater than the number of edges of complete graph. This estimate is possible when any three nails do not lie on the same line.  $\square$

**Another idea for problem 9.** Using projective duality one can identify the configuration space of all the lines in  $\mathbb{R}^2$  with  $\mathbb{RP}^2$  minus one point. The removed point corresponds to the “line at infinity”. See e. g. [S].

The set of lines passing through a point  $A \in \mathbb{R}^2$  corresponds to a line in  $\mathbb{RP}^2$ . As a result, our problem reduces to finding the number of parts into which  $\mathbb{RP}^2$  is divided by  $k$  lines (the removed point does not matter for the number of parts).  $\square$

**Solution for problem 10.** Suppose  $S$  is the starting point. For each point  $A$  on the route denote the sum of lengths of dry sections from  $S$  to  $A$  by  $x$ , and the sum of lengths of swampy sections from  $S$  to  $A$  by  $y$ . Then we will assign the point  $(x, y)$  in the plane to the point  $A$  on the route.

Let us draw a plot in space for every car's movement with coordinates  $x, y, t$ . Each of the plots is a polygonal curve. Let us note that each of these polygonal curves lies in some plane  $t = t_0 + \frac{x}{u} + \frac{y}{v}$ , where  $t_0$  is the passing time of point  $S$ ,  $u$  and  $v$  are velocities of the car on dry and swampy road sections respectively. Denote these planes by  $\alpha_1, \dots, \alpha_8$ .

Let us draw vertical lines  $l_1, \dots, l_{500}$  for the judges. We need to show that the points of intersection of some two lines with the planes are in the same order.

Let us consider pairwise intersections of the planes  $\alpha_i \cap \alpha_j$  and project them onto a horizontal plane  $\beta$ . We get no more than  $C_8^2 = 28$  different lines. They divide  $\beta$  into no more than  $1 + C_{29}^2 = 407$  parts. Using pigeonhole principle we get that some two lines of  $l_1, \dots, l_{500}$  pass through the same part.  $\square$

## Discrete phase spaces

**Solution for problem 11.** Answer: 12 attempts.

Let us identify every two-digit number with a cell in a table  $9 \times 10$  where rows correspond to the ten's digit and columns, to the one's digit. If Bob suggests a number, then it covers a square  $3 \times 3$  in the table. But to cover by such squares all marked rows (all numbers starting with 2, 5, and 8) we need to place 12 such squares, that is to suggest minimum 12 numbers.

An example is easy to construct by looking at the table: Bob should suggest numbers 21, 24, 27, 29, 51, 54, 57, 59, 81, 84, 87, and 89.  $\square$

	0	1	2	3	4	5	6	7	8	9
1										
2										
3										
4										
5										
6										
7										
8										
9										

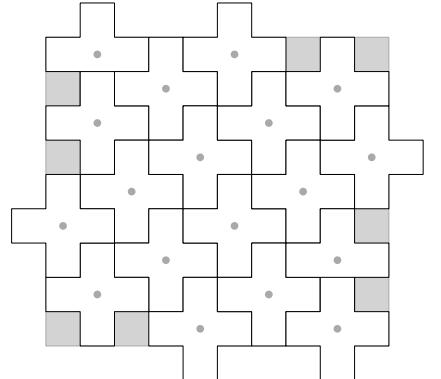
**Solution for problem 12.** An idea is the same, but this time we need to cover all the cells of the rectangle  $9 \times 10$  by “crosses” constructed from five cells.

(a) Answer: No.

Genuinely, if 18 crosses were enough then they would cover the rectangle without any intersections and stay within the rectangle. But it is impossible because, for example, a corner cell cannot be covered this way.

(c) Answer: Yes.

Let us put 18 crosses as shown in the figure (for more clarity a centre of each cross is marked) and we can cover eight not covered cells with the rest 4 crosses.  $\square$



**Solution for problem 13.** (a) A current state of the system is determined by a number of beads in every box and a box from which we will start to place the beads next time. Hence the total amount of the system's states is finite.

From every state it is possible to get to some other well-defined state by placing beads.

On the other hand, we can uniquely determine the systems' state before the last beads placement knowing a current state of the system. Genuinely, the last placement ended at the marked box. Hence we need to take one bead from that box and then going in a counterclockwise order take one bead from every box while we can to restore the previous state. When we meet an empty box, we place all the beads we took into it and mark this box.

Let us construct an oriented graph of the states of the system. For this purpose we will denote the systems' states by points and the possibility of transfer from one state to another, by an arrow

connecting the corresponding points. There will be only one arrow going out from a point and only one arrow going in.

Let us start to move along the arrows starting with the given state  $A_1$ . We get a sequence of states  $A_2, A_3, \dots$ . We get that at some moment we will have a repetition in our sequence  $\{A_i\}$  because the number of the states is finite. Suppose, for example,  $A_k = A_l$  where  $k < l$ . As long as there is only one arrow going in the point  $A_k$  we obtain from the equality  $A_k = A_l$  that  $A_{k-1} = A_{l-1}, \dots, A_1 = A_{l-k+1}$ . Thereby we return to the state  $A_1$  after  $l - k$  moves.

**(b)** As opposed to (a) now the system's state is defined only by the way the beads are placed into the boxes. Note that if a move goes from state  $A$  to state  $B$ , then according to (a) we can (in several moves) get back from  $B$  to  $A$ . If we can get from  $A$  to  $C$  in several moves then we can get back from  $C$  to  $A$  by “rolling back” our moves one by one.

Hence if we can get from any state to some fixed state  $M$ , then we can get from any state to any other state going through  $M$ . Denote a state where all the beads lie in some fixed box  $m$  by  $M$ . Let us take the beads from the closest to  $m$  (in a clockwise order) non-empty box for each move. Then either the number of beads in  $m$  will grow or the closest to  $m$  non-empty box will get closer. Sooner or later all the beads will be in  $m$ .  $\square$

**Hint for problem 14.** A phase space for this problem is a set of all possible pairs  $(x, v)$  where  $x$  is an initial position of the ship and  $v$  is a vector in which the ship moves at each turn. It is easy to show that the phase space is countable and this condition is sufficient for constructing an algorithm for shooting.  $\square$

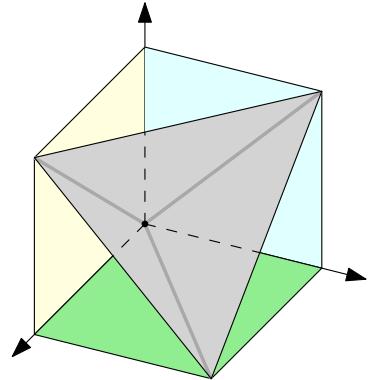
## Selected problems

**Hint for problem 15.** Construct a configuration space of the water in jugs as in problem 0 and examine how a state of the system changes under the operation of pouring water from one jug to another. See [CG, Chapter 4, §6]  $\square$

**Solution for problem 16.** Answer: it is impossible.

A configuration space for an amount of water in all three tanks is a subset  $X \subset \mathbb{R}^3$  consisting of points with non-negative coordinates. A point corresponding to a current state of the system moves in a line segment  $I$  connecting starting and ending states.

An intersection of the planes  $x + y = z$ ,  $y + z = x$ , and  $z + x = y$  with  $X$  is a boundary of an infinite triangular cone. Since the cone is convex the line segment  $I$  intersects its boundary in not more than two points. But according to the problem's statement segment  $I$  passes through at least one point from every face of the cone. Hence  $I$  passes through at least one edge of the cone. Finally note that the edges of the cone lie in the planes  $x = 0$ ,  $y = 0$ , and  $z = 0$ .  $\square$



**Solution for problem 17.** A configuration space of amounts of rabbits and wolves is the first quadrant of the plane  $\mathbb{R}^2$ . Denote the quadrant by  $X$ . The position of the system changes over time: a point with positive coordinates  $(x, y)$  moves in a velocity vector  $(a_0 - a_1 y, -b_0 + b_1 x)$ .

Note that the velocity vector is equal to the null vector at the point  $(\frac{b_0}{b_1}, \frac{a_0}{a_1})$ . Let us move the origin of the plane to this point. Then the matching each point to its velocity vector is a linear transformation  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ . Note that this linear transformation maps the  $x$  axis to the  $-y$  axis, and the  $y$  axis to the  $x$  axis. So this transformation can become a rotation by scaling coordinate axis.

Namely, consider the linear substitution

$$\tilde{x} = \frac{-b_0 + b_1 x}{\sqrt{b_1}} \quad \text{and} \quad \tilde{y} = \frac{-a_0 + a_1 y}{\sqrt{a_1}}.$$

In this new coordinate system a velocity vector of a point  $(\tilde{x}, \tilde{y})$  not from the boundary of  $X$  is written down as  $\sqrt{a_1 b_1} \cdot (-\tilde{y}, \tilde{x})$ . This means that all such points move in circles of centre in the origin of the plane. As a result the movement of all the points such that their circles do not intersect the boundary of  $X$  is periodical. If a point gets to the boundary of  $X$  then it keeps moving along the boundary with a constant speed. That is movement of such points that

$$\tilde{x}^2 + \tilde{y}^2 \leq \min \left( \frac{b_0^2}{b_1}, \frac{a_0^2}{a_1} \right),$$

is not periodic, that is the distance to the origin (in the new coordinates) is not greater than the distance to at least one of the lines  $x = 0$  and  $y = 0$ .  $\square$

**Solution for problem 18.** (a) Let us trace just the *velocities* of the balls. In a space with coordinates  $v_1, v_2$  the law of conservation of energy  $m_1 v_1^2 + m_2 v_2^2 = \text{const}$  plots an ellipse. For the sake of convenience we can multiply coordinates by positive numbers in such a way that the ellipse becomes a circle.

Namely suppose  $x = \sqrt{m_1} \cdot v_1$  and  $y = \sqrt{m_2} \cdot v_2$ . (The first ball is the furthest from the wall and we suppose that velocity is positive if it is directed towards the wall.) From the law of conservation of energy it follows that the points corresponding to the system's positions are in a circle  $x^2 + y^2 = \text{const}$ . This circle is our phase space, let us denote it by  $X$ .

A collision between a ball and the wall is represented in the phase space as a map  $(x, y) \mapsto (x, -y)$ , that is a reflection in a line  $l$  where  $l$  is the line  $y = 0$ . Note that collision can happen if and only if  $v_2 > 0$  that is if  $y > 0$ .

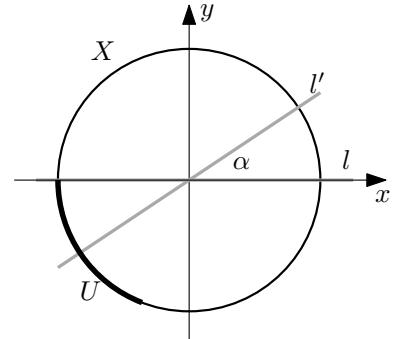
With every collision between the balls there is a reflection in a line, passing through the origin and a point  $(\sqrt{m_1}, \sqrt{m_2})$ , in the phase space. It follows from the law of conservation of momentum. Denote this line by  $l'$ , it is written as  $\frac{x}{\sqrt{m_1}} = \frac{y}{\sqrt{m_2}}$ . Note that a collision can happen if and only if  $v_1 > v_2$ , that is  $\frac{x}{\sqrt{m_1}} > \frac{y}{\sqrt{m_2}}$ .

Let us denote an angle between  $l$  and  $l'$  by  $\alpha$ . We know that  $\alpha = \arctg \frac{\sqrt{m_2}}{\sqrt{m_1}}$ . Obviously a composition of the two described transformations of  $X$  is a rotation on an angle  $-2\alpha$ .

Let us mark an ark  $[\pi; \pi + 2\alpha]$  on the circle and denote it by  $U$ . Sooner or later every point will get to the set  $U$ . In such position of the system there will be no more collisions with the wall.

(b) Suppose  $(x_0, y_0)$  is an initial state of the system. It follows from the statement of the problem that  $y_0 < 0$ . Define  $\beta$  as an angle of the vector  $(x_0, y_0)$ . Formally  $\beta = \operatorname{arcctg} \frac{x_0}{y_0} - \pi$ . Then the number of collisions between the balls is equal to  $\lceil \frac{\pi + \beta - \alpha}{2\alpha} \rceil$  and the number of collisions between the second ball and the wall is equal to  $\lceil \frac{\pi + \beta - 2\alpha}{2\alpha} \rceil$ .

We can advise you to take a look on some of the additional materials for this problem on YouTube: summarizing video [1] where the connection between the problem and the decimals for  $\pi$  is shown, video [2] with a solution in the space of velocities, and also video [3] with the solution using billiards in the space of coordinates.  $\square$



# Problems after the semifinal

Problems here are divided into two independent topics. In section 2 we study different topological properties of phase spaces that appear in problems with quite simple statements. In section 3 we deal with geometry of phase spaces, namely with transformations preserving volume. *Because of the expanse of these topics we suggest the participants to focus their effort on just one of them.*

The main results of §2 are problems  $20^m$  and  $22^m$ . The main results of §3 are problems  $42^m$  and  $51^m$ . Problems marked with asterisks require knowledge of some techniques (such as continuous mappings), if you do not know the formal definitions needed, then you do not have to solve these problems.

Sometimes we formulate some lemmas as hints for difficult problems. These lemmas tell us much about the nature of considered objects and therefore might be interesting on their own. Proofs of these lemmas are divided into smaller problems placed after the lemmas' statements.

Also we give statements of some theorems for reference, you do not need to send us their proofs.

## 2 Topology of phase spaces

### 2.1 Problem about wagons

**Problem 19.** At 9 a.m. a tourist left her home. She was walking the whole day and arrived to a camp by 9 p.m. She stayed over the night and at the next day she was walking home by the same road from 9 a.m. till 9 p.m. Her velocity is not constant and she can stop or sometimes even go back. Prove that she was in some point of the road at the same time both days.

**Problem 20<sup>m</sup>** (N. N. Konstantinov). Two nonintersecting roads lead from city A to city B. We know that two cars connected by a 10-meter rope manage to go from A to B along different roads without breaking the rope. Can two circular wagons of radius 6 meters, which centres move along the different roads in the opposite directions, pass each other without colliding?

Further we map a path to the *formal* solution for problem  $20^m$  for *piecewise-linear* trajectory of the cars and wagons. It means that the time interval is divided into finite number of parts, and velocities of the cars and wagons are constant on each part. Then we can prove the following preliminary conjecture for solving problem  $20^m$ .

**Lemma 1.** *There are two polygonal curves  $\alpha$  and  $\beta$  in a square ABCD. The polygonal curve  $\alpha$  connects vertices A and C and the polygonal curve  $\beta$ , vertices B and D. Then  $\alpha \cap \beta \neq \emptyset$ .*

The polygonal curves can be self-intersecting unless we explicitly specify otherwise.

Why don't we consider *continuous curves* instead of polygonal curves? The following problem illustrate the difficulties that may arise due to switching from piecewise-linear to continuous setting (answers for (a) and (b) are different).

**Problem 21.** There is a mountain in the middle of an even steppe. There are two paths up to the top of the mountain (these paths do not go below the steppe level). Two mountain climbers started their way to the top using different paths and staying on the same height. Is it possible to reach the top of the mountain moving continuously if (a) paths are polygonal curves; (b\*) paths are arbitrary plots of continuous functions?

(c) Solve an analogue for (a) for an arbitrary number of climbers.

Lemma 1 seems obvious, but it is difficult to give a rigorous proof for it. Hints for such a proof see in §2.3.1.

## 2.2 Rectangle inscribed in a curve

**Problem 22<sup>m</sup>.** We have a closed non self-intersecting curve in the plane. Prove that there exists a rectangle such that its vertices lie on this curve.

Consider points  $A = (0, 0)$ ,  $B = (1, 0)$ ,  $C = (1, 1)$ , and  $D = (0, 1)$  in the plane. We can define the *Möbius strip* as the square  $ABCD$  (with its interior) with sides  $AD$  and  $CB$  identified by the map  $(0, t) \mapsto (1, 1 - t)$ . Let us denote the Möbius strip by  $M$ .

The following two conjectures are useful for solving problem 22<sup>m</sup>.

**Problem 23.** Identify  $M$  with the configuration space of pairs of points in a circle.

**Lemma 2.** Suppose we have a plane  $\alpha$  in space  $\mathbb{R}^3$ . Then there is no continuous embedding  $M \rightarrow \mathbb{R}^3$  such that the boundary of  $M$  is in  $\alpha$  and all the interior points are in one of the semispaces.

(By “embedding” we mean a map such that different points of  $M$  are mapped to different points of  $\mathbb{R}^3$ .)

Generally speaking, notion of continuity is used in Lemma 2 and careful treatment for this notion is far beyond the scope of our project. Nevertheless we can prove rigorously the *piecewise-linear* variation of Lemma 2. Comments and hints for the proof see in §2.3.2.

## 2.3 Topological lemmas

### 2.3.1 Closed curves in the plane

The aim of this section is to prove Lemma 1.

**Definition.** A set of points in the plane is called *set in general position* if

- (1) any three points do not lie on a line and
- (2) any 6 of them cannot be covered by three lines passing through the same point (this point may not be in the set).

**Problem 24.** Is it true that if a set of points consists of at least 6 points then condition (1) of the definition above follows from condition (2)?

**Problem 25.** Show that any finite set of points in the plane can be transformed into a set in general position by arbitrary small movement (i. e. each point is moved by not more than some given distance).

**Problem 26.** We have a square  $ABCD$  and polygonal curves  $\alpha = A_0A_1 \dots A_m$ , and  $\beta = B_0B_1 \dots B_n$  where  $A_0 = A$ ,  $B_0 = B$ ,  $A_m = C$ ,  $B_n = D$  and the rest of the vertices are inside the square. Suppose the set of all the vertices is in general position. Then the number of intersections of  $\alpha$  and  $\beta$  is odd. (Hint: use induction on  $m$  and  $n$ .)

**Problem 27.** Is the statement of problem 26 true if for the set of vertices of  $\alpha$  and  $\beta$  the following does not hold: **(a)** condition (1) or **(b)** condition (2) from the definition of set in general position?

**Problem 28.** **(a)** Prove Lemma 1. **(b\*)** Prove the variation of Lemma 1 for continuous curves.

Likewise the following conjecture can be deduced from problem 26.

**Jordan curve theorem.** We say that a subset  $A$  of the plane is *connected* if there exists a polygonal curve between any two of its points such that the curve lies inside  $A$ . Then **(a)** any closed non self-intersecting polygonal curve divides the plane into parts (that is, complement of the curve is not connected); **(b)** moreover, there are exactly two of these parts.

### 2.3.2 Linked closed curves in space

The aim of this section is to prove Lemma 2.

**Definition.** A set of points in space is called *set in general position* if

- (1) any three points do not lie on the same line,
- (2) any four points do not lie in the same plane and
- (3) any eight points cannot be covered by two planes and a line passing through the same point (this point may not be in the set).

Polygonal curves in space are called polygonal curves in general position if the set of their vertices is a set in general position.

**Problem 29.** Show that any finite set of points in space can be transformed into a set in general position by arbitrary small movement.

**Problem 30.** Show that if a union of a set of the vertices of a closed polygonal curve in space and a set of vertices of any tetrahedron is a set in general position, then the number of intersections of the polygonal curve with the surface of the tetrahedron is even.

**Definition.** Suppose  $\alpha, \beta \subset \mathbb{R}^3$  are two closed polygonal curves in general position. Take point  $O \in \mathbb{R}^3$  in general position with their vertices. Suppose  $A_0, A_1, \dots, A_n = A_0$  are the vertices of  $\alpha$ . Let us count for  $i = 0, \dots, n-1$  a remainder modulo 2 for the number of points of intersection of the triangle  $OA_iA_{i+1}$  and polygonal curve  $\beta$ . The sum  $n$  of these remainders is called linking number of  $\alpha$  and  $\beta$  modulo 2. It is denoted by  $\text{lk}(\alpha, \beta)$ .

**Problem 31.** Show that  $\text{lk}(\alpha, \beta)$  does not depend on the choice of point  $O$ . (Hint: take point  $O'$  and consider the intersection of tetrahedrons  $OO'A_iA_{i+1}$  and polygonal curve  $\beta$ .)

(b) Show that  $\text{lk}(\alpha, \beta) \equiv \text{lk}(\beta, \alpha)$ . (By  $\equiv$  we denote congruence modulo 2.)

**Problem 32.** Suppose  $\alpha, \beta \subset \mathbb{R}^3$  are two non self-intersecting and non intersecting polygonal curves.

(a) Prove that there exists  $\varepsilon > 0$  such that for any movement of each vertex of  $\alpha$  and  $\beta$  on a distance less than  $\varepsilon$  the polygonal curves remain non self-intersecting and non intersecting.

(b) We can obtain two polygonal curves in general position  $\alpha', \beta'$  by moving the vertices of  $\alpha, \beta$  on a distance less than  $\varepsilon$ . Prove that  $\text{lk}(\alpha', \beta')$  is well-defined, i.e. it does not depend on this move.

Problem 32 allows us to define linking number modulo 2 for *arbitrary* pair of non intersecting and non self-intersecting closed polygonal curves  $\alpha, \beta \subset \mathbb{R}^2$ . We say that  $\alpha$  and  $\beta$  are *linked modulo 2* if  $\text{lk}(\alpha, \beta) \equiv 1$ .

It is convenient to use the following property of the graph  $K_6$  (complete graph with 6 vertices) for an easier proof of Lemma 2. We call a map  $K_6 \rightarrow \mathbb{R}^3$  *piecewise-linear* if images of all the edges under this map are polygonal curves.

**Lemma 3.** *For any piecewise-linear embedding  $K_6 \rightarrow \mathbb{R}^3$  there exists a pair of non intersecting cycles linked modulo 2.*

**Problem 33.** Let us denote a sum of linking numbers modulo 2 for all pairs of non intersecting cycles for a piecewise-linear embedding  $\gamma : K_6 \rightarrow \mathbb{R}^3$  by  $\text{slk}(\gamma)$ . Construct some embedding  $\gamma_0 : K_6 \rightarrow \mathbb{R}^3$  and check that  $\text{slk}(\gamma_0) \equiv 1$ .

**Problem 34.** Suppose piecewise-linear embeddings  $\gamma_1, \gamma_2 : K_6 \rightarrow \mathbb{R}^3$  are equal for all edges except one. Prove that  $\text{slk}(\gamma_1) \equiv \text{slk}(\gamma_2)$ .

**Problem 35.** Prove Lemma 3.

### 2.3.3 Embeddings of the Möbius strip into space

We call a graph  $\Gamma \subset M$  such that all its faces are triangles a *triangulation* of the Möbius strip  $M$ . Note that in such a case the boundary of  $M$  consists entirely of the edges. A map  $f : M \rightarrow \mathbb{R}^3$  is called *piecewise-linear* if for some triangulation of  $M$  map  $f$  transforms its faces into triangles in  $\mathbb{R}^3$ .

**Problem 36.** (a) Construct an embedding of  $K_6$  into  $M$  such that one of the cycles goes to the boundary of  $M$  and the other cycle, to centre line of  $M$ . Let us call these cycles  $\alpha$  and  $\beta$ .

(b) Show that if a map  $f : M \rightarrow \mathbb{R}^3$  is given then no three cycles in  $f(K_6)$  cannot be linked except  $f(\alpha)$  and  $f(\beta)$ .

**Problem 37.** Suppose we have a piecewise-linear embedding  $f : M \rightarrow \mathbb{R}^3$ . Denote the boundary of  $M$  by  $\alpha$  and denote the centre line of  $M$  by  $\beta$ . Prove that  $f(\alpha)$  and  $f(\beta)$  are linked polygonal curves in  $\mathbb{R}^3$ .

**Problem 38.** Prove that Lemma 2 for piecewise-linear embedding  $M \rightarrow \mathbb{R}^3$  follows from problem 37

**Problem 39\*.** Prove Lemma 2 for continuous embedding  $M \rightarrow \mathbb{R}^3$ .

## 3 Mirrors and billiards

### 3.1 Invisible systems of mirrors

In this section we consider *systems of mirrors*, which are formally just collections of curves in the plane. The law “the angle of reflection of a ray equals the angle of incidence” holds for light rays. Mirrors can be curved, then this law applies to a tangent line to the mirror at a point of collision. Rays hitting edges of the mirrors can be neglected. A system of mirrors have to be bounded. All the mirrors cannot be parallel to each other.

**Problem 40.** Construct a system of mirrors such that it is (a) invisible in some direction; (b) invisible in some two directions.

*Invisibility in a direction* of a line  $l$  means that every ray parallel to  $l$  and starting far enough after some number of reflections continues to follow the same line as there was no reflections at all.

**Problem 41.** (a) Suppose that all the mirrors in a system are line segments and their angles are  $0^\circ$  and  $90^\circ$ . Prove that such system of mirrors cannot be invisible in directions  $45^\circ$  and  $135^\circ$ . Angles are measured with respect to the horizontal axis.

(b) Suppose that all the mirrors in a system are line segments and their angles are  $0, \frac{\pi}{n}, \frac{2\pi}{n}, \dots, \frac{(n-1)\pi}{n}$  for some natural  $n$ . We call these directions *obtainable*.

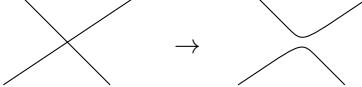
Suppose we have a finite set of lines  $l_1, \dots, l_k$ , such that any ray of light parallel to some line  $l_i$  after reflection in the mirror aligned in obtainable direction will continue its way in a direction parallel to some line  $l_j$ . Prove that such system of mirrors cannot be invisible in directions  $l_1, \dots, l_k$ .

**Problem 42<sup>m</sup>.** Prove that there is no system of mirrors invisible in all directions.

We can consider a transformation of a phase space preserving volume for solving problem 42<sup>m</sup>. Such transformations are considered further via less complex examples in problems 46 and 50. Another technique that is needed for solving problem 42<sup>m</sup> is shown in the following discrete example.

**Problem 43.** An island has a shape of a disk  $D$ . There are  $2n$  transportation hubs of  $n$  different companies on the boundary of  $D$ . Each company owns 2 hubs, that are connected by a straight railway on which trains travel from end to end. There are bridges at railway crossings so that each train moves in a straight line and cannot turn off at the crossing point.

Minister of Railway Transport decided to cut down on a number of bridges by replacing them by railway switches as shown in the figure.



Also it is required that each train continues to travel between transportation hubs of the same company. Prove that Minister cannot implement his idea.

### 3.2 Outer billiards

Suppose  $T$  is a convex bounded region in the plane  $\mathbb{R}^2$ . Consider a point  $x_0$  outside  $T$ . There exist two supporting lines (tangents) to  $T$  from the point  $x_0$ . Choose the right one of these lines looking from  $x_0$  and denote it by  $l$ . If  $l$  intersects  $T$  in one point  $y_1$ , then denote an image of  $x_0$  under the reflection in  $y_1$  by  $x_1$ .

Likewise one can construct the next point  $x_2$  using  $x_1$  (as long as the right supporting line from  $x_1$  intersects  $T$  in a unique point), etc. The map  $R$  carrying a point in the plane into its image is called the *outer billiard map* and the sequence  $x_0, x_1, x_2, \dots$  is called the *orbit of point  $x_0$* .

If at some step the supporting line intersects the boundary of  $T$  in more than one point, but by a line segment, then we say that the orbit of  $x_0$  is not defined.

**Problem 44.** Suppose  $T$  is a square in the plane. (a) Draw a set of points for which orbits are defined. (b) How to find the length of the orbit of some arbitrary point in  $\mathbb{R}^2$ ?

**Problem 45.** Solve the similar problem where  $T$  is an arbitrary triangle in the plane.

**Problem 46.** Prove that the map  $R$  preserves area (that is, for any region  $A$  non intersecting with  $T$  areas of  $A$  and  $R(A)$  are equal), (a) if  $T$  is a convex polygon; (b) if  $T$  is an arbitrary strictly convex bounded region.

Let us call an orbit  $x_0, x_1, x_2, \dots$  *almost periodic* if for any  $\varepsilon > 0$  and for some  $n \in \mathbb{N}$  the distance between  $x_0$  and  $x_n$  is less than  $\varepsilon$ .

**Problem 47\*.** Is it true that any orbit of an outer billiard  $T$  is almost periodic if

- (a)  $T$  is a convex polygon with rational vertices;
- (b)  $T$  is a convex polygon;
- (c)  $T$  is a strictly convex bounded region;
- (d)  $T$  is a convex bounded region?

We do not know a simple solution for that problem. Although the answer for similar question about interior billiards is far more easier as we will see in the next section.

### 3.3 Interior billiards

Let  $T$  be a convex bounded figure on the plane. Let us take a point  $x$  inside  $T$  and choose some unit vector of velocity for that point. This defines billiard trajectory of the point as follows: inside  $T$  the point is moving with constant velocity and on the boundary it change the velocity vector according to the law “The angle of incidence is equal to the angle of reflection” (the angles are measured between current velocity and tangent line to the boundary of  $T$  at the point of collision).

If at some moment the point  $x$  hits boundary at the point where the tangent line does not exist we say that the trajectory of  $x$  is not defined. A trajectory of the point  $x$  is said to be *periodic* if after some time since the beginning of the path,  $x$  appears in the same place with the same speed.

**Problem 48.** Let  $T$  be a square. (a) Which pairs of starting points and velocities yield periodic trajectories? (b) Show that any periodic trajectory in  $T$  has even number of reflections from the border.

Further,  $T$  can be assumed to be a convex polygon or an arbitrary convex figure with smooth boundary.

**Problem 49.** Fix some vector of velocity  $v$ . Let  $f_t(x)$  be a position of a point  $x$  after time  $t$  if it starts movement with velocity  $v$ . Show that the area of the image  $f_t(A)$  of a region  $A \subset T$  not necessarily equals the area of  $A$  (here  $f_t(A)$  consists of images for all points in  $A$  which trajectories are defined).

**Problem 50.** For any starting point  $x$  and initial velocity  $v$  consider the position and the velocity of the point after time  $t$ . This gives us a mapping  $F_t : T \times [0; 2\pi) \rightarrow T \times [0; 2\pi)$ .

(a) Show that if  $T$  is a polygon, then  $F_t$  is defined everywhere on  $T \times [0; 2\pi)$  except a set of zero volume.

(b) Show that for any  $t$  the mapping  $F_t$  preserves volume.

Consider point  $x$  with some initial velocity vector. The trajectory of  $x$  is said to be *almost periodic* if for any  $\varepsilon_1, \varepsilon_2 > 0$  there is  $t > 0$  such that the distance between  $x$  and  $f_t(x)$  is less than  $\varepsilon_1$  and the angle between velocities at point  $x$  and at point  $f_t(x)$  is less than  $\varepsilon_2$ .

**Problem 51<sup>m</sup>.** Show that almost all initial conditions  $(x, \varphi) \in T \times [0; 2\pi)$  give us an almost periodic orbit. Here “almost all” means “all except some set of zero volume in  $T \times [0; 2\pi)$ ”.

Informally, if we shine a flashlight from a random place in a mirrored room in a random direction, the light will hit the back of our head with good accuracy.

The property of volume-preserving transformations, which is proposed to prove for solving the problem 51<sup>m</sup>, can be formulated in the general case as follows:

**Poincaré recurrence theorem.** Let  $U \subset \mathbb{R}^3$  be a bounded domain,  $f : U \rightarrow U$  — a mapping which preserves volume. Consider lesser domain  $A \subset U$ . For a point  $x \in A$  consider a sequence  $f(x), f(f(x)), f(f(f(x))), \dots$ . Define  $Z \subset A$  as a set of points for which this sequence lies entirely outside of  $A$ . Then  $Z$  has zero volume.

In order to give mathematical rigor to this claim some specifications should be made about which ‘domains’ we consider and for which subsets of  $U$  the mapping  $f$  ‘preserves volume’. (Famous paradoxes [4], [5] show that *there is no way* to define a notion of volume for all subsets. For theory see e.g. [Ox]).

# Hints and solutions for problems after the semifinal

## Topology. Problem about wagons

### Closed curves in the plane

**Solution for problem 24.** The answer is “no”. Indeed (1) does not follow from (2).

Consider two parallel lines  $l, m$ . Choose three points on each of the lines:  $A_1, A_2, A_3 \in l$  and  $B_1, B_2, B_3 \in m$ . If three lines  $A_1B_i, A_2B_j, A_3B_k$  do not intersect in one point for every  $\{i, j, k\} = \{1, 2, 3\}$ , then (2) holds and (1) does not hold by construction.

Let us prove that such six points exist. Choose arbitrary points  $A_1, A_2, A_3 \in l$  and  $B_1, B_2 \in m$ . Then there are finitely many prohibited positions for the point  $B_3$ . Namely, this number is not greater than three. (For example, denote the intersection  $A_1B_1 \cap A_2B_2$  by  $C$ . Then  $B_3$  cannot lie on the intersection of  $A_3C$  and  $m$ .)  $\square$

**Solution for problem 25.** Suppose we have a set of arbitrary points  $A_1, \dots, A_n \in \mathbb{R}^2$ . We can also suppose that all the points are different because otherwise we can fix that using arbitrary small movement. Then let us move these points one by one every time making the next point to be in general position with all previous points.

Suppose the points  $A_1, \dots, A_{k-1}$  are in general position. Consider a set of positions prohibited for  $A_k$ . Firstly, this set includes all the lines  $A_iA_j$  for all possible  $i, j < k$ . Secondly, this set includes all the lines  $A_jC$  where  $C$  is the intersection point  $A_{i_1}A_{i_2} \cap A_{i_3}A_{i_4}$  for all possible  $i_1, i_2, i_3, i_4, j < k$ .

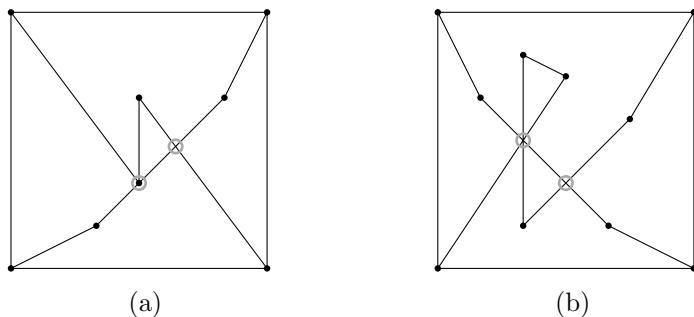
It is clear that the set of prohibited for  $A_k$  positions is a finite union of lines. Therefore we can get  $A_k$  out of this set by an arbitrary small movement.  $\square$

**Solution for problem 26.** The proof is by induction on  $m, n$ . The base of induction is trivial. If  $m = n = 1$  then the claim of the problem is that square’s diagonals intersect in an odd number of points.

Now suppose  $m > 1$ . Draw an edge  $A_{m-2}A_m$  instead of two edges  $A_{m-2}A_{m-1}$  and  $A_{m-1}A_m$  for polygonal curve  $\alpha$ . Let us prove that  $\beta$  and the triangle’s  $A_{m-2}A_{m-1}A_m$  boundary have an even number of intersection points, to show that the parity of the number of intersection points between  $\alpha$  and  $\beta$  stays the same.

Indeed, if vertices  $B_k, B_{k+1}$  are on *different sides* of the boundary  $A_{m-2}A_{m-1}A_m$  (i.e. one of the vertices lies inside the triangle and the other one lies outside), then the line segment  $B_kB_{k+1}$  intersects the boundary  $A_{m-2}A_{m-1}A_m$  in an odd number of points. But if these vertices are on the *same side*, then the intersection consist of an even number of points. Since  $A_0$  and  $A_n$  are both on the same side (i.e. they are both outside the triangle), the number of intersection points is even.  $\square$

**Solution of problem 27.** Answer: (a) no; (b) no. You can see examples in the figures below.



*Remark.* For the set of the polygonal curve’s vertices (2) does not hold in our example for (a). There is no example for (a) such that (2) holds.

It is possible to prove that a number of intersection points is always odd for (b) by adding the restriction for polygonal lines not to be self-intersecting. To do so one should take notice of the

intersection points while moving vertices of the polygonal curves to a general position (e.g. see proof of Lemma 1).  $\square$

**Solution for problem 28.** (a) Suppose  $\alpha \cap \beta = \emptyset$ . Take  $\varepsilon > 0$  such that any distance between a point from  $\alpha$  and a point from  $\beta$  is less than  $\varepsilon$ . Then, we cannot get any more points of intersection moving vertices of  $\alpha$  and  $\beta$  by not more than  $\frac{\varepsilon}{2}$  since any point on an edge also moves by not more than  $\frac{\varepsilon}{2}$ . But according to the problem 25 we can get  $\alpha$  and  $\beta$  into general position moving each vertex by not more than  $\frac{\varepsilon}{2}$ . This concludes our proof.

Note that  $\varepsilon$  can be less than the minimal distance between the vertices of  $\alpha$  and  $\beta$ . One way to compute  $\varepsilon$  is the following. Take a vertex from one polygonal curve and an edge from another curve, measure the distance between them. Do this for every possible combination of a vertex and an edge from different polygonal curves, and take  $\varepsilon$  less than any of these numbers.

(b) *Sketch of solution.* There is a way to approximate any continuous curve by a polygonal curve with accuracy of any  $\varepsilon > 0$ . This means that we draw points on a curve one by one in such a way that the distance between a curve's arc between two neighbouring points and the line segment connecting these points is less than  $\varepsilon$ . We need to construct such approximations for  $\varepsilon = \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots$ . Then for each  $\varepsilon$  we need to find an intersection point  $P_i$  of two polygonal curves. For each point  $P_i$  there are points  $A_i$  and  $B_i$  on continuous curves such that distance between  $A_i$  and  $B_i$  is not greater than  $\frac{1}{2^{i-1}}$ . Finally, we need to choose convergent subsequences with equal indices from  $A_i$  and  $B_i$  using the compactness of the line segments. These subsequences have equal limits, therefore this limit is the required intersection point of our curves.  $\square$

## Problem about wagons

**Solution for problem 19.** Let us identify the road with the line segment  $[0; 1]$ , and time with the line segment  $[9; 21]$ . Time dependences for a current position of the tourist on the road are continuous functions  $[9; 21] \rightarrow [0; 1]$ . Denote such functions for her way to the camp and back by  $f$  and  $g$  respectively. We have  $f(9) = g(21) = 0$  and  $f(21) = g(9) = 1$ .

Consider function  $h = f - g$ . Function  $h$  is negative at point 9 and positive at point 1. Using intermediate value theorem, we obtain the existence of some point  $t \in [9; 21]$  such that  $h(t) = 0$ . Therefore  $f(t) = g(t)$  for some time  $t$ , i.e. the tourist was in some point of the road at time  $t$  both days.  $\square$

**Solution for problem 20<sup>m</sup>.** Identify each road with the line segment  $[0; 1]$ . Then the phase space for the two vehicles on these roads is the square  $[0; 1] \times [0; 1]$ .

piecewise-linear movement of the cars gives us a polygonal line in the square going from the vertex  $(0, 0)$  to the vertex  $(1, 1)$ . piecewise-linear movement of the wagons gives us a polygonal line in the square going from the vertex  $(0, 1)$  to the vertex  $(1, 0)$ . Using Lemma 1, we obtain the existence of the common point for these polygonal curves. Therefore, at some time the position of the cars will be similar with the position of the wagons. Hence, it is impossible for wagons to pass each other without colliding.  $\square$

**Solution for problem 21.** (a) Answer: yes.

Suppose that there is no horizontal sections of the path. Identify each of the paths with the line segment  $[0; 1]$ . Then the set of all possible positions of the mountain climbers (on the same height) is a subset  $M$  of the square  $[0; 1] \times [0; 1]$  containing the square's vertices  $(0, 0)$  and  $(1, 1)$ .

Note that  $M$  consists of line segments. Let us consider it as a graph: states in which at least one of the climbers is in the vertex of the polygonal path are the vertices of the graph. It is easy to show that the degree of each vertex except  $(0, 0)$  and  $(1, 1)$  is even. Therefore there exists a path from  $(0, 0)$  to  $(1, 1)$ .

If some sections of the mountain are horizontal, then “collapse” these sections into points. We call these points *special*. For the new mountain the algorithm exists as was proven above. Suppose

a climber stays at this point for a minute when the climber passes through it. This adds finite amount of minutes to overall time. It is easy to obtain an algorithm for the initial mountain from this algorithm.

Also note that if no two vertices of the polygonal path are on the same height then there exists a unique way to get to the top such that the go through every position not more than one time.

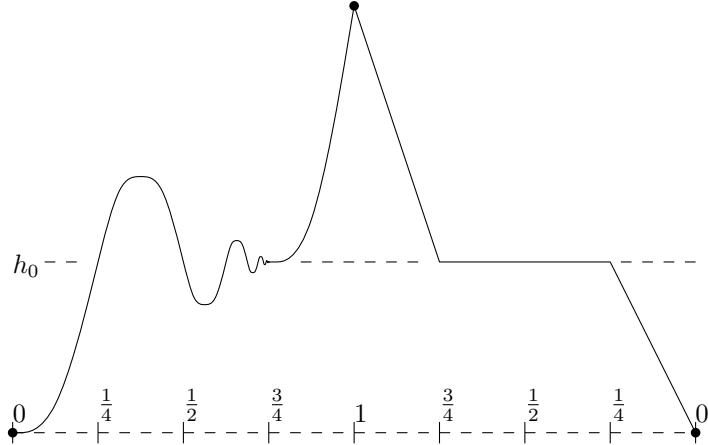
**(c)** Answer: yes. The proof is by induction on the number of climbers. The base of induction for one climber is trivial.

Consider the first two climbers and their algorithm for reaching the top from (a). Time dependence for their height is piecewise-linear. Draw the plot for this dependence and say that this is a new path to the top. Then we can swap the first two climbers for one climber moving along the new path. Thus, we can swap  $k$  climbers for  $k - 1$  climbers.

**(b)** Answer: no.

The example of such paths is shown in the figure. One of them is constructed the following way. In each of the neighbourhoods of the point  $\frac{3}{4}$  our path has both monotonically increasing section and monotonically decreasing section. Each of these sections goes through the height  $h_0$ .

The second climber needs to travel from the point  $\frac{1}{4}$  to the point  $\frac{3}{4}$  back and forth infinitely many times to get to the top. Therefore time dependence for the second climber cannot be continuous under such condition. The proof of this conjecture is a great exercise on continuous functions.



We recommend participants to draw the set  $M \subset [0; 1] \times [0; 1]$  for this mountain defined exactly as in (a), and then to show that the continuous path from the point  $(0, 0)$  to the point  $(1, 1)$  does not exist.  $\square$

## Topology. Rectangle inscribed in a curve

### Linkings of closed curves in space

**Solution for problem 29.** This solution is analogous to the solution for problem 25. Let us move the points one by one to get them into general position. The first three points we will move in such a way that they do not lie on the same line. The set of the prohibited positions of  $A_k$  after the  $k$ -th move ( $k \geq 4$ ) consists of the finite amount of planes. Therefore we can get  $A_k$  out of this set by an arbitrary small move.  $\square$

**Solution for problem 30.** Since the set of all vertices is a set in general position, neither of the polygonal line's vertices lies on the tetrahedron's surface and any of its edges can intersect the tetrahedron's surface only in interior points of the faces.

Denote vertices of the polygonal line by  $A_0, A_1, \dots, A_n = A_0$ . Colour point  $A_i$  red if it is inside the tetrahedron, otherwise colour it blue. Then the edge  $A_i A_{i+1}$  of the polygonal curve intersects

the surface of the tetrahedron in an odd number of points if and only if  $A_i$  and  $A_{i+1}$  are coloured in different colours. We have an even number of such edges.  $\square$

**Solution for problem 31.** (a) Denote the vertices of the polygonal curves  $\alpha$  and  $\beta$  by  $A_1, \dots, A_n$  and  $B_1, \dots, B_m$  respectively.

Suppose,  $\{A_1, \dots, A_n, B_1, \dots, B_m, O, O'\}$  is in general position. By problem 30 for each tetrahedron  $OO'A_iA_{i+1}$  the number of intersections of its surface with  $\beta$  is even. Then take the sum for all such tetrahedrons and we are done.

But in general  $\{A_1, \dots, A_n, B_1, \dots, B_m, O, O'\}$  may not be in general position. However, by the problem statement the sets  $\{A_1, \dots, A_n, B_1, \dots, B_m, O\}$  and  $\{A_1, \dots, A_n, B_1, \dots, B_m, O'\}$  are in general position. Choose a point  $O'' \in \mathbb{R}^3$  such that when we add  $O''$  to each of the sets it remains to be in general position. Then replace the point  $O$  by  $O''$  and then  $O''$  by  $O'$  as it was described the previous paragraph.

(b) *Hint.* Take two parallel planes in  $\mathbb{R}^3$  such that  $\alpha$  and  $\beta$  lie between them. Choose the point  $O$  on the first plane. We can compute  $\text{lk}(\alpha, \beta)$  and  $\text{lk}(\beta, \alpha)$  using the point  $O$ .

Project  $\alpha$  and  $\beta$  onto the second plane from the point  $O$ . Denote the obtained polygonal curves by  $\tilde{\alpha}$  and  $\tilde{\beta}$ . To show that  $\text{lk}(\alpha, \beta) \equiv \text{lk}(\beta, \alpha)$  it is enough to check that  $\tilde{\alpha}$  and  $\tilde{\beta}$  intersect at an even number of points. This can be proved similarly to problem 26.  $\square$

**Solution for problem 32.** (a) The proof is similar to problem 28. Take  $\varepsilon > 0$  such that the distance between any point of  $\alpha$  and any point of  $\beta$  is less than  $\varepsilon$  and also the distance between any two points on nonadjacent edges of  $\alpha$  or nonadjacent edges of  $\beta$  is less than  $\varepsilon$ . Then if we move the vertices of  $\alpha$  and  $\beta$  by the distance  $< \frac{\varepsilon}{2}$ , then intersection points do not appear since any point of any edge also moves by the distance  $< \frac{\varepsilon}{2}$ . By problem 29, we can transform  $\alpha$  and  $\beta$  to general position moving each of the vertices to the distance  $< \frac{\varepsilon}{2}$ .

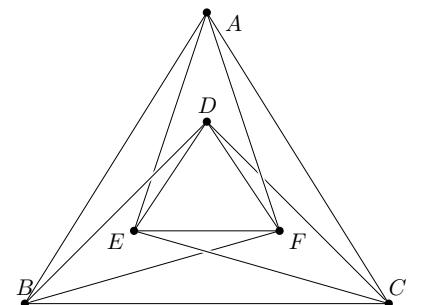
(b) Suppose the polygonal curves  $\alpha'$  and  $\beta'$  are in general position. Move one vertex  $A'_i$  of  $\alpha'$  so that when it moves, the edges  $A'_{i-1}A'_i$  and  $A'_iA'_{i+1}$  are disjoint with the other edges of  $\alpha'$  and  $\beta'$ . Denote the obtained vertex by  $A''_i$  and the obtained polygonal curve by  $\alpha''$ . Next we will show that  $\text{lk}(\alpha', \beta') \equiv \text{lk}(\alpha'', \beta')$ .

Take a point  $O$  in general position with all the vertices of  $\alpha'$  and  $\beta'$  including  $A''_i$ . Consider the intersection of the tetrahedrons  $OA'_{i-1}A'_iA''_i$  and  $OA'_iA''_iA'_{i+1}$  with  $\beta'$ . By the construction, the faces  $A'_{i-1}A'_iA''_i$  and  $A'_iA''_iA'_{i+1}$  are disjoint with  $\beta'$ . Then  $\text{lk}(\alpha', \beta') \equiv \text{lk}(\alpha'', \beta')$  by problem 30.  $\square$

**Solution for problem 33.** Take an embedding  $\gamma_0 : K_6 \rightarrow \mathbb{R}^3$  as in the figure.

For this embedding the cycle  $AEF$  is linked modulo 2 with the cycle  $DBC$ , the cycle  $BFD$  is linked modulo 2 with the cycle  $ECA$ , and the cycle  $CDE$  is linked modulo 2 with the cycle  $FAB$ .

There are no other pairs of cycles which are linked modulo 2 for this embedding  $K_6 \rightarrow \mathbb{R}^3$ . Therefore  $\text{slk}(\gamma_0) \equiv 1$ .  $\square$



**Solution for problem 34.** Suppose the embeddings  $\gamma_1, \gamma_2 : K_6 \rightarrow \mathbb{R}^3$  differ only on the edge  $AB$ . Consider the pair of cycles  $ABC$  and  $DEF$ . Denote the polygonal curve  $\gamma_1(ABC)$  by  $\alpha$ , the polygonal curve  $\gamma_2(ABC)$  by  $\alpha'$ , the polygonal curve  $\gamma_1(DEF)$  by  $\beta$ , and the union  $\gamma_1(AB) \cup \gamma_2(AB)$ , which is also a closed polygonal curve, by  $\alpha''$ . Then one can show that

$$\text{lk}(\alpha, \beta) - \text{lk}(\alpha', \beta) \equiv \text{lk}(\alpha'', \beta).$$

There are 4 pairs of cycles in  $K_6$  such that one of the cycles contains the edge  $AB$ . If we sum such the equalities for each of the pairs of the cycles, then we have

$$\text{slk}(\gamma_1) - \text{slk}(\gamma_2) \equiv \text{lk}(\alpha'', \gamma_1(DEF)) + \text{lk}(\alpha'', \gamma_1(CEF)) + \text{lk}(\alpha'', \gamma_1(CDF)) + \text{lk}(\alpha'', \gamma_1(CDE)).$$

It remains to show that the sum on the right is zero. This assertion should remind problem 30. The difference is that here instead of a tetrahedron in  $\mathbb{R}^3$  we have a piecewise-linear embedding of the graph  $K_4 = CDEF$ , and instead of the number of intersection points of  $\alpha''$  with the surface of the tetrahedron we compute the sum of linking numbers modulo 2.

Take a point  $O$  in general position with all other vertices of the polygonal curves. Then the equality of the sum on the right to zero follows by the definition of linking number modulo 2.  $\square$

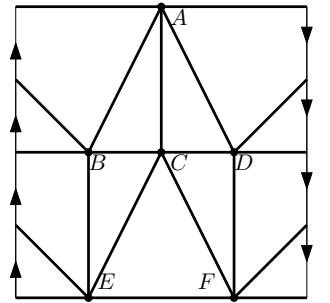
**Solution for problem 35.** By problem 34 the sum  $\text{slk}(\gamma)$  modulo 2 does not depend on the embedding  $\gamma : K_6 \rightarrow \mathbb{R}^3$ . Then by problem 33 for all embeddings  $K_6 \rightarrow \mathbb{R}^3$  we have  $\text{slk} \equiv 1$ . Therefore, for each embedding  $K_6 \rightarrow \mathbb{R}^3$  there is a pair of cycles which images are linked.  $\square$

## Embeddings of the Möbius strip into space

**Solution for problem 36. (a)** The embedding is shown in the figure.

**(b)** If a cycle in  $K_6$  bounds a polygon in  $M$ , then the image of this cycle cannot be linked with the image of any other cycle.

Let us list all the cycles of length 3 that do not bound a polygon:  $ABD$ ,  $AEF$ ,  $BCD$ ,  $BEF$ . There is only one pair of disjoint cycles:  $AEF$  and  $BCD$ . The first one of them is the curve  $\alpha$  and the second one is the curve  $\beta$ . Since  $\text{slk}(f(K_6)) \equiv 1$ , we have  $\text{lk}(\alpha, \beta) \equiv 1$ .  $\square$



**Solution for problem 37.** If  $K_6$  is embedded into  $M$  as in problem 36 (a), then  $f$  sets a piecewise-linear embedding  $K_6 \rightarrow \mathbb{R}^3$ . It remains to use problem 36 (b).  $\square$

**Solution for problem 38.** Suppose such an embedding exists. As we have shown in problem 37, the image of the boundary of  $M$  must be linked with the image of the centre line of  $M$ . But then the image of the boundary lies in a plane and the image of the centre line lies in one of the semispaces. Therefore these curves cannot be linked, so we have a contradiction.  $\square$

**Solution for problem 39\*.** One can try to reduce this problem to the piecewise-linear one, similarly to the proof of problem 28 (b). The difficulty is that the piecewise-linear maps  $M \rightarrow \mathbb{R}^3$  which approximate the given continuous embedding also must be *embeddings*. It is hard to control this condition.

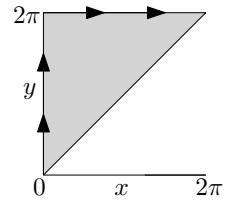
Another way that is much easier is to define the linking number modulo 2 for a pair of closed continuous curves in  $\mathbb{R}^3$ . To this end we approximate the curves by polygonal lines. One can show that if approximations are sufficiently close to the original curves then their linking number modulo 2 does not depend on the choice of the approximations. Further, we have to show that if one of the curves bounds a disk (continuously embedded into  $\mathbb{R}^3$ ) which is disjoint from the other curve, then the linking number equals zero.

For more conceptual approaches to the definition of the linking number for closed continuous curves in  $\mathbb{R}^3$  see [H, §1.2] and [FF, 17.6].  $\square$

## Rectangle inscribed in a curve

**Solution for problem 23.** We assign to each unordered pair of points in the circle an ordered pair of points  $x \leq y$  in the segment  $[0; 2\pi]$ .

Then pairs  $(0, a)$  and  $(a, 2\pi)$  of points in the segment correspond to the same pair of points in the circle. So the configuration space of pairs of points in the circle can be identified with the triangle glued as in the figure to the right. We suggest the participations to prove it.



Note that the boundary of  $M$  corresponds to the set of pairs of coinciding points.  $\square$

**Solution for problem 22<sup>m</sup>.** We denote the circle by  $S^1$ . Suppose we are given a continuous map  $\gamma : S^1 \rightarrow \mathbb{R}^2$ . We assume  $\mathbb{R}^2$  to be embedded into  $\mathbb{R}^3$  as the plane  $z = 0$ .

Next we define the map of the configuration space of pairs of points in the circle to  $\mathbb{R}^3$  as follows. We set the image of an unordered pair  $(a, b)$  to be the point  $(\frac{\gamma(a)+\gamma(b)}{2}, |\gamma(a) - \gamma(b)|)$ . Here  $\frac{\gamma(a)+\gamma(b)}{2}$  is the middle point of the segment in  $\mathbb{R}^2$  connecting  $\gamma(a)$  with  $\gamma(b)$ .

We obtain a map  $M \rightarrow \mathbb{R}^3$ . Note that the image of the boundary of  $M$  coincides with the given curve  $\gamma$ . According to Lemma 2 this map cannot be an embedding. So there are two different pairs of points in  $\gamma$  such that the segments between them have the same middle point and the same length. These four points are the vertices of a rectangle.

This proof is shown in the video [6] on YouTube. □

## References

- [CG] H. S. M. Coxeter, S. L. Greitzer, *Geometry Revisited*, New Mathematical Library, Volume 19, Washington, AMM, 1967.
- [FF] A. Fomenko, D. Fuchs, *Homotopical Topology*, Springer, 2016.
- [H] A. Hatcher, *Algebraic topology*, Cambridge University Press, 2002.
- [Ox] J. C. Oxtoby, *Measure and Category*, Springer, 1980.
- [Sh] A. Shiryaev, *Probability*, Springer-Verlag, 2016.
- [S] A. Sossinski, *Geometries*, IUM, Moscow, 2012.
- [1] <https://www.youtube.com/watch?v=HEfHFsfGXjs>
- [2] <https://www.youtube.com/watch?v=jsYwFizhncE>
- [3] <https://www.youtube.com/watch?v=brU5yLm9DZM>
- [4] Wikipedia. *Example of non-measurable set*
- [5] Wikipedia. *Banach-Tarski paradox*
- [6] <https://www.youtube.com/watch?v=AmgkSdhK4K8>

# Кубики фокусов и циркулярные кубики

А.Заславский, П.Кожевников

(На ЛКТГ проект представляют Д.Дёмин, М.Дидин, А.Заславский,  
О.Заславский, К.Иванов, П.Кожевников, Ф.Нилов, И.Фролов)

*Карлсон спланировал на пол и приземлился возле Малыша.*

*— Пока тебя не будет, я хочу заняться чем-нибудь интересным.*

*У тебя правда нет больше паровых машин?*

*— Нет, — ответил Малыш. — Машина нет, но есть кубики.*

*А.Линдгрен*

Одной из основных целей проекта является изучение так называемой кубики фокусов. Она может быть определена разными способами, например, как множество точек, из которых два данных отрезка видны под равными направленными углами. В процессе изучения обнаруживаются интересные взаимные связи между разными сюжетами элементарной геометрии (вписанные углы, пересекающиеся окружности и т.д.), геометрическими преобразованиями (симметрия, инверсия, изогональное сопряжение и др.), и свойствами кубических кривых (сложение точек на кубике и др.).

Содержание и схема зависимостей частей:

- В разделах 0 — 3 изучаются некоторые (интересные сами по себе) геометрические конструкции и развивается геометрический аппарат (преобразования и пр.), используемый далее. В разделах 0 — 3 НЕТ КУБИК, и любители элементарной геометрии могут заниматься ими и не переходя к дальнейшему. Раздел 4 полностью посвящен кубикам, но во многих задачах последующих разделов КУБИКИ НЕ ПОТРЕБУЮТСЯ.

- В части 0 собраны известные факты об изогональном сопряжении (см. также, например, [9] (т. об изогоналях), [13] (изогональные шестерки, использование при решении задач), [3]). Здесь же даются вводные результаты о кубике фокусов.

- Отметим, что среди задач 1 и 2 части есть важные, но не так широко известные факты.

- Часть 3 — отступление в некоторый отдельный сюжет; далее эта часть практически не используется.

- В части 4 собраны некоторые общие факты о кубиках и задачи, связанные с этими фактами, которые окажутся полезными далее в частях 5 и 6. Особо отметим важность сюжета, связанного с теоремой о 9 точках и с операцией сложения точек на кубике: для некоторых вопросов (в том числе сформулированных в терминах элементарной геометрии) язык кубик оказывается наиболее «правильным». Здесь мы старались, чтобы базовых фактов было немного (иначе часть разрослась бы до большого проекта по кубикам), а с другой стороны — чтобы их хватало для эффективной работы с кубиками в частях 5 и 6. Приветствуется (но не обязательно) более подробное знакомство с кубическими кри-

выми (см., например, [6], [12], [10]), еще лучше — владение начальным курсом по алгебраическим кривым (см., например, [11]).

- Части 5 и 6 — основные. Здесь представлены насыщенные красивыми фактами геометрические «площадки», на которых происходит взаимодействие идей элементарной и алгебраической геометрии.

В некоторых задачах рассматриваются сюжеты, относящиеся не к общему, а к некоторому специальному случаю (например, случаю вписанного, описанного, вырожденного четырехугольника, параллелограмма, и т.д.) В таких задачах после номера даем соответствующую пометку в звездочках.

# 0 Изогональное сопряжение в многоугольниках

## Изогонали относительно угла (пары прямых)

Пусть на плоскости даны точки  $O, X, Y, X', Y'$ .

**Определение.** Скажем, что точки  $X$  и  $X'$  (или прямые  $OX$  и  $OX'$ ) являются *изогональными* относительно угла  $YOY'$  (или, лучше сказать, относительно пары прямых  $OY, OY'$ ), если прямые  $OX$  и  $OX'$  симметричны относительно биссектрисы угла  $YOY'$ .

Тот факт, что прямые  $OX$  и  $OX'$  являются изогоналями относительно угла  $YOY'$  условимся иногда для краткости обозначать  $Isog_O(XX', YY')$ .

**0.1.** Пусть прямые  $OX, OX', OY, OY'$  различны.

Докажите, что условие  $Isog_O(XX', YY')$  эквивалентно каждому из условий:

- a)  $Isog_O(YY', XX')$ ;
- b) пары прямых  $OX, OX'$  и  $OY, OY'$  имеют общую пару биссектрис;
- c)  $\angle(OX, OY) = \angle(OY', OX')$ , т.е. отрезки  $XY$  и  $Y'X'$  видны из  $O$  под равными направленными углами (в зависимости от расположения точек это условие может означать одно из равенств  $\angle XOY = \angle Y'OX'$ ,  $\angle XOY + \angle Y'OX' = 180^\circ$ , скажем, если  $O$  лежит внутри выпуклого четырехугольника  $XYX'Y'$ , выполнено второе равенство).
- d)  $\rho(X, OY)/\rho(X, OY') = \rho(X', OY')/\rho(X', OY)$  (где  $\rho(X, \ell)$  — ориентированное расстояние от точки  $X$  до прямой  $\ell$ ).
- e) Проекции  $X$  и  $X'$  на  $OY$  и  $OY'$  (в случае если все четыре проекции различные) лежат на одной окружности.

**0.2. Теорема об изогоналях.** Пусть  $Z = XY \cap X'Y'$  и  $Z' = X'Y \cap XY'$  (так, что  $X, X', Y, Y', Z, Z'$  — вершины полного четырехсторонника). Тогда из  $Isog_O(XX', YY')$  следует  $Isog_O(XX', ZZ')$  (и аналогично  $Isog_O(ZZ', YY')$ ).

Иногда мы будем задействовать *бесконечно удаленные точки* плоскости (фактически при этом мы переходим на проективную плоскость). Можно считать, что обычная плоскость пополнена так называемой бесконечно удаленной прямой. Каждая точка этой прямой считается общей точкой всех прямых, параллельных друг другу.

**0.3.**

- a) Определите условие  $Isog_O(XX', YY')$  для бесконечно удаленной точки  $O$ .
- b) Сформулируйте и докажите теорему об изогоналях для бесконечно удаленной точки  $O$ .
- c) **Прямая Ньютона-Гаусса.** Докажите, что середины трех диагоналей четырехсторонника лежат на одной прямой.

## Изогональное сопряжение в треугольнике

**0.4.** Пусть дан треугольник  $ABC$  и не лежащая на его сторонах точка  $P$ . Докажите, что прямые, симметричные  $AP, BP, CP$  относительно биссектрис углов

$A, B, C$  соответственно, пересекаются в одной точке (возможно, бесконечно удаленной).

**Определение.** Если указанные в задаче прямые пересекаются в точке  $P'$ , то эта точка называется *изогонально сопряженной* точке  $P$  относительно треугольника  $ABC$ . (Если же прямые параллельны, то изогонально сопряженной к точке  $P$  считается соответствующая бесконечно удаленная точка.)

Очевидно, что, если  $P'$  изогонально сопряжена с  $P$ , то и  $P$  изогонально сопряжена с  $P'$ . Поэтому можно говорить о паре изогонально сопряженных точек. Изогонально сопряженными можно считать также вершину треугольника и любую точку противоположной стороны.

**0.5.** Докажите, что точка, изогонально сопряженная  $P$ , является бесконечно удаленной, тогда и только тогда, когда  $P$  лежит на описанной окружности треугольника  $ABC$ .

**0.6.** Пусть точки  $P_a, P_b, P_c$  симметричны точке  $P$  относительно сторон треугольника. Докажите, что центр описанной окружности треугольника  $P_aP_bP_c$  совпадает с точкой  $P'$ .

**0.7.** Докажите, что проекции изогонально сопряженных точек  $P, P'$  на стороны треугольника  $ABC$  лежат на одной окружности (эта окружность называется *недальней окружностью* каждой из точек  $P, P'$ ).

**0.8.** Пусть точки  $P, P'$  изогонально сопряжены относительно треугольника  $ABC$ . Докажите, что существует коника с фокусами  $P, P'$ , касающаяся прямых  $AB, BC, CA$ .

**0.9.** Пусть  $X, X'$  и  $Y, Y'$  — две пары точек, изогонально сопряженных относительно треугольника  $ABC$ . Докажите, что точка пересечения прямых  $XY$  и  $X'Y'$  изогонально сопряжена точке пересечения прямых  $XY'$  и  $X'Y$ .

## Изогональное сопряжение в четырехугольнике

Пусть фиксированы четыре различные точки  $A, A', B, B'$  (не все лежащие на одной прямой). Далее под четырехугольником  $ABA'B'$  понимаем точки  $A, B, A', B'$  в данном циклическом порядке (в частности, ломаная  $ABA'B'$  может быть самопересекающейся).

**0.10.** Пусть даны четырехугольник  $ABA'B'$  и точка  $X$ . Пусть изогонали прямых  $AX, BX, A'X$  относительно углов  $A, B, A'$  четырехугольника соответственно, пересекаются в одной точке  $X'$  (возможно, бесконечно удаленной). Докажите, что изогональ прямой  $B'X$  относительно угла  $B'$  тоже проходит через  $X'$ .

**Определение.** В случае выполнения условия задачи будем называть точки  $X, X'$  *изогонально сопряженными* относительно четырехугольника  $ABA'B'$ . (Вершины  $A$  и  $A'$  (и также  $B$  и  $B'$ ) считаем изогонально сопряженными друг с другом.)

Множество точек, для которых существует изогонально сопряженная, будем обозначать  $ISO(ABA'B')$ .

Таким образом,  $X$  и  $X'$  изогонально сопряжены относительно  $ABA'B'$ , если выполнены условия  $Isoga(BB', XX')$ ,  $Isog_{A'}(BB', XX')$ ,  $Isog_B(AA', XX')$ ,

$Isog_B'(AA', XX')$ . Предыдущая задача показывает, что достаточно наложить три из четырех указанных условий (тогда оставшееся следует автоматически).

**0.11.** Докажите, что  $X \in ISO(ABA'B')$  равносильно условию  $Isog_X(AA', BB')$ .

Вспомним, что условие  $Isog_X(AA', BB')$  означает, что  $AA'$  и  $BB'$  видны из  $X$  под равными направленными углами; это согласуется с английским названием *Isoptical cubic* для  $ISO(ABA'B')$ .

**0.12.** (Изогональная шестерка) Рассматриваем шестерку (а точнее, тройку пар) точек  $(A, A'; B, B'; C, C')$  (разрешаем совпадение только точек внутри пары  $A$  и  $A'$  и т.д.)

a) Докажите, что  $C$  и  $C'$  изогонально сопряжены относительно  $ABA'B'$  тогда и только тогда, когда  $A$  и  $A'$  изогонально сопряжены относительно  $BCB'C'$ .

b) Если из шести условий  $Isog_A(BB', CC')$ ,  $Isog_A'(BB', CC')$ ,  $Isog_B(AA', CC')$ ,  $Isog_B'(AA', CC')$ ,  $Isog_C(AA', BB')$ ,  $Isog_C'(AA', BB')$  выполнены любые три, то выполнены и оставшиеся три.

**0.13.** Пусть никакие три из точек  $A, B, A', B'$  не лежат на одной прямой. Докажите, что точки  $X$  и  $X'$  изогонально сопряжены относительно  $ABA'B'$  тогда и только тогда, когда они изогонально сопряжены относительно некоторых двух из четырех треугольников, образованных прямыми  $AB, BA', A'B', B'A$ .

**0.14.** Пусть никакие три из точек  $A, B, A', B'$  не лежат на одной прямой. Докажите, что условие  $X \in ISO(ABA'B')$  равносильно каждому из следующих условий:

a) Проекции  $X$  на прямые  $AB, AB', A'B, A'B'$  лежат на одной окружности или прямой (при этом на той же окружности лежат и проекции  $X'$ , если эта точка не бесконечно удаленная).

b) Существует коника с фокусом  $X$ , касающаяся прямых  $AB, AB', A'B, A'B'$  (при этом второй фокус — это  $X'$ ).

c) Существует пирамида  $SABA'B'$ , все плоскости граней которой касаются сферы, и  $X$  — точка касания сферы и плоскости  $ABA'B'$ .

**0.15.** Найдите множество середин отрезков  $XX'$ , где  $X$  пробегает  $ISO(ABA'B')$ , а  $X'$  — изогонально сопряженная точка для  $X$ .

**0.16. (\*КОЛЛИНЕАРНЫЕ\*)** Определим  $ISO(ABA'B')$  для коллинеарных точек  $A, B, A', B'$  как множество точек  $X$ , для которых выполнено  $Isog_X(AA', BB')$ . Найдите  $ISO(ABA'B')$

a) в случае, когда точка  $A = A'$  расположена на отрезке  $BB'$ ;

b) в случае, когда векторы  $\vec{AB}$  и  $\vec{B'A'}$  сонаправлены, но не равны.

Продолжим изучать  $ISO(ABA'B')$  в разделе 5.

# 1 Изоциклические инволюции

Несложная конструкция с окружностями позволяет определить следующие преобразования (инволюции), которые назовем *изоциклическими*.

Пусть фиксированы четыре различные точки  $A, B, C, D$ . Пусть преобразование  $f_{AB,CD}$  сопоставляет точке  $X$  точку  $Y$ , являющуюся второй точкой пересечения окружностей (прямых)  $(ABX)$  и  $(CDX)$  (отметим, что  $Y$  не определена однозначно для некоторых «нерегулярных» точек  $X$ ).

Определенные выше преобразования интересны и сами по себе, и, как оказалось, с помощью них удобно формулировать и доказывать многие утверждения.

## 1.1.

а) Положение точки  $X$  «почти всегда» определяется (направленными) углами, под которыми из  $X$  видны данные отрезки  $AB$ ,  $BC$  и т.д. Определите  $f_{AB,CD}$  в терминах преобразования этих углов.

б) Докажите, что  $f_{AB,CD}$  переводит окружность, проходящую через  $A$  и  $D$ , в окружность, проходящую через  $B$  и  $C$ .

## 1.2.

а) (Теорема Клиффорда, переформулировка). Докажите, что

$$f_{AB,CD} f_{BC,DA} = f_{BC,DA} f_{AB,CD}.$$

б) Как доопределить композицию  $f_{AB,CD} f_{BC,DA}$  на «нерегулярных» точках? (в частности, какая точка — образ точки  $A$ ? бесконечно удаленной точки?)

## 4-орбиты

Для данных точек  $A, B, A', B'$  пара (перестановочных) преобразований  $f_{AB,A'B'}$ ,  $f_{AB',A'B}$  (а точнее, группа из четырех преобразований  $f_{AB,A'B'}$ ,  $f_{AB',A'B}$ ,  $f_{AB,A'B'} f_{AB',A'B}$  и тождественного преобразования  $Id$ ) дает разбиение «регулярных» точек плоскости на 4-орбиты вида:  $X, Y = f_{AB,A'B'}(X), Y' = f_{AB',A'B}(X)$  и  $X' = f_{AB,A'B'}(Y') = f_{AB',A'B}(Y)$ . Точки  $A, A', B, B', X, X', Y, Y'$  образуют «замкнутую конструкцию» (Клиффорда) из 8 точек и 8 окружностей, обладающую богатой комбинаторной симметрией: любые две из четырех равноправных неупорядоченных пар  $(A, A')$ ,  $(B, B')$ ,  $(X, X')$ ,  $(Y, Y')$  образуют 4-орбиту для других двух пар. Три пары из указанных четырех образуют конструкцию, на которую обратим отдельное внимание в разделе 3.

1.3. (\*ВПИСАННЫЙ\*) Пусть точки  $A, B, A', B'$  — на одной окружности  $\Omega$  с центром  $O$ .

- Чем является в таком случае  $f_{AB,A'B'}$ ?
- Найдите множество неподвижных точек для  $f_{AB,A'B'}$ .
- Найдите 4-орбиту точки  $O$ .
- Докажите, что каждая 4-орбита лежит на одной окружности (прямой);
- и все эти окружности соосны.

1.4. (\*ПАРАЛЛЕЛОГРАММ\*) Пусть  $ABA'B'$  — параллелограмм.

- Докажите, что в таком случае  $f_{AB,A'B'} f_{AB',A'B}$  — центральная симметрия.

- b) Докажите, что каждая 4-орбита — параллелограмм  $XYX'Y'$ , углы которого равны углам параллелограмма  $ABA'B'$ .
- c) Пусть  $P$  — произвольная точка,  $O_1, O_2, O_3, O_4$  — центры описанных окружностей треугольников  $ABP, BA'P, A'B'P, B'AP$ . Докажите, что угол между прямыми  $O_1O_3$  и  $O_2O_4$  не зависит от выбора точки  $P$ .
- d) Пусть параллелограмм  $ABA'B'$  — педальный четырехугольник для четырехугольника  $CDC'D'$  и точки  $P$ . Докажите, что  $f_{CD,C'D'}f_{CD',C'D}(P)$  — точка пересечения диагоналей  $CDC'D'$ .

## 8-орбиты и квартеты

Для данных точек  $A, B, C, D$  можно рассмотреть все три (попарно перестановочных) инволюции  $f_{AB,CD}, f_{AC,BD}, f_{AD,BC}$  (а точнее, группу  $G$  из восьми преобразований, порожденную ими). Это дает разбиение «регулярных» точек плоскости на *8-орбиты* (каждая 8-орбита может быть представлена как объединение двух 4-орбит).

Инволюция  $g_{A,B,C,D} = f_{AB,CD}f_{AC,BD}f_{AD,BC}$  интересна тем, что не зависит от порядка точек в четверке  $A, B, C, D$ .

Можно рассматривать в  $G$  только подмножество  $H$  преобразований, равных произведению четного количества изоциклических инволюций. Таких преобразований — 4 (включая *Id*), и как мы увидим далее в разделе 2, все они круговые. Орбиты относительно действия  $H$  мы назовем *квартетами*. Четверка  $A, B, C, D$  является одним из квартетов. Каждая 8-орбита может быть представлена как объединение пары квартетов, которые переводятся друг в друга инволюцией  $g_{A,B,C,D}$ .

Эту насыщенную конструкцию продолжим обсуждать в разделе 6.

## 2 Инверсия+симметрия

**2.1.** Докажите, что

- a) описанные окружности четырех треугольников, образованных прямыми  $AB, AB', A'B, A'B'$ , пересекаются в одной точке (*точка Микеля*);
- b) точка Микеля — центр поворотной гомотетии, переводящей  $\vec{XY}$  в  $\vec{X'Y'}$ .

**Определение.** *Инверсия+симметрия* с центром в точке  $O$  — это композиция инверсии относительно некоторой окружности  $\omega$  с центром  $O$  и осевой симметрии относительно некоторой прямой  $\ell$ , проходящей через  $O$ .

Для данной четверки точек  $X, X', Y, Y'$  пусть  $\varphi_{XYX'Y'}$  — единственное круговое преобразование 1 типа (=дробно-линейное преобразование полной комплексной плоскости), меняющая местами точки  $X \leftrightarrow X', Y \leftrightarrow Y'$ .

Если середины отрезков  $XX'$  и  $YY'$  совпадают (далее этот случай называем центрально-симметричным, или случаем ПАРАЛЛЕЛОГРАММА), то  $\varphi_{XYX'Y'}$  — центральная симметрия. Иначе (регулярный случай)  $\varphi_{XYX'Y'}$  — инверсия+симметрия, центр которой совпадает с центром в точке Микеля  $M = M_{XYX'Y'}$ .

Фиксированная инверсия+симметрия позволяет одновременно «увидеть» все регулярные четверки точек. Точное утверждение на этот счет:

**2.2.** (универсальность  $\varphi$ ) Пусть  $\varphi$  — фиксированная инверсия+симметрия с центром  $O$ . Для каждой (регулярной) четверки точек плоскости  $(X, X'; Y, Y')$  существует ровно две симметричные относительно  $O$  четверки  $(A, \varphi(A); B, \varphi(B))$ , подобные (с сохранением ориентации) четверке  $(X, X'; Y, Y')$ .

В следующей задаче указана важная связь с изоциклическими инволюциями.

**2.3. (split)** Докажите, что

$$\varphi_{ABCD} = f_{AB,CD} f_{BC,AD}.$$

**2.4.**

- a) Докажите, что  $\varphi_{ABCD} \varphi_{ACBD} = \varphi_{ACBD} \varphi_{ABCD}$ .
- b) Чему равна эта композиция?

Ниже для точек Микеля (=центры инверсий+симметрий) и соответствующих инверсий+симметрий используем также более короткие обозначения (которые согласуются с [15]):  $X = M_{ABDC}, Y = M_{ABCD}, Z = M_{ACBD}, \varphi_X = \varphi_{ABDC}, \varphi_Y = \varphi_{ABCD}, \varphi_Z = \varphi_{ACBD}$ . Также полагаем  $P_X = AD \cap BC, P_Y = BD \cap AC, P_Z = CD \cap AB$ .

**2.5.** Докажите, что  $\varphi_X(P_Y) = P_Z$ .

(Отметим, что этот факт согласуется с теоремой об изогоналях.)

**2.6.** Докажите, что  $\varphi_X(Y) = Z$ .

Видим, что можно зафиксировать преобразования  $\varphi_X, \varphi_Y, \varphi_Z$  и варировать квартет  $A, B, C, D$  — далее см. раздел 6.

### 3 Гармонические шестерки точек

На плоскости (пополненной точкой  $\infty$ ) будем рассматривать упорядоченные шестерки (а точнее, тройки неупорядоченных пар) точек  $(A, A'; B, B'; C, C')$ . Допускаем совпадение точек в парах  $A$  и  $A'$ ,  $B$  и  $B'$ ,  $C$  и  $C'$ .

**Определение.** Шестерку  $(A, A'; B, B'; C, C')$  назовем *гармонической*, если выполнено равенство

$$\frac{a - b'}{b' - c} \cdot \frac{c - a'}{a' - b} \cdot \frac{b - c'}{c' - a} = -1, \quad (1)$$

где  $a, a'$  и т.д. — комплексные числа, отвечающие точкам  $A, A'$  и т.д.

**3.1.** Докажите, что условие гармоничности шестерки  $(A, A'; B, B'; C, C')$  сохраняется при

- a) обменах пар  $(A, A') \leftrightarrow (B, B')$ ,  $(B, B') \leftrightarrow (C, C')$ ,  $(C, C') \leftrightarrow (A, A')$ ;
- b) обменах точек внутри пар  $(A, A')$ ,  $(B, B')$ ,  $(C, C')$ ;
- c) выбора комплексной системы координат на плоскости;
- d) при круговых преобразованиях (см., например, книгу [7]).

**3.2.** Пятерка точек  $A, A', B, B', C$  единственным образом дополняется до гармонической шестерки  $(A, A'; B, B'; C, C')$ .

#### 3.3.

a) Шестерка  $(A, A'; B, B'; C, C')$  является гармонической тогда и только тогда, когда  $C' = \varphi_{ABA'B'}(C)$ , или  $\varphi_{ACA'C'} = \varphi_{ABA'B'}$ .

b) Пусть  $A, A'; B, B'; C, C'; D, D'$  — восемь точек (разрешены совпадения точек только в парах  $A, A'$  и т.д.) Пусть шестерки  $(A, A'; B, B'; C, C')$  и  $(A, A'; B, B'; D, D')$  являются гармоническими. Тогда и шестерка  $(A, A'; C, C'; D, D')$  является гармонической.

Заметим дополнительно, что если при этом  $\varphi_{ACA'C'} = \varphi_{ABA'B'} = \varphi$  — это центральная симметрия, то середины  $AA'$ ,  $BB'$ ,  $CC'$  совпадают, и соответствующая гармоническая шестерка  $(A, A'; B, B'; C, C')$  является центрально-симметричной. Иначе (если  $\varphi$  — это инверсия+симметрия), то середины  $AA'$ ,  $BB'$ ,  $CC'$  различны, и скажем, что гармоническая шестерка  $(A, A'; B, B'; C, C')$  *регулярная*. Фиксированная инверсия+симметрия позволяет «увидеть» все регулярные гармонические шестерки в виде «подобной копии»  $(A, \varphi(A); B, \varphi(B); C, \varphi(C))$ .

**3.4.** Пусть  $(A, A'; B, B'; C, C')$  — гармоническая шестерка. Тогда

$$\angle(AB, AC) + \angle(AB', AC') = \angle(A'B, A'C) + \angle(A'B', A'C').$$

### Гармоничность и композиции поворотных гомотетий

Условимся обозначать через  $h_{X,Y \rightarrow Z}$  поворотную гомотетию с центром  $X$ , которая переводит точку  $Y$  в точку  $Z$ .

Рассмотрим следующие соотношения (здесь  $R$  и  $L$  выбраны для соотношений на углы (rotation) и длины (lengths); последовательность  $A'B'C'$  однозначно задает циклический порядок  $BA'CB'AC'$ ):

$$\angle(\overrightarrow{A'B}, \overrightarrow{A'C}) + \angle(\overrightarrow{B'C}, \overrightarrow{B'A}) + \angle(\overrightarrow{C'A}, \overrightarrow{C'B}) = 0, \quad (R - A'B'C')$$

где под углом  $(\vec{a}, \vec{b})$  понимаем угол вращения против часовой стрелке от направления  $\vec{a}$  до направления  $\vec{b}$ , взятый по модулю  $2\pi$ .

$$\frac{BA'}{A'C} \cdot \frac{CB'}{B'A} \cdot \frac{AC'}{C'B} = 1. \quad (L - A'B'C')$$

### 3.5.

- a) Докажите, что шестерка  $(A, A'; B, B'; C, C')$  является гармонической тогда и только когда выполнены условия  $(R - A'B'C')$  и  $(L - A'B'C')$ .
- b) Докажите, что шестерка  $(A, A'; B, B'; C, C')$  является гармонической тогда и только когда  $h_{B', C \rightarrow A} h_{A', B \rightarrow C} h_{C', A \rightarrow B} = Id$ .
- c) (обобщенная теорема Наполеона) Выведите из  $(R - A'B'C')$  и  $(L - A'B'C')$  условие  $(L - C'AB')$ .
- d) Опишите построение центра композиции двух данных поворотных гомотетий.
- e) Среди условий вида  $(R - \dots)$ ,  $(L - \dots)$  укажите пары условий, из которых вытекают все остальные условия.

Некоторые конструкции с условиями  $(R - A'B'C')$  и  $(L - A'B'C')$  рассматриваются в статье [4]. Эти условия сформулированы в форме условия существования четверки точек  $X, Y, Z, T$  такой, что  $AC'B \sim XTY$ ,  $BA'C \sim YTZ$ ,  $CB'A \sim ZTX$ . В [8], например, показаны примеры, как обобщенная теорема Наполеона работает в некоторых конструкциях с «нашлётками»  $BA'C$ ,  $CB'A$ ,  $AC'B$  на сторонах треугольника  $ABC$ : если удовлетворяются условия  $(R - A'B'C')$  и  $(L - A'B'C')$ , то, согласно  $(L - C'AB')$ , углы треугольника  $A'B'C'$  выражаются только через углы «нашлёток», назависимо от углов треугольника  $ABC$ .

**3.6.** Установите следующее описание: шестерка точек  $(A, A'; B, B'; C, C')$ , в которой  $A \neq A'$  и  $B \neq B'$ , является гармонической в точности в следующих ситуациях:

- 1) окружности (прямые)  $(ABC')$ ,  $(A'BC)$ ,  $(AB'C)$ ,  $(A'B'C')$  попарно различны и имеют общую точку;
- 2)  $A, A', B, B', C, C'$  — точки на одной окружности такие, что  $AA'$ ,  $BB'$ ,  $CC'$  конкурентны, либо коллинеарные точки, переводящиеся круговым преобразованием в такую конциклическую шестерку.

### 3.7.

- a) Докажите, что изогональная шестерка  $(A, A'; B, B'; C, C')$  является гармонической.
- b) Докажите, что гармоническая шестерка  $(A, A'; B, B'; C, C')$  с условием  $Isoga(BB', CC')$  является изогональной.
- c) Докажите, что регулярная гармоническая шестерка  $(A, A'; B, B'; C, C')$ , для которой середины  $AA'$ ,  $BB'$ ,  $CC'$  коллинеарны, является изогональной.

## 4 Некоторые сведения о кубиках

**Определение.** Алгебраической кривой на (комплексной) плоскости называется множество точек с (комплексными) координатами  $(x, y)$ , удовлетворяющих уравнению  $F(x, y) = 0$ , где  $F(x, y)$  — многочлен от двух переменных, вообще говоря с комплексными коэффициентами. Порядком алгебраической кривой называется наименьшая из степеней задающих ее многочленов.

Алгебраические кривые порядка 2 и 3 называют также *кониками* и *кубиками*.

**Определение.** Однородными координатами точки проективной (комплексной) плоскости называется тройка не равных одновременно нулю (комплексных) чисел  $(x : y : z)$ , определенная с точностью до общего ненулевого (комплексного) множителя. Если  $z \neq 0$ , тройку  $(x, y, z)$  можно отождествить с точкой, имеющей обычные координаты  $(x/z, y/z)$ . Тройкам с  $z = 0$  соответствуют бесконечно удаленные точки проективной плоскости.

Так, алгебраические кривые часто рассматривают как множества точек на (комплексной) проективной плоскости. При этом уравнение  $F(x, y) = 0$  степени  $n$  в однородных координатах переписывается в виде  $P(x, y, z) = 0$ , где  $P = z^n F(x/z, y/z)$  — однородный многочлен степени  $n$ , так что  $F(x, y) = P(x, y, 1)$  (например, если  $F(x, y) = x^3 - 2y^2 + 3xy - x + 1$ , то  $P(x, y, z) = x^3 - 2y^2z + 3xyz - xz^2 + z^3$ ). При этом кривая  $P(x : y : z) = 0$  может, помимо "обычных", содержать также и бесконечно удаленные точки.

**Определение.** Алгебраическая кривая называется *вырожденной*, если любой задающий ее многочлен приводим (т.е. раскладывается в произведение многочленов меньшей степени).

Так, вырожденная кубика задается уравнением  $QL = 0$ , где  $Q$  и  $L$  — многочлены степени 2 и 1 соответственно; тем самым, вырожденная кубика является объединением прямой  $L = 0$  и коники  $Q = 0$  (эта коника может, в свою очередь, оказаться вырожденной).

Нам в разных ситуациях понадобится рассматривать пересечение кубики  $\mathcal{C}$  и прямой  $\ell$ . Нахождение  $\mathcal{C} \cap \ell$  сводится к решению системы  $P(x, y, z) = 0$ ,  $L(x, y, z) = 0$  однородных уравнений 3-й и 1-й степени. Из  $L(x, y, z) = 0$  можно выразить одну из переменных через другие и подставить в  $P(x, y, z) = 0$ . Скажем, подстановка  $z$  приведет к однородному уравнению 3-й степени  $R(x, y) = 0$ . В вырожденном случае  $R \equiv 0$  многочлен  $P$  делится на  $L$  и  $\ell \subset \mathcal{C}$ . Если  $R \neq 0$ , то  $R$  раскладывается в произведение линейных многочленов  $L_1 L_2 L_3$  ( $L_i$  вообще говоря, с комплексными коэффициентами). Решение каждого уравнения  $L_i = 0$  определяет точку  $A_i \in \mathcal{C} \cap \ell$  (возможно, невещественную или бесконечно удаленную). Среди  $L_i$  могут встретиться пропорциональные. Если  $L_1 = \lambda L_2$ , то точка  $A_1 = A_2$  считается *кратной* точкой пересечения: точкой кратности 2, если  $L_3$  не пропорционально  $L_1$ , и кратности 3, если все  $L_i$ ,  $i = 1, 2, 3$ , пропорциональны. Можно показать, что кратность точки пересечения не зависит от выбора системы координат  $x, y, z$ . Таким образом, невырожденная кубика  $\mathcal{C}$  пересекает любую прямую  $\ell$  ровно трижды, с учетом кратности.

Некоторые *особые* кубики  $\mathcal{C}$  содержат так называемые *особые* точки (например, точка  $(0, 0)$  является точкой самопересечения кривой  $y^2 = x^3 + x^2$  и точкой возврата кривой  $y^2 = x^3$ ; формально, особые точки — это точки, в которых обнуляются частные производные задающего многочлена). Геометрически тот факт, что неособая точка  $A_1 \in \mathcal{C} \cap \ell$  является кратной точкой пересечения, означает касание  $\ell$  и  $\mathcal{C}$  в точке  $A_1$ ; если при этом кратность  $A_1$  равна 3,  $A_1$  называют *точкой перегиба* кубики  $\mathcal{C}$ . (Поймите, что это означает геометрически.)

Трехкратное пересечение с каждой прямой позволяет для данной неособой точки  $P \in \mathcal{C}$  определить *проектирование* с центром  $P$ : инволюцию  $s_P : \mathcal{C} \rightarrow \mathcal{C}$ , сопоставляющую точке  $X \in \mathcal{C}$  третью точку пересечения  $PX$  с  $\mathcal{C}$  (в случае  $X = P$  считаем, что прямая  $PX$  — касательная к  $\mathcal{C}$ ; для *точки перегиба*  $O$  имеем  $s_O(O) = O$ ).

Более общая задача отыскания точек пересечения двух кривых порядка  $m$  и  $n$  может быть сведена к алгебраическому уравнению степени  $mn$ . В соответствии с этим знаменитая *теорема Безу* гласит:

Две алгебраические кривые порядка  $m$  и  $n$ , задаваемые взаимно-простыми многочленами, пересекаются ровно в  $mn$  точках, с учетом кратности.

Мы не приводим здесь строгого определения кратности, поскольку для решения задач оно не понадобится. Отметим только, что случай касания кривых в их (неособой) точке  $A$  соответствует тому, что  $A$  — точка пересечения кратности не меньше 2. (В качестве примера, предлагаем понять, что две концентрические окружности касаются друг друга в двух мнимых, бесконечно удаленных точках (это определяемые ниже круговые точки)).

Из теоремы Безу следует, что любая коника пересекает невырожденную кубику в шести точках, с учетом кратности; а две различные невырожденные кубики имеют ровно девять общих точек, с учетом кратности.

Известно, что через любую точку  $X$  проходит шесть (с учетом кратности) прямых, касающихся данной неособой кубики  $\mathcal{C}$ . При этом шесть точек касания лежат на одной конике. Если же  $X \in \mathcal{C}$ , то две или три из этих шести прямых считаются совпадающими с касательной, проведенной в  $X$ .

Упомянем еще одну важную теорему:

*Теорема Шалля (о 9 точках на трех кубиках).* Пусть даны две кубики, пересекающиеся (с учетом кратности) в девяти точках. Тогда любая третья кубика, проходящая через восемь точек их пересечения, проходит и через девятую точку.

Эта теорема может эффективно использоваться и в случае вырожденных кубик.

**Определение.** Пусть дана кубика  $\mathcal{C}$  и неособая точка  $O$  (нуль) на ней. Для произвольных неособых точек  $A, B \in \mathcal{C}$  найдем третью точку  $C$  пересечения

прямой  $AB$  с  $\mathcal{C}$ , а затем третью точку пересечения прямой  $OC$  с  $\mathcal{C}$ . Эта точка называется *суммой*  $A + B$  точек  $A$  и  $B$ .

**4.1.** Докажите, что

a) сложение точек на кубике ассоциативно:  $(A + B) + C = A + (B + C)$ ;

b) для любых (неособых) точек  $A, B$  однозначно определена их разность, т.е такая точка  $A - B$ , что  $B + (A - B) = A$ .

**4.2.** Выразите операцию « $+$ » с выбором нуля в точке  $O' \in \mathcal{C}$  через операцию « $+$ » с выбором нуля в точке  $O \in \mathcal{C}$ .

**4.3.**

a) Докажите, что для любых трех неособых точек  $A, B, C$  кубики  $\mathcal{C}$ , лежащих на одной прямой  $\ell$ , сумма  $A + B + C$  не зависит от  $\ell$ .

b) Докажите, что если за  $O$  выбрана точка перегиба, то  $A + B + C = O$  тогда и только тогда, когда  $A, B, C$  лежат на одной прямой.

Утверждение задачи 4.1. означает, что введенное сложение точек задает на  $\mathcal{C}$  (за вычетом особых точек) структуру абелевой группы. Можно доказать (см. задачу 4.2), что структура этой группы не зависит от выбора  $O$ . Этую группу можно инвариантно описать как группу преобразований  $\mathcal{C} \rightarrow \mathcal{C}$  вида  $X \mapsto X + C$ .

**4.4.** (критерий перестановочности проектирований). Пусть  $P, P' \in \mathcal{C}$  — неосо- бые точки. Докажите, что  $s_P s_{P'} = s_{P'} s_P$  тогда и только тогда, когда

a) для любой  $X \in \mathcal{C}$  выполнено условие замыкания:  $s_P s_{P'} s_P s_{P'}(X) = X$ ;

b) касательные к  $\mathcal{C}$ , проведенные в  $P$  и  $P'$ , пересекаются на  $\mathcal{C}$ .

Условие a) позволяет в случае  $s_P s_{P'} = s_{P'} s_P$  задать биекцию между парами  $(X, X')$ ,  $(Y, Y')$  точек  $\mathcal{C}$  по правилу  $Y = s_P(X)$ ,  $X' = s_{P'}(Y)$ ,  $Y' = s_P(X') = s_P(X)$  (так, что  $XX'$ ,  $YY'$ ,  $PP'$  — диагонали четыресторонника, вписанного в  $\mathcal{C}$ ).

**4.5.** (Точки порядка 2 и инволюции сдвига.) Пусть  $C \in \mathcal{C}$  — такая точка,  $C \neq O$  и  $C + C = O$ . (Иначе говоря,  $C$  — точка порядка 2 в абелевой группе.) Тогда сдвиг  $X \mapsto X + C$  является инволюцией  $X \leftrightarrow X'$ .

a) Выбрав  $O$  в точке перегиба, опишите геометрически точки порядка 2 и соответствующие инволюции. Сколько может быть точек порядка 2?

b) Докажите, что касательные к  $\mathcal{C}$ , проведенные в  $X$  и  $X'$  пересекаются на  $\mathcal{C}$ ; и наоборот, пара точек  $P, P' \in \mathcal{C}$  такая, что касательные к  $\mathcal{C}$ , проведенные в них, пересекаются на  $\mathcal{C}$ , определяет инволюцию сдвига  $X \mapsto X + P' - P$ .

**4.6.** Пусть на невырожденной кубике  $\mathcal{C}$  за  $O$  выбрана точка перегиба. Тогда сумма шести точек равна  $O$  тогда и только тогда, когда они лежат на конике.

**4.7.**

a) Фиксируем  $A, B, C, D \in \mathcal{C}$ . Каждой точке  $X$  ставим с соответствие точку  $Y$  — шестую (с учетом кратности) точку пересечения коники, проходящей через  $A, B, C, D, X$  с  $\mathcal{C}$ . Докажите, что прямые  $XY$  проходят через фиксированную точку.

b) Фиксируем  $P, C, D \in \mathcal{C}$ . Через  $P$  проводим всевозможные секущие и получаем пары точек пересечения  $X \in \mathcal{C}$  и  $Y = s_P(X)$ . Проводим через  $C, D, X, Y$  коники, пересекающие  $\mathcal{C}$  еще в паре точек  $Z, T$ . Докажите, что прямые  $ZT$  проходят через фиксированную точку  $Q \in \mathcal{C}$ .

## Циркулярные кубики

**Определение.** Точки комплексной проективной плоскости с однородными координатами  $(1 : i : 0)$  и  $(1 : -i : 0)$  называются *круговыми*.

**Определение.** Кубика, проходящая через круговые точки, называется *циркулярной*.

**4.8.** Докажите, что любая окружность (т.е. кривая с уравнением  $(x - a)^2 + (y - b)^2 = r^2$ , где  $a, b, r$  — комплексные числа) проходит через круговые точки.

**4.9.** Пусть  $X \leftrightarrow X'$  — инволюция сдвига на циркулярной кубике  $\mathcal{C}$ :  $X' = X + C$ , где  $C + C = O$ . Для неособых точек  $A, B, X \in \mathcal{C}$ , отличных от круговых точек, докажите, что вторая (отличная от круговых) точка пересечения окружностей  $(ABX)$  и  $(A'B'X)$  лежит на  $\mathcal{C}$ .

**4.10.** (пучки «антипараллелей») Пусть  $P$  и  $Q$  — точки на циркулярной кубике  $\mathcal{C}$ . Через  $P$  проводим всевозможные секущие и получаем пары точек пересечения  $X, Y$ . Через  $Q$  проводим всевозможные секущие и получаем пары точек пересечения  $Z, T$ .

a) Докажите, что если точки  $X, Y, Z, T$  лежат на одной окружности для одного положения секущих, то это будет выполнено и для любого положения секущих.

b) Условия предыдущего пункта выполнены тогда и только тогда, когда  $PQ$  параллельна *асимптоте* (под асимптотой понимаем третью, помимо двух круговых, бесконечно удаленную точку циркулярной кубики).

## 5 Кубика фокусов

Далее (в частях 5 и 6) когда мы имеем дело с уравнением кубики, мы имеем в виду, что коэффициенты в этом уравнении вещественные (хотя мы можем подставлять точки с любыми комплексными координатами в это уравнение).

### Свойства кубики фокусов

#### 5.1.

- a) Докажите, что если  $X \in ISO(ABA'B')$ , то и  $Y = f_{ABA'B'}(X) \in ISO(ABA'B')$ ;  
b) и при этом все прямые  $XY$  проходят через одну точку.

5.2. Докажите, что  $\varphi = \varphi_{ABA'B'}$  переводит любую точку  $X \in ISO(ABA'B')$  в изогонально сопряженную точку  $X'$ .

5.3. Докажите, что  $ISO(ABA'B')$  — циркулярная кубика.

5.4. Докажите, что (в регулярном случае)  $ISO(ABA'B')$  содержит следующие точки:

- a)  $A, B, A', B'$ ;  
b)  $P = AB \cap A'B', P' = AB' \cap A'B$ ;  
c) точка Микеля  $M = M_{ABA'B'}$ ;  
d) проекция точки пересечения  $AA'$  и  $BB'$  на прямую  $PP'$ ;  
e) точка  $T = T_{AB',A'B}$  такая, что треугольники  $TAB'$  и  $TA'B$  подобны и противоположно ориентированы (и аналогичная точка  $T_{AB,A'B'}$ ).

5.5. Для указанных в предыдущей задаче точек укажите

- a) изогонально сопряженные точки  
b) и соответствующую 4-орбиту.

5.6. (асимптота и прямая Ньютона-Гаусса) Докажите, что асимптота  $ISO(ABA'B')$

- a) параллельна прямой Ньютона-Гаусса;  
b) проходит через точку, симметричную  $M$  относительно прямой Ньютона-Гаусса.

c) Докажите, что если  $X \in ISO(ABA'B')$ , то середина отрезка между  $X$  и  $s_M(X)$  лежит на прямой Ньютона-Гаусса.

#### 5.7.

a) (С.Берлов) Докажите, что прямые все  $XY$  (см. задачу 5.1) проходят через  $T_{AB',A'B'}$ .

b) Докажите, что прямая  $PT_{AB',A'B'}$ , где  $P = AB \cap A'B'$ , параллельна прямой Ньютона-Гаусса.

5.8. Пусть  $(C, C')$  и  $(D, D')$  — две пары изогонально сопряженных точек на кубике фокусов  $ISO(ABA'B')$ . Докажите, что кубика фокусов  $ISO(CDC'D')$  совпадает с  $ISO(ABA'B')$ , причем пары сопряженных точек одни и те же для обеих кубик.

5.9. Пусть  $X, X'$  — изогонально сопряженные точки кубики фокусов. Докажите, что разность  $X - X' = K$  — не зависящая от точки  $X$  точка второго порядка (т.е.  $K + K = O$ ).

**5.10.** (\*ВПИСАННЫЙ\*) Пусть точки  $A, B, A', B'$  — на одной окружности  $\Omega$  с центром  $O$ . Пусть  $X, Y, X', Y'$  — 4-орбита точки  $X \in ISO(ABA'B')$ . Докажите, что вписанные в  $ABA'B'$  коники с парами фокусов  $X, X'$  и  $Y, Y'$ , подобны.

**5.11.** (\*ГАРМОНИЧЕСКИЙ\*) Пусть точки  $ABA'B'$  — гармонический четырехугольник (т.е. вписанный и такой, что произведения его противоположных сторон равны).

a) Докажите, что середины  $M_A$  и  $M_B$  отрезков  $AA'$  и  $BB'$  принадлежат  $ISO(ABA'B')$ .

b) (точки Брокара) Докажите, что  $M_A$  и  $M_B$  принадлежат одной 4-орбите вместе с точками Брокара  $Br_1, Br_2$ .

c) Пусть  $AA' \cap PP' = W$ , а — окружность  $(M_A Br_1 M_B Br_2)$ . Докажите, что при центральном проектировании  $\omega \rightarrow \omega$  с центром  $W$  4-орбита  $M_A Br_1 M_B Br_2$  переходит в 4-орбиту точки  $O$ .

**5.12.** (\*ПАРАЛЛЕЛОГРАММ\*) Пусть  $ABA'B'$  — параллелограмм.

a) Докажите, что  $X \in ISO(ABA'B')$  тогда и только тогда, когда  $\angle(BA, AX) = \angle(A'X, A'B)$ .

b) Докажите, что  $X \in ISO(ABA'B')$  тогда и только тогда, когда окружности  $(XAB), (XAB'), (XA'B'), (XA'B)$  равны.

c) Докажите, что  $ISO(ABA'B')$  — объединение бесконечно удаленной прямой и гиперболы, проходящей через  $A, B, A', B'$ ;

d) причем эта гипербола прямоугольная, а ее асимптоты параллельны биссектрисам углов  $ABA'B'$ .

**5.13.** (\*ОПИСАННЫЙ + ВЫРОЖДЕНИЕ  $A = A'$ \*)

a) Пусть  $ABA'B'$  — четырехугольник, отличный от параллелограмма, а  $I$  — его вырожденная 4-орбита (т.е. такая орбита, что все 4 точки этой орбиты совпадают). Верны ли следствия:  $I \in ISO(ABA'B') \Leftrightarrow AB, BA', A'B', B'A$  касаются некоторой окружности.

b) В таком случае  $M_{ABA'B'}$  совпадает с проекцией центра окружности  $(AIA')$  на симедиану, треугольника  $AIA'$ , проведенную из  $I$ .

**5.14.** (\*ac=bd\*) Пусть  $C$  — третья точка на  $AA'$ , принадлежащая  $ISO(ABA'B')$ , аналогично  $D$  — третья точка на  $BB'$ , принадлежащая  $ISO(ABA'B')$ .

a) В каком случае  $C = D$ ?

b) В каком случае  $D = C'$ ?

c) (полуБрокар). Скажем, что  $P$  — (первая/вторая) точка полуБрокара, если  $\angle(PA, AB) = \angle(PA', A'B')$  и  $\angle(PB, BA') = \angle(PB', B'A)$ . Докажите, две из четырех точек 4-орбиты точки полуБрокара лежат на  $AA'$  и  $BB'$ .

d) (IMO2018) Выпуклый четырехугольник  $ABCD$  удовлетворяет условию  $AB \cdot CD = BC \cdot DA$ . Точка  $X$  внутри четырехугольника  $ABCD$  такова, что  $\angle XAB = \angle XCD$  и  $\angle XBC = \angle XDA$ . Докажите, что  $\angle BXA + \angle DXC = 180^\circ$ .

## Другие описания кубики фокусов

**5.15.** Пусть точка Микеля  $M$  является началом координат, а сопряженная ей точка — бесконечно удаленной точкой оси  $y$ . Докажите, что уравнение кубики фокусов имеет вид  $(x^2 + y^2)(x + A) = Bx + Cy$ .

**5.16.** Докажите, что

- а) циркулярная кубика является кубикой фокусов тогда и только тогда, когда касательные в круговых точках пересекаются на кубике;
- б) в этом случае точка пересечения касательных совпадает с точкой Микеля  $M$ .

**5.17.** (точки касания окружностей пучка) Пусть  $L, L'$  — отличные от круговых точки кубики фокусов  $\mathcal{C}$ , касательные в которых проходят через  $M$ . Возьмем произвольную окружность, проходящую через  $L$  и  $L'$ , и проведем к ней касательные  $MX, MY$ . Докажите, что

- а)  $X, Y \in \mathcal{C}$ ;
  - б) все прямые  $XY$  пересекают  $\mathcal{C}$  в одной и той же точке.
  - с) Пусть дан пучок окружностей и произвольная точка  $M$ . Докажите, что ГМТ  $X, Y$ , где  $MX, MY$  — касательные к произвольной окружности пучка, является кубикой фокусов.
  - д) При этом выяснить, как зависит вид кубики от типа пучка.
- 5.18.** (Универсальность  $\varphi$ , или коллекция всех кубик фокусов) Пусть  $\varphi$  — данная инверсия и симметрия с центром  $M$ .
- а) Пусть  $m$  — данная прямая. Докажите, что множество точек  $X$  таких, что середина  $X\varphi(X)$  лежит на  $m$ , является кубикой фокусов.
  - б) Установите соответствие между прямыми  $m$  и кубиками фокусов.
  - с) Опишите точки пересечения разных кубик фокусов.

## 6 Квартеты и изогональные кубики

**6.1.** Пусть даны треугольник  $ABC$  и точка  $J$ . Докажите, что

а) ГМ таких точек  $P$ , что  $P$ , изогонально сопряженная точка  $P'$  и  $J$  лежат на одной прямой, — кубика, проходящая через вершины треугольника, центры его вписанной и вневписанных окружностей,  $J$  и изогонально сопряженную точку  $J'$ ;

б) эта кубика циркулярна тогда и только тогда, когда  $J$  — бесконечно удаленная точка

Пусть дан треугольник  $XYZ$ . Как в разделе 2, обозначим через  $\varphi_X$  композицию инверсии с центром  $X$  и симметрии относительно биссектрисы угла  $X$ , меняющую местами точки  $Y$  и  $Z$ . Аналогично определим преобразования  $\varphi_Y$ ,  $\varphi_Z$ .

**6.2.** Докажите, что эти преобразования перестановочны друг с другом и изогональным сопряжением.

Пусть  $A$  — произвольная точка,  $B = \varphi_Z(A)$ ,  $C = \varphi_Y(A)$ ,  $D = \varphi_X(A)$ . Четверку  $\{A, B, C, D\}$  будем называть *квартетом* относительно треугольника  $XZY$ .

**6.3.** Докажите, что

а) четверка изогонально сопряженных точек  $\{A', B', C', D'\}$  также является квартетом;

б) прямые  $AA'$ ,  $BB'$ ,  $CC'$ ,  $DD'$  параллельны;

с) точки  $A, B, C, D, A', B', C', D', X, Y, Z$  лежат на одной циркулярной кубике (назовем ее *кубикой квартетов*;

д)  $A+A=B+B=C+C=D+D$ , т.е. касательные к кубике квартетов в точках  $A, B, C, D$  пересекают кубику в одной точке.

Свойствам квартетов был посвящен проект на XXII ЛКТГ [15]. В частности, там предлагалась задача, которую не смог решить ни один из участников.

**6.4.** Пусть  $A, B, C, D$  — квартет,  $A', B', C', D'$  — изогонально сопряженный квартет;  $P_X$  — точка пересечения  $AD$  и  $BC$ ,  $P_Y$  —  $AC$  и  $BD$ ,  $P_Z$  —  $AB$  и  $CD$ . Точки  $Q_X, Q_Y, Q_Z$  определяются аналогично по точкам  $A', B', C', D'$ . Докажите, что

а) прямые  $P_XQ_X, P_YQ_Y, P_ZQ_Z$  пересекаются в одной точке, лежащей на описанной окружности треугольника  $XZY$  (из предыдущих обозначений);

б) прямые  $P_XQ_Y, P_YQ_X$  и  $XY$  пересекаются в одной точке  $Z'$ ;

с)  $ZZ'$  параллельна  $AA', BB', CC', DD'$ .

**6.5.** Пусть  $D_1, D'_1$  и  $D_2, D'_2$  — две пары изогонально сопряженных точек такие, что  $D_1D'_1 \parallel D_2D'_2$ . Докажите, что прямые  $A_1A_2, B_1B_2, C_1C_2, D_1D_2$  пересекаются в одной точке ( $A_1, B_1, C_1, D_1$  и  $A_2, B_2, C_2, D_2$  — квартеты).

**6.6.** Пусть касательные к кубике квартетов в точках  $X$  и  $Y$  пересекаются в точке  $P$ , а касательные в круговых точках в точке  $Q$ . Докажите, что  $PQ$  — диаметр окружности  $XZY$ .

**6.7.** Когда кубика квартетов является кубикой фокусов?

**6.8.** Пусть  $\mathcal{C}$  — произвольная циркулярная кубика,  $J$  — ее бесконечная точка, отличная от круговых,  $X, Y, Z$  — такие точки, что  $X + X = Y + Y = Z + Z =$

$J + J$ . Докажите, что  $\mathcal{C}$  является кубикой квартетов относительно треугольника  $XYZ$ .

### Еще про 8-орбиты

**6.9.** Пусть  $A, B, C, D, A^* = g_{A,B,C,D}(A), B^*, C^*, D^*$  — 8-орбита относительно данных четырех точек  $X, Y, Z, T$ .

- a) Докажите, что окружности  $(TAA^*)$ ,  $(TBB^*)$ ,  $(TCC^*)$ ,  $(TDD^*)$  касаются;
- b) Докажите, что окружности  $(TAD)$ ,  $(TA^*DA^*)$ ,  $(TYZ)$  соосны (здесь  $D = \varphi_{XYZT}(A)$ ).

## 7 ДОБАВКА

### Изогональное сопряжение... окружностей

**7.1.** (Ф. Нилов) Дан четырехугольник  $ABCD$ . Пусть  $l_a, l_b, l_c, l_d$  – внутренние биссектрисы углов  $A, B, C, D$  соответственно. Пусть прямые  $a, b, c$  и  $d$  проходят через точки  $A, B, C, D$  соответственно, причём точки пересечения  $a$  и  $b$ ,  $b$  и  $c$ ,  $c$  и  $d$ ,  $d$  и  $a$  лежат на одной окружности  $\alpha$ . Пусть прямые  $a', b', c'$  и  $d'$  симметричны прямым  $a, b, c$  и  $d$  относительно биссектрис  $l_a, l_b, l_c, l_d$  соответственно.

- a) Докажите, что точки пересечения  $a'$  и  $b'$ ,  $b'$  и  $c'$ ,  $c'$  и  $d'$ ,  $d'$  и  $a'$  лежат на одной окружности  $\alpha'$ ;
- b) при этом  $\alpha' = \varphi_{ABCD}(\alpha)$ .

## Список литературы

- [1] А. Акопян. Геометрия в картинках. Издание 2-е, дополненное, Изд-во МЦНМО, М., 2017.
- [2] А. Акопян, А. Заславский. Геометрические свойства кривых второго порядка. Издание 2-е, дополненное, Изд-во МЦНМО, М., 2011.
- [3] А. Акопян, А. Заславский. Разные взгляды на изогональное сопряжение. Матем. просв., сер. 3, 11, Изд-во МЦНМО, М., 2007, 61–78.
- [4] Н. Белухов О некоторых парах перспективных треугольников. Матем. просв., сер. 3, 14, Изд-во МЦНМО, М., 2010, , 256–259.
- [5] С. Берлов, Ф. Петров. Решение задачи M2497. Квант, 2018, 4, 13–15.
- [6] Н. Васильев. Гексаграммы Паскаля и кубические кривые. Квант, 1987, 8, 2–8.
- [7] А. Заславский. Геометрические преобразования. Изд-во МЦНМО, М., 2004.
- [8] П. Кожевников. Обобщенная теорема Наполеона. Сборник «Элементы математики в задачах. Через олимпиады и кружки к профессии.» Изд-во МЦНМО, М., 2018, 196–202.
- [9] А. Куликова, Д. Прокопенко. Теорема об изогоналях. Квант, 2018, 4, 41–44, 5, 34–37.
- [10] В. Острик, М. Цфасман. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые. Изд-во МЦНМО, М., 2005.
- [11] В. Прасолов, Ю. Соловьев. Эллиптические функции и алгебраические уравнения., М.: Факториал, 1997.
- [12] Ю. Соловьев. Арифметика эллиптических кривых. Квант, 1987, 7, 2–8.
- [13] А. Уткин. Изогональное сопряжение в четырехугольнике. Квант, 2019, 2, 37–42.
- [14] <https://mathcurve.com/courbes2d.gb/focaledevanrees/focaledevanrees.shtml>
- [15] <https://www.turgor.ru/lktg/2010/1/index.htm>

# **Кубики фокусов и циркулярные кубики**

Решения, схемы решений, указания.

# 0 Изогональное сопряжение в многоугольниках

## Изогональное сопряжение в четырехугольнике

**0.10.** Можно воспользоваться условием 0.1d.

**0.11.** можно доказать, пользуясь условием 0.14а.

**0.12.**

а) Вытекает из предыдущей задачи.

б) Имеется два (комбинаторно различных) случая. Один сводится к 0.10, другой — к 0.11.

**0.13.** В согласии с задачами 0.7, 0.8, из того, что  $X$  и  $X'$  изогонально сопряжены относительно пар прямых  $a, b$ , и  $b, c$ , следует, что  $X$  и  $X'$  изогонально сопряжены относительно  $c, a$ .

Можно утверждать следующее: если  $X$  и  $X'$  изогонально сопряжены относительно некоторого многоугольника, то они изогонально сопряжены относительно любой пары прямых, содержащих пару его сторон.

**0.14.**

а) 1) Пусть  $X \in ISO(ABA'B')$ . Тогда, в силу 0.1e, проекции  $X$  и  $X'$  на прямые  $AB, AB'$  лежат на одной окружности  $\omega$ , при этом ее центр  $O$  проектируется в середины проекций отрезка  $XX'$ , значит,  $O$  — середина  $XX'$ . Аналогично проекции  $X$  и  $X'$  на прямые  $AB', A'B$  лежат на одной окружности с центром  $O$  и радиусом  $R = OX_{AB'}$  (где  $X_{AB'}$  — проекция  $X$  на  $AB'$ ), т.е. на окружности  $\omega$ . Далее повторяем рассуждения для прямых  $A'B, A'B'$ .

1') Пусть проекции  $X$  на прямые  $AB, AB', A'B, A'B'$  лежат на одной окружности  $\omega$  с центром  $O$ . Тогда изогонально сопряженная для  $X$  относительно треугольника, стороны которого лежат на прямых  $AB, AB', A'B$ , — это точка  $X'$ , симметричная  $X$  относительно  $O$ . Та же точка — изогонально сопряженная для  $X$  относительно треугольника, стороны которого лежат на прямых  $A'B', AB', A'B$ . Значит, по задаче 0.13,  $X$  и  $X'$  изогонально сопряжены относительно  $ABA'B'$ .

2) Условие  $Isog_X(AA', BB')$  эквивалентно критерию концикличности проекций  $X_{AB}, X_{BA}, X_{A'B'}, X_{B'A}$ . Действительно, пользуясь  $\angle(X_{AB}X_{BA}, X_{BA'}X_{A'B'}) = \angle(X_{AB}X_{BA}, X_{BA'}X) + \angle(XX_{BA}, X_{BA'}X_{A'B'}) = \angle(AB, BX) + \angle(XA', A'B')$  и аналогичными равенствами, имеем  $\angle(X_{AB}X_{BA}, X_{BA'}X_{A'B'}) = \angle(X_{AB}X_{B'A}, X_{B'A}X_{A'B'}) \Leftrightarrow \angle(BX, AX) = \angle(B'X, A'X)$ .

б) Эквивалентность б) и  $X \in ISO(ABA'B')$  вытекает из следующих рассмотрений. Пусть  $R = OX_{AB} = OX'_{AB}$ . Пусть  $X_0$  симметрична  $X$  относительно  $AB$ ,  $T = X'X_0 \cap AB$ . Тогда  $XT$  и  $X'T$  симметричны относительно  $AB$  (угол падения равен углу отражения); и  $XT \pm X'T = \pm 2R$ , т.е.  $OX_{AB}$  — средняя линия треугольника  $OX'X_0$  и  $XT = X_0T$ . Коника с фокусами  $X, X'$  и (большой) полуосью  $\pm 2R$  касается  $AB$ .

*Замечание.* Отметим, что эта коника дважды касается (педальной) окружности с центром  $O$  радиуса  $R$ . Эта коника является коникой Брокара точки  $X$ , отвечающая углу  $90^\circ$ . (Замечание обобщается на *косопедальную окружность*).

с) Пусть такая пирамида, все грани которой касаются сферы  $\omega$ , существу-

ет. Тогда прямой прямой круговой конус  $K$  с вершиной  $S$ , описанный вокруг  $\omega$ , является также вписаным в пирамиду. Впишем в  $K$  еще одну сферу  $\omega'$ , касающуюся плоскости  $ABA'B'$  в точке  $X'$ . Возникает известная конструкция сфер Данделена, и для коники, вписанной в  $ABA'B'$  (эта коника — сечение  $K$  с плоскостью  $ABA'B'$ ), точки  $X$  и  $X'$  являются фокусами.

*Замечание.* Отметим, что для описанной пирамиды выполнено равенство на плоские углы  $\angle ASB + \angle A'SB' = \angle BSA' + \angle B'SA$ , которое обобщает равенство  $\angle AXB + \angle A'XB' = \angle BXA' + \angle B'XA$ , эквивалентное (для точки внутри  $ABA'B'$  условию  $Isog_X(AA', BB')$ ).

**0.15.** Середины  $XX'$  — центры вписанных в  $ABA'B'$  коник. Известно, что они лежат на прямой Ньютона-Гаусса. Каждой точке прямой Гаусса соответствует ровно одна пара  $X, X'$ , симметричная относительно нее. Это следует, например, из рассмотрений в комплексных координатах (см. 3.7.).

#### 0.16.

Пусть  $X$  не лежит на прямой  $AA'BB'$ . Так как углы  $AXA'$  и  $BXB'$  имеют одну и ту же пару биссектрис, то  $X$  лежит на общей окружности Аполлония для пар  $A, A'$  и  $B, B'$ . Такая окружность единственная (как общая окружность двух разных пучков, или как окружность, относительно которой пары  $A$  и  $A'$ ,  $B$  и  $B'$  инверсны). В условиях нашей задачи а) множество точек  $X$ , для которых выполнено  $Isog_X(AA', BB')$ , представляет собой объединение прямой  $AA'$  и окружности Аполлония  $\omega$  точек  $A$  и  $A'$ , проходящую через  $B = B'$ .

*Замечание.* Эта задача оправдывает другое названия для  $ISO(ABA'B')$  — Apollonius cubic.

Задача б) предлагалась Л. Емельяновым на Южном турнире математических боев около 20 лет назад.

# 1 Изоциклические инволюции

(В этом параграфе — плоскость пополненная точкой  $\infty$  ( $=$  сфера  $= \overline{\mathbb{C}}$ ).

## 1.1.

a) Направленные углы  $\angle(XB, XA)$  и  $\angle(XD, XC)$  остаются неизменными.

$$\angle(YC, YB) = \angle(YC, YX) + \angle(YX, YB) = \angle(DC, DX) + \angle(AX, AB) = \angle D + \angle(DA, XD) + \angle A + \angle(XA, DA) = \angle D + \angle A + \angle(XA, XD).$$

Аналогично связаны  $\angle(YA, YD)$  и  $\angle(XB, XC)$ .

b) Следует из предыдущего пункта — постоянство  $\angle(XA, XD)$  влечет постоянство  $\angle(YB, YC)$ .

1.2. После инверсии в точке  $A$  утверждение сводится к существованию точки Микеля для четверки прямых.

Также это утверждение независимо последует из явного описания  $f_{AB,CD}f_{BC,DA}$  (как инверсии+симметрии) в разделе 2. Из этого же описания ясно, как доопределить композицию  $f_{AB,CD}f_{BC,DA}$  на «нерегулярных» точках?

## 4-орбиты

### 1.3. (\*ВПИСАННЫЙ\*)

a) Пусть  $P = AB \cap A'B'$ . Тогда  $P$  — радикальный центр окружностей  $(ABXY)$ ,  $(A'B'XY)$  и  $\Omega$ , поэтому  $XY$  проходит через  $P$ , при этом  $PX \cdot PY = \deg_\Omega P$ , поэтому  $f_{AB,A'B'}$  — инверсия с центром  $P$ , переводящая  $\Omega$  в себя.

b) Соответственно, множество неподвижных точек для  $f_{AB,A'B'}$  — окружность с центром  $P$  радиуса  $\sqrt{\deg_\Omega P}$ .

c) Пусть  $P' = AB' \cap A'B$ ,  $E = AA' \cap BB'$ ,  $L = P'E \cap PO$ ,  $L' = PE \cap P'O$ . Как известно,  $P'E$  — поляра точки  $P$  относительно  $\Omega$ , поэтому  $P'E \perp PO$  и  $PO \cdot PL = \deg_\Omega P$ , значит  $L = f_{AB,A'B'}(O)$ . Аналогично,  $L' = f_{A'B,AB'}(O)$  и  $E = PL' \cap P'L$  — четвертая вершина 4-орбиты  $O, L, E, L'$ .

d) Так как  $PX \cdot PY = PX' \cdot PY' = \deg_\Omega P$ , то  $X, Y, X', Y'$  лежат на одной окружности, причем  $P$  имеет равные степени относительно окружностей  $(XYX'Y')$  (для всевозможных 4-орбит  $X, Y, X', Y'$ ).

e) Аналогично  $P'$  имеет равные степени относительно окружностей  $(XYX'Y')$ , поэтому  $PP'$  — общая радикальная ось окружностей  $(XYX'Y')$ .

### 1.4. (\*ПАРАЛЛЕЛОГРАММ\*)

a) Пусть  $Y = f_{AB,A'B'}(X)$ . Тогда  $\angle(AY, YB') = \angle(AY, XY) + \angle(XY, YB') = \angle(AB, BX) + \angle(XA', A'B') = \angle(XA', AB) + \angle(AB, BX) = \angle(A'X, XB)$ . Пусть  $X', Y'$  симметричны  $X, Y$  относительно центра параллелограмма. Тогда из симметрии  $\angle(A'Y', Y'B) = \angle(AY, YB')$ , откуда  $\angle(A'Y', Y'B) = \angle(A'X, XB)$ , поэтому  $B, A'X, Y'$  — на одной окружности. Аналогично  $B', AX, Y'$  — на одной окружности, откуда  $Y' = f_{A'B,AB'}(X)$ . Аналогично рассуждая про  $X'$ , понимаем, что  $X, Y, X', Y'$  — 4 орбита (точки  $X$ ).

b) Имеем  $\angle(XY, XY') = \angle(XY, XB) + \angle(XB, XY') = \angle(AY, AB) + \angle(A'B, A'Y')$ , что в силу симметрии, равно  $\angle(AY, AB) + \angle(AB', AY) = \angle(AB', AB)$ .

c) Пусть  $X = P$  и  $X, Y, X', Y'$  — 4-орбита точки  $X$ . Тогда  $O_1O_3 \perp XY$  (линия центров перпендикулярна общей хорде окружностей  $(ABP)$  и  $(A'B'P)$ )

и аналогично  $O_2O_4 \perp XY'$ . Тогда, согласно предыдущему пункту, угол между  $O_1O_3$  и  $O_2O_4$  равен углу между  $XY$  и  $XY'$  и равен углу параллелограмма.

*Замечание.* Эта задача предлагалась П. Кожевниковым на Южном турнире математических боев 2017 г.

d) Пусть  $A, B, A', B'$  — проекции  $P$  на  $CD, DC', C'D', D'C$  соответственно,  $Q = f_{CD', C'D}(P)$ ,  $K = CC' \cap DD'$ . Тогда  $\angle(DQ, QC) = \angle(DQ, QP) + \angle(PQ, QC) = \angle(DC', C'P) + \angle(PD', D'C) = \angle(BA', A'P) + \angle(PA', A'B) = \angle(BA', A'B)$ . По предыдущему пункту (так как  $D, C', D', C$  — образы  $O_1, O_2, O_3, O_4$  с центром  $P$  и коэффициентом 2),  $\angle(DK, KC) = \angle(BA', A'B)$ , откуда  $C, D, Q, K$  лежат на одной окружности. Аналогично  $C', D', Q, K$  лежат на одной окружности, откуда  $K = f_{CD, C'D}(Q)$ , что и требовалось установить.

*Замечание.* В случае вписанного  $CDC'D'$  факт согласуется с 1.3с.

## 2 Инверсия+симметрия

**2.1.** (известный факт)

**2.2.** По  $ABA'B'$  центр инверсии+симметрии, ось симметрии и радиус инверсии однозначно описываются так: центр — это точка Микеля  $M$  для  $ABA'B'$ , ось — биссектриса угла между  $MA$  и  $MA'$ , радиус  $= \sqrt{MA \cdot MA'}$ . Подобие переводит  $(X, X'; Y, Y')$  в  $(A, \varphi(A); B, \varphi(B))$  тогда и только тогда, когда центр, ось и окружность инверсии для  $(X, X'; Y, Y')$  переходят соответственно в центр, ось и окружность инверсии для  $(A, \varphi(A); B, \varphi(B))$ .

В следующей задаче указана важная связь с изоциклическими инволюциями.

**2.3.** (split) Центрально-симметричный случай — см. задачу 1.4.

Пусть  $\varphi = \varphi_{ABA'B'}$  — инверсия+симметрия с центром  $M$ .

Для произвольной точки  $C$  положим  $D = f_{AB,A'B'}(C)$  и  $C' = \varphi(C)$ . Покажем, что  $A, B', D, C'$  лежат на одной окружности, или эквивалентно, что  $\angle(AD, DB') = \angle(AC', C'B')$ . Этого будет достаточно, поскольку аналогично можно показать, что  $A', B, D, C'$  лежат на одной окружности, откуда сделать вывод, что  $C' = f_{AB', A'B'}(D)$ .

Из окружностей  $\angle(AD, DB') = \angle(AD, DC) + \angle(DC, DB') = \angle(AB, BC) + \angle(CA', A'B')$ . Из инверсии+симметрии,  $\angle(AC', C'B') = \angle(AC', C'M) + \angle(MC', C'B') = \angle(CA', A'M) + \angle(MB, BC)$ . Отсюда  $\angle(AD, DB') - \angle(AC', C'B') = \angle(AB, BC) + \angle(CA', A'B') + \angle(A'M, CA') + \angle(BC, MB) = \angle(AB, MB) + \angle(A'M, A'B') = 0$ .

**2.4.** Покажем, что  $\varphi_{ABCD}\varphi_{ACBD} = \varphi_{ABDC}$  (и аналогично  $\varphi_{ACBD}\varphi_{ABCD} = \varphi_{ABDC}$ ). И левая, и правая части — круговые преобразования I типа, меняющее местами  $A$  с  $D$ ,  $B$  с  $C$ . А такое преобразование единственно.

Другое решение можно получить из предыдущей задачи:  $\varphi_{ABCD} = f_{AB,CD}f_{BC,AD} = f_{BC,AD}f_{AB,CD}$ . Тогда  $\varphi_{ACBD}\varphi_{ABCD} = (f_{AC,BD}f_{BC,AD})(f_{BC,AD}f_{AB,CD}) = f_{AC,BD}f_{BC,AD}^2f_{AB,CD} = f_{AC,BD}f_{AB,CD} = \varphi_{ABDC}$ .

(Как обойти ограничение на регулярные точки для  $f_{AB,CD}, \dots$ ?)

**2.5.** Следует из того, что  $\varphi_X(BD) = (XAC)$ ,  $\varphi_X(AC) = (XBD)$ , а поскольку  $X$  — точка Микеля, окружности  $(XAC)$  и  $(XBD)$  проходят через  $P_Z = AB \cap CD$ .

*Замечание:* этот факт согласуется с теоремой об изогоналях.

**2.6.** Следует из того, что  $\varphi_X((BCZ)) = (CBY)$  и  $\varphi_X((ADZ)) = (DAY)$ , поскольку  $P_Y$  лежит на окружностях  $(BCZ)$  и  $(ADZ)$ , а  $P_Z$  лежит на окружностях  $(CBY)$  и  $(DAY)$ .

### 3 Гармонические шестерки точек

#### 3.1.

- a) непосредственная проверка.
- b) непосредственная проверка.
- c) Следует из того, что (1) сохраняется при сдвиге  $z \rightarrow z + c$ , умножении на константу  $z \rightarrow cz$ ,  $c \neq 0$ , и сопряжении  $z \rightarrow \bar{z}$ .
- d) Непосредственно проверяется, что (1) сохраняется при обращении  $z \rightarrow 1/z$ . Отсюда и из предыдущего пункта следует, что (1) сохраняется при всех дробно-линейных преобразованиях (т.е. при круговых преобразованиях I типа), а также при композиции сопряжения и дробно-линейного преобразования (т.е. при круговых преобразованиях II типа).

**3.2.** Если зафиксировать значение циклического отношения из левой части (1), а также пять из шести точек, то шестая точка (возможно, бесконечно удаленная) определяется однозначно (из линейного уравнения на ее комплексную координату).

#### 3.3.

a) Пусть  $ABA'B'$  регулярная, т.е.  $\varphi = \varphi_{ABA'B'}$  — инверсия+симметрия. Введем комплексные координаты так, чтобы  $\varphi(z) = 1/z$ , так что  $A(a)$ ,  $A'(1/a)$ ,  $B(b)$ ,  $B'(1/b)$ ,  $C(c)$ . Положим  $C''(1/c)$ . Непосредственная проверка (1) показывает, что шестерка  $(A, A'; B, B'; C, C'')$  является гармонической. Отсюда, с учетом единственности (см. предыдущую задачу), следует нужное утверждение.

Если  $ABA'B'$  — центрально-симметричная, т.е.  $\varphi = \varphi_{ABA'B'}$  — центральная симметрия, введем комплексные координаты так, чтобы  $\varphi(z) = -z$  и проведем аналогичные рассуждения.

b) Указанная транзитивность следует из предыдущего пункта: по условию  $\varphi_{ACA'C'} = \varphi_{ABA'B'}$  и  $\varphi_{ADA'D'} = \varphi_{ABA'B'}$ , откуда  $\varphi_{ACA'C'} = \varphi_{ADA'D'}$ , поэтому  $(A, A'; C, C'; D, D')$  является гармонической.

**3.4.** Угол  $\angle(AB, AC) - \angle(A'B, A'C)$  равен (направленному) углу между окружностями  $(ABC)$  и  $(A'BC)$ . Так как  $\varphi$  сохраняет углы между окружностями, этот угол равен углу между  $(AB'C')$  и  $(A'B'C')$ , или  $\angle(A'B', A'C') - \angle(AB', AC')$ .

*Замечание.* Указанное равенство (как и аналогичные ему) может бы преобразовано к разным видам, например

$$\angle(BA, BA') + \angle(B'A, B'A') = \angle(CA, CA') + \angle(C'A, C'A').$$

Если  $M$  — центр инверсии+симметрии  $\varphi$ , то  $\angle(BA, BA') + \angle(B'A, B'A')$  преобразуется к виду  $(\angle(BA, AM) + \angle(AM, A'M) + \angle(A'M, BA')) + (\angle(B'A, B'M) + \angle(B'M, B'A')) = \angle(AM, A'M) + (\angle(BA, AM) + \angle(B'M, B'A')) + (\angle(A'M, BA') + \angle(B'A, B'M)) = \angle(AM, A'M) + 0 + 0$ . Аналогично для  $\angle(CA, CA') + \angle(C'A, C'A')$

Иначе, говоря, если  $A, A' = \varphi(A)$  — пара фиксированных точек, то сумма

$$\angle(XA, XA') + \angle(X'A, X'A')$$

не зависит от выбора пары  $X, X' = \varphi(X)$ .

Последний факт обобщается так: сумма

$$\angle(XA, XB) + \angle(X'B', X'A')$$

не зависит от выбора пары  $X, X' = \varphi(X)$  (при фиксированных  $A, A' = \varphi(A), B, B' = \varphi(B)$ ). Указанная сумма равна  $\angle(MA, MB)$  — доказывается аналогично.

## Гармоничность и композиции поворотных гомотетий

### 3.5.

- a) Достаточно в равенстве (1) из определения гармоничности приравнять аргументы и модули комплексных чисел.
- b) Коэффициенты поворотных гомотетий — модули дробей в левой части (1), а углы поворота противоположны аргументам этих дробей.
- c) Из условия следует, что шестерка  $(A, A'; B, B'; C, C')$  является гармонической, а значит, и  $(C, C'; A', A; B, B')$  тоже, откуда следует  $(L - C'AB')$ .
- d) Пусть  $A'$  и  $B'$  — два центра поворотных гомотетий. Углы треугольника  $A'B'C'$  известны (например, по обобщенной теореме Наполеона).
- e) to be added

**3.6.** Условия на углы типа  $(R - \dots)$  обеспечивают конкурентность окружностей.

В случае, если все шесть точек лежат на одной окружности, условие  $(L - \dots)$ , вместе с  $(R - \dots)$ , которое обеспечивает подходящий порядок точек на окружности, дают конкурентность.

### 3.7.

- a) В изогональной шестерке нетрудно проверить выполнение двух условий вида  $(R - \dots)$ , которые обеспечивают конкурентность окружностей (см. предыдущую задачу).
- b) Пятерку  $A, B, B', C, C'$  единственным образом достроим до изогональной шестерки  $(A, A'; B, B'; C, C'')$  (прямые  $BA$  и  $B'A$  однозначно строятся из условий  $Isog_B(AA', CC')$ ,  $Isog_{B'}(AA', CC'')$ ). По предыдущему пункту,  $(A, A'; B, B'; C, C'')$  гармоническая, и в силу единственности (задача 3.2) имеем  $C'' = C'$ .

Другое решение можно получить в комплексных координатах (см. например, следующий пункт).

- c) Введем комплексные координаты, так что  $A, A'; B, B'; C, C'$  соответствуют  $a, 1/a, b, 1/b, c, 1/c$ . Тогда условие  $Isog_A(BB', CC')$  (эквивалентное тому, что шестерка изогональна, согласно предыдущему пункту) запишется как  $\frac{1/c-a}{1/b-a} \cdot \frac{c-a}{b-a} \in \mathbb{R}$ , или  $\frac{1-a/c-ac+a^2}{1-a/b-ab+a^2} \in \mathbb{R} \Leftrightarrow \frac{1/a+a-1/c-c}{1/a+a-1/b-b} \in \mathbb{R}$ . но последнее условие эквивалентно коллинеарности середин  $\frac{a+1/a}{2}, \dots$  отрезков  $AA'$ , ....

## 4 Некоторые сведения о кубиках

### 4.1.

а) Пусть  $U, V$  — третьи точки пересечения кубики с прямыми  $AB, BC$  соответственно. Тогда  $P = A + B$  и  $Q = B + C$  — третьи точки пересечения кубики с прямыми  $OU, OV$  и надо доказать, что точка пересечения прямых  $CP$  и  $AQ$  лежит на данной кубике. Рассмотрим две вырожденных кубики, одна из которых является объединением прямых  $ABU, OVQ$  и  $CP$ , а другая — прямых  $BCV, OUP$  и  $AQ$ . Данная кубика проходит через восемь точек их пересечения:  $A, B, C, O, U, V, P, Q$ ; следовательно, она проходит и через девятую.

б) Пусть прямая  $OA$  пересекает кубику в третий раз в точке  $C$ . Тогда  $A - B$  — третья точка пересечения кубики с прямой  $BC$ .

4.2. Обозначим  $A +' B = C$ . Тогда  $O' + C = A + B$ , т.е.  $C = A + B - O'$ .

### 4.3.

а) По определению сложения  $A + B + C$  — это третья точка пересечения кубики с касательной к ней в точке  $O$ .

б) Если  $O$  — точка перегиба, то  $A + B + C = O$ . Нетрудно видеть, что для любой точки  $P$   $P + O = P$ .

### 4.4.

а) Очевидно следует из равенства  $s_P s_P(X) = X$ .

б) По предыдущей задаче  $P + X + s_P(X) = P' + s_P(X) + s_{P'} s_P(X)$ , т.е.  $s_{P'} s_P(X) = X + P - P'$ . Тогда условие коммутирования равносильно равенству  $P - P' = P' - P$  или  $2P = 2P'$ . Но последнее равенство и означает, что касательные в точках  $P$  и  $P'$  пересекают кубику в одной точке.

### 4.5.

а) Из точки перегиба  $O$  можно провести к кубику три касательные, отличные от касательной к ней в точке  $O$ . Основания этих касательных и будут точками второго порядка

б) Очевидно, следует из предыдущей задачи.

4.6. Пусть  $A_1 + \dots + A_6 = 0$ . Найдем третью точки пересечения кубики с прямыми  $A_1A_2, A_3A_4, A_5A_6$ . Сумма этих точек также равна нулю, поэтому они лежат на одной прямой, обозначим ее через  $\ell$ . Рассмотрим две вырожденных кубики: объединение прямых  $A_1A_2, A_3A_4, A_5A_6$  и объединение прямой  $\ell$  с коникой, проходящей через точки  $A_1, \dots, A_5$ . Восемь из девяти точек их пересечения лежат на  $\mathcal{C}$ , следовательно, девятая тоже лежит на  $\mathcal{C}$ , т.е. совпадает с  $A_6$ .

Обратно, пусть точки  $A_1, \dots, A_6$  лежат на конике. Найдем третии точки  $B, C$  пересечения  $\mathcal{C}$  с прямыми  $A_1A_2, A_3A_4$ . Кубика, являющаяся объединением коники  $A_1 \dots A_6$  и прямой  $BC$ , проходит через восемь точек пересечения  $\mathcal{C}$  с объединением прямых  $A_1A_2, A_3A_4, A_5A_6$ , значит, прямые  $BC$  и  $A_5A_6$  пересекаются на  $\mathcal{C}$ , откуда и следует искомое равенство.

### 4.7.

а) По предыдущей задаче сумма  $X + Y$  не зависит от  $X$ .

б) Аналогично  $Z + T$  не зависит от выбора секущей.

## Циркулярные кубики

**4.8.** Проверяется непосредственной подстановкой.

**4.9.** Следует из равенства  $A' + B' = A + B$ .

**4.10.**

a) Сумма  $X + Y + Z + T$  зависит только от точек  $P, Q$ . Поэтому, если эти точки лежат на одной конике с круговыми для какого-то выбора секущих, то это выполнено для любых секущих.

b) Прямая  $PQ$  параллельна асимптоте тогда и только тогда, когда  $P + Q$  равно сумме круговых точек. Так как точки  $P, Q, X, Y, Z, T$  лежат на одной (вырожденной) конике, это условие необходимо и достаточно для того, чтобы  $X, Y, Z, T$  лежали на одной окружности.

## 5 Кубика фокусов

### Свойства кубики фокусов

#### 5.1.

a) Так как  $\angle(AX, XB) = \angle(AY, YB)$  и  $\angle(A'X, XB') = \angle(A'Y, YB')$ , условия  $Isog_X(AA', BB')$  и  $Isog_Y(AA', BB')$  эквивалентны.

(С только использованием того, что  $ISO(ABA'B')$  — изоциркулярная кубика): Пусть  $Y'$  — шестая точка пересечения с кубикой окружности  $(ABX)$ . Тогда  $Y' = -A - B - X - O_1 - O_2$  (где  $O_1, O_2$  — круговые точки). Аналогично для  $Y''$  — шестой точки пересечения с кубикой окружности  $(A'B'X)$ . Поскольку  $A' + B' = A + B$  (так как  $A' = A + C$ ,  $B' = B + C$ , где  $C + C = O$ ), имеем  $Y' = Y''$ .

b) (С использованием того, что  $ISO(ABA'B')$  — изоциркулярная кубика): Третья точка пересечения  $XY$  с кубикой постоянна, так как  $X + Y = -A - B - O_1 - O_2 = const$ .

5.2. Следует из задач 3.7 и 3.3.

5.3. Это следует, например, из вывода уравнения (задача 5.15).

#### 5.4.

a) Нетрудно проверить, что  $A, B, A', B'$  удовлетворяют уравнению.

b) В согласии с описанием  $ISO$ , как множество точек  $X$  таких, что середины  $AA', BB'$  и  $XX'$  коллинеарны.

c) Следует например, из того, что  $M$  — центр поворотной гомотетии, переводящей  $\vec{AB}$  в  $\vec{B'A'}$ .

d) Четверка  $A, E = AA' \cap BB', A', AA' \cap PP'$  гармоническая, а значит гармоническая и четверка прямых, соединяющих их с проекцией  $F$  точки  $E$  на  $PP'$ . Так как  $FE \perp PP'$ , то  $FA$  и  $FA'$  изогональны относительно  $FE$ . То же верно и для  $FB$  и  $FB'$ , откуда следует  $Isog_F(AA', BB')$ .

e) Условие  $Isog_T(AA', BB')$  очевидно из определения.

5.5. В согласии с задачей 5.1, в 4-орбите с точкой  $A$  лежит на пересечении прямой  $AT$  и окружности  $(A'B'A)$ .

В соответствии с определением изоциркулярных инволюций,  $P, M, P', \infty$  — 4-орбита. ( $\infty$  — точка кубики, соответствующая асимптоте).

Если рассмотреть 4-орбиту  $XYX'Y'$ , то, согласно задачам 5.1 и 5.7,  $T = XY \cap X'Y', T' = X'Y \cap XY'$ . Следовательно,  $T$  и  $T'$  сопряжены.

#### 5.6.

a) Следует из уравнения.

b) Следует из уравнения, и в согласии с тем, что  $\infty$  и  $M$  сопряжены.

c) Так как  $s_M(X) = s_\infty(X')$ , а середина  $XX'$  — на прямой Гаусса.

#### 5.7.

a) (С.Берлов) О геометрическом решении — см. С. Берлов, Ф. Петров. Решение задачи М2497. Квант, 2018, 4, 13–15.

b) Пусть  $XYX'Y'$  — 4-орбита. Так как  $P, T, A, B, X, Y$  лежат на циркулярной кубике, а  $A, B, X, Y$  — на одной окружности, то по задаче 4.10b,  $PT$  проходит

через  $\infty$ , что и требуется.

**5.8.** «Транзит изогональных шестерок» следует, например, из задачи 3.7.

**5.9.** Рассмотрим две пары изогонально сопряженных точек  $X, X'$  и  $Y, Y'$ . По теореме об изогоналях точки  $XY \cap X'Y'$  и  $XY' \cap X'Y$  тоже изогонально сопряжены, т.е. лежат на кубике. Следовательно,  $X + Y = X' + Y'$  и  $X + Y' = X' + Y$  или  $X - X' = Y - Y' = Y' - Y$ .

**5.10.** (\*ВПИСАННЫЙ\*) Для вписанного четырехугольника  $ABA'B'$  преобразование  $f_{AB,A'B'}$  совпадает с инверсией, переводящей  $A$  в  $B$ , а  $A'$  в  $B'$ . Центром этой инверсии является точка  $P$  пересечения прямых  $AB, A'B', XY, X'Y'$ , причем  $\angle APX = \angle Y'PA'$ . Пусть точка  $X_1$  симметрична  $X$  относительно  $PA$ , а  $Y'_1$  симметрична  $Y'$  относительно  $PA'$ . Тогда из подобия треугольников  $PXX'$  и  $PY'Y$  следует равенство отношений  $X'X_1 : XX' = YY'_1 : YY'$ , равносильное утверждению задачи.

**5.11.** (\*ГАРМОНИЧЕСКИЙ\*)

a) Прямая  $AA'$  является симедианой треугольников  $ABB'$  и  $A'BB'$ , а прямая  $BB'$  симедианой треугольников  $ABA'$  и  $AB'A'$ . Поэтому  $M_A$  и  $M_B$  изогонально сопряжены.

b)  $\angle M_AB'A' = \angle AB'B = \angle M_AA'B$ . Для точки Брокара  $\angle BrB'A' = \angle BrA'B$ , откуда  $A', B', M_A, Br$  лежат на одной окружности.

c) Можно рассмотреть инверсию с центром  $W$ .

**5.12.** (\*ПАРАЛЛЕЛОГРАММ\*)

a) Действительно, это необходимое условие, оно эквивалентно  $isog_B(AA', XX')$ , так как из симметрии  $\angle(A'X, A'B) = \angle(AX', AB')$ . Задача 3.7 говорит о том, что этого условия достаточно для выполнения любого из остальных условий изогональности

b) Нетрудно убедиться, что, если две из четырех окружностей равны, то и две оставшихся равны им. При этом, если окружности  $XAB$  и  $XA'B'$  равны, то равны и опирающиеся на равные хорды углы  $(XA, XB)$  и  $(XB', XA')$ .

c) При изменении радиуса равных окружностей  $ABX$  и  $A'BX$  прямые  $AX$  и  $A'X$  врачаются с равными скоростями в противоположных направлениях. Поэтому точка их пересечения описывает равностороннюю гиперболу.

**5.13.**

a) При инверсии относительно вписанной окружности прямые  $AB, AB', A'B, A'B'$  переходят в окружности равного радиуса, следовательно, точки их пересечения образуют параллелограмм. Значит, окружность  $ABI$  касается окружности  $A'B'I$ , а окружность  $AB'I$  окружности  $A'BI$ .

b) Пусть  $T_1, T_2, T_3, T_4$  — точки касания окружности с прямыми  $AB, AB', A'B, A'B'$ . Середины отрезков  $T_iT_j$ , точки пересечения диагоналей и противоположных сторон четырехугольника  $T_1T_2T_3T_4$  и центр  $I$  окружности лежат на равносторонней гиперболе, а инверсные образы этих точек на кубике фокусов.

**5.14.**

a) Имеем  $A + A' = B + B'$ , т.е.  $A + A = B + B$ . Значит, касательные к кубике в точках  $A, B, A', B'$  пересекают кубику в одной точке.

b) Пусть  $E$  — точка на диагонали  $BB'$  такая, что  $Isog_A(BA', B'E)$  и  $Isog_{A'}(BA, B'E)$ . Из теорем синусов для треугольников  $ABA'$ ,  $AB'A'$ ,  $ABE$ ,  $AB'E$ ,  $A'BE$  и  $A'B'E$

выводится условие  $AB \cdot A'B' = AB' \cdot A'B$ .

с) Отметим точку пересечения  $Q = BB' \cap (PA'B')$ . Из вписанных углов нетрудно вывести, что  $A, P, Q, B$  — на одной окружности, т.е.  $Q$  принадлежит 4-орбите точки  $P$ .

д) Можно вывести из двух предыдущих пунктов.

## Другие описания кубики фокусов

**5.15.** Выведем сначала уравнение в случае, когда  $\varphi$  совпадает с комплексным сопряжением:  $(x, y) \mapsto (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$ . Запишем условие принадлежности середин  $XX'$  одной прямой  $2Ax + 2By = 1$  (прямой Ньютона-Гаусса): получим  $(Ax + By + 1)(x^2 + y^2) + Ax - By = 0$ . Остается сделать поворот, после которого прямая Ньютона-Гаусса вертикальна, а уравнение приобретает указанный вид.

**5.16.**

а) Выберем систему координат так, чтобы отличная от круговых бесконечная точка кубики совпадала с бесконечной точкой оси ординат. Тогда уравнение кубики примет вид  $(x^2 + y^2)(x + A) = Bx + Cy + D$ . Легко видеть, что касательные в круговых точках проходят через начало координат.

б)  $M$  и  $M' = \infty$  (точка, соответствующая асимптоте) — сопряжены, поэтому, согласно общей теории, сопряженная  $O'_1 = O_2$  к круговой точке  $O_1$  получается последовательным центральным проектированием в  $M'$  и  $M$ . Но  $s_{M'}(O_1) = O_2$ , поэтому  $s_M(O_1) = O_2$ .

**5.17.** (точки касания окружностей пучка) ??

а) То, что ГМТ  $X, Y$  — кубика, проверяется непосредственным вычислением. Эта кубика совпадает с  $\mathcal{C}$ , потому что проходит через  $M, L, L'$  и круговые точки, а касательные к ней в  $L, L'$  и круговых точках проходят через  $M$ .

б) Сумма  $X + Y$  не зависит от выбора окружности.

**5.18.** Все фактически показано при выводе кубического уравнения для  $ISO(ABA'B')$ .

## 6 Квартеты и изогональные кубики

### 6.1.

а) Пусть барицентрические координаты точки  $J = (x_0 : y_0 : z_0)$ , а точки  $P = (x : y : z)$ . Тогда барицентрические координаты точки  $P' = (a^2yz : b^2zx : c^2XY)$ , где  $a, b, c$  — длины сторон  $YZ, ZX, XY$  соответственно, и условие коллинеарности трех точек дает уравнение третьей степени относительно  $x, y, z$ .

б) Так как при изогональном сопряжении бесконечная прямая переходит в описанную окружность, круговые точки сопряжены друг другу.

**6.2.** Пусть  $P_1 = \varphi_X(P), P_2 = \varphi_Y(P_1)$ . Так как  $XZ \cdot XY = XP \cdot X P_1$  и  $\angle ZXP = \angle P_1XY$ , треугольники  $XPZ$  и  $XY P_1$  подобны. Аналогично треугольник  $XY P_1$  подобен треугольнику  $P_2YZ$ , и, значит,  $P_2 = \varphi_Z(P)$ . Таким образом, композиция любых двух из преобразований  $\varphi_X, \varphi_Y, \varphi_Z$  равна третьему.

Пусть  $Q$  — точка изогонально сопряженная  $P, Q_1 = \varphi_X(Q)$ . Тогда  $X, P, Q_1$  лежат на одной прямой, так же как и точки  $X, Q, P_1$ . Кроме того,  $\angle XYP_1 + \angle XYQ_1 = \angle XPZ + \angle XQZ + \pi + \angle Y$ , следовательно, прямые  $YQ_1$  и  $YP_1$  симметричны относительно биссектрисы угла  $Y$  и точки  $P_1, Q_1$  изогонально сопряжены (рис. 6.1).

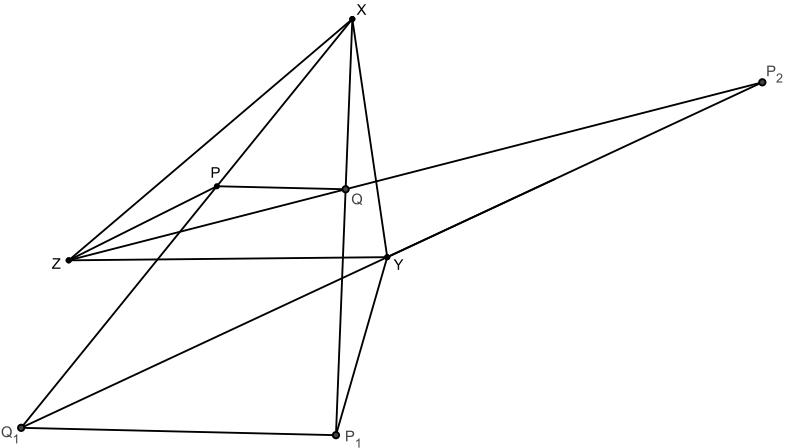


Рис. 6.1.

**Примечания.** 1. То, что  $\varphi_X$  коммутирует с изогональным сопряжением можно доказать и так. Применяя к точке  $P$  в любом порядке изогональное сопряжение и  $\varphi_X$ , мы получим точку на прямой  $XP$ . Легко видеть, что обе композиции задают проективные отображения этой прямой на себя, поэтому

достаточно проверить, что они совпадают для трех положений точки  $P$ . Но обе композиции меняют местами  $X$  и точку пересечения прямой с  $XP$  с  $YZ$  и описанной окружностью, а также бесконечно удаленную точку с точкой пересечения  $XP$  и  $YZ$ .

2. Из равенства  $XP \cdot XP_1 = XQ \cdot XQ_1$  следует также  $PQ \parallel P_1Q_1$ .

### 6.3.

- a) Следует из предыдущей задачи.
- b) Следует из примечания 2 к предыдущей задаче.
- c) Из предыдущего пункта следует, что эти точки лежат на кубике, задаваемой бесконечной точкой прямых  $AA'$ ,  $BB'$ ,  $CC'$ ,  $DD'$ .
- d) Имеем равенства  $A + D + X = A + C + Y = B + C + X = B + D + Y$ , из которых, очевидно, следует,  $A + A = B + B$ .

Свойствам квартетов был посвящен проект на XXII ЛКТГ [?]. В частности, там предлагалась задача, которую не смог решить ни один из участников.

**6.4.** Пусть  $A, B, C, D$  — квартет,  $A', B', C', D'$  — изогонально сопряженный квартет;  $P_X$  — точка пересечения  $AD$  и  $BC$ ,  $P_Y$  —  $AC$  и  $BD$ ,  $P_Z$  —  $AB$  и  $CD$ . Точки  $Q_X, Q_Y, Q_Z$  определяются аналогично по точкам  $A', B', C', D'$ . Докажите, что

- a) Из равенств  $A + D' = B + C'$ ,  $D + D' = C + C'$  и  $D' + D' = C' + C'$  следует, что  $A + D = B + C$ , т.е.  $P_X$  лежит на кубике. Аналогично на кубике лежат  $P_Y, P_Z, Q_X, Q_Y, Q_Z$ . Тогда из равенств  $A + D + P_X = A' + D' + Q_X = B + D + P_Y = B' + D' + Q_Y$  получаем  $A + A' + P_X + Q_X = B + B' + P_Y + Q_Y$ . Поскольку  $A + A' = B + B' = \infty$  (бесконечная точка кубики), это равенство означает, что прямые  $P_XQ_X$  и  $P_YQ_Y$  пересекают кубику в одной и той же точке. Эта точка изогонально сопряжена бесконечной и, значит, лежит на описанной окружности. Прямая  $P_ZQ_Z$  пересекает кубику в той же точке.
- b) Из равенств  $A + D + P_X = A' + D' + Q_X = B + D + P_Y = B' + D' + Q_Y = A + D' + X = B' + D + Y$  получаем  $X + Y = P_X + Q_Y = P_Y + Q_X$ .
- c) Точка  $Z'$  пересечения кубики со стороной  $XY$  изогонально сопряжена  $Z$ , следовательно  $ZZ'$  проходит через  $\infty$ .

**6.5.** Из условия следует, что квартеты  $A_1, B_1, C_1, D_1$  и  $A_2, B_2, C_2, D_2$  порождают одну и ту же кубику. При этом  $A_1 - B_1$  и  $A_2 - B_2$  — одна и та же точка второго порядка. Следовательно,  $A_1 + A_2 = B_1 + B_2$ , т.е. прямые  $A_1A_2$  и  $B_1B_2$  пересекают кубику в одной и той же точке.

**6.6.** Так как  $X, Y, Z, \infty$  — квартет, касательные в этих точках пересекают кубику в одной и той же точке. Эта точка изогонально сопряжена бесконечно удаленной и, значит, лежит на описанной окружности.

Все кубики квартетов проходят через точки  $X, Y, Z$ , центры  $I, I_X, I_Y, I_Z$  вписанной и внеписанных окружностей треугольника  $XYZ$  и круговые точки. Таким образом, эти кубики образуют пучок. Геометрическим местом точек пересечения касательных к кубикам пучка в круговых точках будет коника, поскольку соответствие между касательными проективно. Рассмотрим вырожденную кубику, состоящую из внешней биссектрисы  $I_XI_Y$  угла  $Z$  и окружности  $XYIIZ$ . Касательные к ней в круговых точках пересекаются в центре окружности — середине дуги  $XY$ . При этом сама кубика пересекает описанную окружность

ность в противоположной точке — середине дуги  $XZY$ . Аналогично получаем, что касательные в круговых точках пересекаются в точке описанной окружности, даметрально противоположной точке кубики, для пяти других вырожденных кубик пучка. Следовательно, это верно для всех кубик.

**6.7.** Касательные к кубике фокусов в круговых точках пересекаются на кубике. По предыдущей задаче получаем, что четвертая точка пересечения кубики с описанной окружностью должна быть противоположна одной из вершин. Бесконечная точка кубики изогонально сопряжена этой точке и, значит, лежит на соответствующей высоте треугольника.

**Примечание.** Пусть бесконечная точка кубики лежит на высоте из вершины  $Z$ ;  $A, B, C, D$  — произвольный квартет. Тогда кубика является кубикой фокусов для прямых  $AC, BC, AD, CD$ . Точкой Микеля этих прямых будет точка  $Z$ , а прямой Гаусса — серединный перпендикуляр к отрезку  $XY$ .

**6.8.** Пусть  $U$  — точка пересечения касательных к кубике в точках  $X, Y, Z$  и  $J$ . Из равенств  $X+X+U=Y+Y+U=Z+Z+U=J+J+U=J_1+J_2+J=0$ , где  $J_1, J_2$  — круговые точки, получаем, что  $J_1+J_2+X+Y+Z+U=0$ , т.е.  $U$  лежит на окружности  $XYZ$ . Рассмотрим кубику квартетов, проходящую через  $U$ . Она совпадает с данной, поскольку имеет с ней семь общих точек:  $X, Y, Z, U, J, J_1, J_2$ , причем касательные в точках  $X, Y, Z$  к обеим кубикам совпадают.

## Еще про 8-орбиты

**6.9. Указание.** Пусть инверсия с центром  $T$  переводит точки  $X, Y, Z$  в  $X', Y', Z'$ . Тогда 8-орбита переходит в два изогонально сопряженных относительно треугольника  $X'Y'Z'$  квартета.

Если точки  $T, X, Y, Z$  лежат на одной окружности, можно также использовать инверсию, переводящую эти точки в вершины прямоугольника. Преобразованию  $g_{T,X,Y,Z}$  при этой инверсии будет соответствовать инверсия относительно описанной окружности этого прямоугольника.

# Isoptic cubics (cubics of foci) and more circulal cubics

P.Kozhevnikov, A.Zaslavsky

(Presented by D.Demin, M.Didin, A.Zaslavsky, A.Zaslavsky, K.Ivanov,  
P.Kozhevnikov, F.Nilov, I.Frolov)

One of the goals of this project is to study so-called isoptic cubic curve. It could be defined in different ways, e.g., as the locus of points from which from which the (oriented) angles viewing the two given segments are equal. While studying interesting connections are revealed between different plots of elementary geometry (inscribed angles, intersecting circles, etc.), geometry transformations (like symmetry, inversion, isogonal conjugation, etc.), and some properties of cubic curves (operation of addition of points on a cubic, etc.).

Content and section dependancy:

- In sections 0 — 3 we consider some (interesting in themselves) geometrical constructions, and study some geometry technique needed further. In sections 0—3 we have NO CUBICS, so fans of elementary geometry could work with these sections independently. Section 4 is devoted to cubics only, nevertheless, in many further questions NO CUBICS required.

- In section 0 we collect some known facts on isogonal conjugation (see also, e.g., [8] (theorem on isogonals), [12] (isogonal sextets and use of them in problem solving), [3]). Also here initial results on isoptic cubics are presented.

- Note that sections 1 and 2 contain some important by not so well-known questions.

- Section 3 is some branch connected with previous, but not used further.

- Section 4 contains some general facts on cubics; these facts could be helpful further. Note the importance of Cayley-Bacharach theorem on 9 points and the operation of addition of points on cubics. For some questions (including the questions from elementary geometry) the language of cubics appears to be possibly the most natural. On one hand, we tried to limit the number of presented facts (otherwise, we have a large and detailed course on cubics only); on the other we tried to provide the possibility of some effective use of cubics. A more detailed acquaintance with cubic curves is welcome but not required (see, e.g., [5], [11], [9], [10]).

- Later the main sections 5 and 6 will be presented; they contain some nice pieces on which the interaction of ideas of elementary and algebraic geometry takes place. Section 5 is devoted to isoptic cubics, here some key questions are already in this list. Section 6 mostly connected with the project of TofT Summer Conference-2010 [13]. We believe that some new ideas could be helpful for better understanding and, in particular, for solving problem 19a which was not solved by the students in 2010.

In several problems we deal with some special (not the general) case, (e.g., the case of inscribed, circumscribed, degenerate quadrilateral, parallelogram, etc.) For such problems we put a corresponding note marked with \*\*.

# 0 Isogonal conjugation in polygons

## Isogonals with respect to an angle (pair of lines)

Let  $O, X, Y, X', Y'$  be points in the plane.

**Definition.** Let us say that  $X$  and  $X'$  (or, lines  $OX$  and  $OX'$ ) are *isogonals* with respect to angle  $YOY'$  (or, to the pair of lines  $OY, OY'$ ), if  $OX$  and  $OX'$  are symmetric in the bisector of angle  $YOY'$ .

The fact that  $OX$  and  $OX'$  are isogonals with respect to angle  $YOY'$  denote by  $Isogo_O(XX', YY')$ .

**0.1.** Assume that lines  $OX, OX', OY, OY'$  are distinct. Prove that the condition  $Isogo_O(XX', YY')$  is equivalent to each of the following conditions:

- a)  $Isogo_O(YY', XX')$ ;
- b) pairs of lines  $OX, OX'$  and  $OY, OY'$  have common bisectors;
- c)  $\angle(OX, OY) = \angle(OY', OX')$ , i.e., oriented angles viewing  $XY$  and  $Y'X'$  from  $O$  are equal (depending on the configuration, this condition is equivalent to one of equalities  $\angle X O Y = \angle Y' O X'$ ,  $\angle X O Y + \angle Y' O X' = 180^\circ$ ; e.g., if  $O$  lies inside convex quadrilateral  $XYX'Y'$ , the second equality is true).
- d)  $\rho(X, OY)/\rho(X, OY') = \rho(X', OY')/\rho(X', OY)$  (here by  $\rho(X, \ell)$  denoted the oriented distance from  $X$  to line  $\ell$ ).
- e) Projections of  $X$  and  $X'$  onto  $OY$  and  $OY'$  (in case they are distinct) are concyclic.

**0.2. Theorem on isogonals.** Let  $Z = XY \cap X'Y'$  and  $Z' = X'Y \cap XY'$  (so that  $X, X', Y, Y', Z, Z'$  are the vertices of a complete quadrilateral. Then  $Isogo_O(XX', YY')$  implies  $Isogo_O(XX', ZZ')$  (and similarly,  $Isogo_O(ZZ', YY')$ ).

Sometimes we use *points at infinity* (in fact extending to the projective plane). We may assume that the plane if supplemented by the line at infinity. Each point of the line at infinity considered as a common point of a family of all pairwise parallel lines.

### 0.3.

- a) Define  $Isogo_O(XX', YY')$  if  $O$  is a point at infinity.
- b) Formulate and prove the theorem on isogonals for the case if  $O$  is a point at infinity.
- c) **Newton-Gauss line.** Prove that the midpoints of the diagonals of a complete quadrilateral are collinear.

## Isogonal conjugation in a triangle

**0.4.** Let  $ABC$  be a triangle, and let  $P$  be a point not lying on its sidelines. Prove that lines symmetric to  $AP, BP, CP$  in bisectors of angles  $A, B, C$ , respectively, have a common point (possibly a point at infinity).

**Definition.** Let the lines from the previous problem meet at  $P'$ .  $P'$  is called *isogonally conjugate* to  $P$  with respect to  $ABC$ .

Obviously,  $P'$  is isoonally conjugate to  $P$  iff  $P$  is isoonally conjugate to  $P'$ . Thus isogonally conjugate point form pairs. We may consider each point of a sideline as an isogonally conjugate to the opposite vertex.

**0.5.** Prove that the isogonal conjugate to  $P$  is a point at infinity iff  $P$  lies on the circle  $(ABC)$ .

**0.6.** Let  $P_a, P_b, P_c$  be points symmetric to  $P$  wrt sidelines of  $ABC$ . Prove that  $P'$  is the center of the circle  $(P_a P_b P_c)$ .

**0.7.** Prove that the projections of  $P$  and  $P'$  onto the sidelines of  $ABC$  lie on a circle (it is called the *pedal circle* for each of  $P, P'$ ).

**0.8.** Let  $P$  and  $P'$  be isogonally conjugate wrt  $ABC$ . Prove that there exists a conic with foci  $P, P'$  tangent to  $AB, BC, CA$ .

**0.9.** Let  $X, X'$  and  $Y, Y'$  be two pairs of isogonally conjugate points wrt  $ABC$ . Prove that  $XY \cap X'Y'$  and  $XY' \cap X'Y$  are isogonally conjugates.

## Isogonal conjugation in a quadrilateral

Let  $A, A', B, B'$  be fixed points (not all are collinear). Further by quadrilateral  $ABA'B'$  we mean points  $A, B, A', B'$  in this given cyclic order (in particular, broken line  $ABA'B'$  could be self-intersecting).

**0.10.** Let  $ABA'B'$  be a quadrilateral, and  $X$  be a point. Let the isolonals of  $AX, BX, A'X$  wrt the angles  $A, B, A'$  of  $ABA'B'$ , respectively, intersect at some point  $X'$  (possibly  $X'$  is a point at infinity). Prove that the isogonal of  $B'X$  wrt the angle  $B'$  also passes through  $X'$ .

**Definition.** Under conditions of the previous problem,  $X$  and  $X'$  are called *isogonally conjugates* wrt  $ABA'B'$ . (We consider pair of vertices  $A, A'$  (and  $B, B'$ ) as isogonally conjugates.)

The locus of points having its isogonal conjugate denote by  $ISO(ABA'B')$ .

Thus  $X$  and  $X'$  are isogonally conjugates wrt  $ABA'B'$  iff all the conditions  $Isog_A(BB', XX'), Isog_{A'}(BB', XX'), Isog_B(AA', XX'), Isog_{B'}(AA', XX')$  are true. The previous problem shows that it is sufficient to put only 3 of 4 these conditions.

**0.11.** Prove that  $X \in ISO(ABA'B')$  is equivalent to  $Isog_X(AA', BB')$ .

Recall that  $Isog_X(AA', BB')$  means that from  $X$  oriented angles viewing  $AA'$  and  $BB'$  are equal; this note is in accordance with another name *Isoptical cubic* for  $ISO(ABA'B')$ .

**0.12.** (Isogonal sextet) Consider a sextet (more precisely, a triple of pairs) of points  $(A, A'; B, B'; C, C')$  (here coincidence allowed only inside one of 3 pairs.)

a) Prove that  $C$  and  $C'$  are isogonally conjugates wrt  $ABA'B'$  iff  $A$  and  $A'$  are isogonally conjugates wrt  $BCB'C'$ .

b) Suppose that of the following 6 conditions  $Isog_A(BB', CC'), Isog_{A'}(BB', CC'), Isog_B(AA', CC'), Isog_{B'}(AA', CC'), Isog_C(AA', BB'), Isog_{C'}(AA', BB')$  any three are true. Prove that all 6 conditions are true.

**0.13.** Assume that no 3 of points  $A, B, A', B'$  are collinear. Prove that  $X$  and  $X'$  are isogonally conjugates wrt  $ABA'B'$  iff  $X$  and  $X'$  are isogonally conjugates wrt to some two of triangles fromed by lines  $AB, BA', A'B', B'A$ .

**0.14.** Assume that no 3 of points  $A, B, A', B'$  are collinear. Prove that  $X \in ISO(ABA'B')$  is equivalent to each of the following conditions:

- a) Projections of  $X$  onto  $AB, AB', A'B, A'B'$  lie on a circle or a line (moreover, projections of  $X'$  also lie on it, if  $X'$  is not a point at infinity).
- b) There exists a conic with focus  $X$  tangent to  $AB, AB', A'B, A'B'$  (moreover,  $X'$  is the second focus of this conic).
- c) In 3D there exists a pyramid  $SABA'B'$ , all faces of which are tangent to a sphere, and  $X$  is the tangent point of this sphere to the plane  $ABA'B'$ .

**0.15.** Find the locus of the midpoints of  $XX'$ , where  $X \in ISO(ABA'B')$ , and  $X'$  is the isogonal conjugate of  $X$ .

**0.16.** (\*COLLINEAR\*) For collinear  $A, B, A', B'$  let us define  $ISO(ABA'B')$  as the set of  $X$  for which  $Isogx(AA', BB')$  is true. Find  $ISO(ABA'B')$

- a) in the case  $A = A'$ , and  $A$  lies on the segment  $BB'$ ;
- b) in the case of co-directed, but not equal  $\vec{AB}$  and  $\vec{B'A'}$ .

We will continue working with  $ISO(ABA'B')$  in section ??.

# 1 Isocyclic involutions

In the following construction with circles we define some transformations, we call them *isocyclic*.

Let  $A, B, C, D$  be four points. Let  $f_{AB,CD}$  maps  $X$  to  $Y$  that is the second intersection point of circles (lines)  $(ABX)$  and  $(CDX)$  (note that  $Y$  is not well-defined for some «non-regular» points  $X$ ).

The above-mentioned transformations are interesting in themselves and have proven to be useful in formulating and proving many claims.

## 1.1.

a) The location of «almost always» could be defined by (oriented) angles viewing segments  $AB$ ,  $BC$ , etc., from  $X$ . Determine  $f_{AB,CD}$  in terms of transformations of these angles.

b) Prove that  $f_{AB,CD}$  maps any circle passing through  $A$  and  $D$  to a circle passing through  $B$  and  $C$ .

## 1.2.

a) (Clifford theorem, reformulated). Prove that

$$f_{AB,CD} f_{BC,DA} = f_{BC,DA} f_{AB,CD}.$$

b) Extend  $f_{AB,CD} f_{BC,DA}$  to «non-regular» points. (In particular, find the image of  $A$  and of the point at infinity.)

## 4-orbits

For four given points  $A, B, A', B'$ , (commuting) transformations  $f_{AB,A'B'}$ ,  $f_{AB',A'B}$  (more precisely, the group of four transformations  $f_{AB,A'B'}$ ,  $f_{AB',A'B}$ ,  $f_{AB,A'B'} f_{AB',A'B}$ , and the identity transformation  $Id$ ) defines a partition of all «regular» points into 4-orbits of the form:  $X, Y = f_{AB,A'B'}(X), Y' = f_{AB',A'B}(X)$  и  $X' = f_{AB,A'B'}(Y') = f_{AB',A'B}(Y)$ . Points  $A, A', B, B', X, X', Y, Y'$  form a «closed (Clifford) configuration» of 8 points and 8 circles having the following combinatorial symmetry: and two of four of equitable pairs  $(A, A')$ ,  $(B, B')$ ,  $(X, X')$ ,  $(Y, Y')$  form a 4-orbit for the other two pairs. Three of four pairs form a constructoin which is studied in section 3.

**1.3. (\*INSCRIBED\*)** Let  $A, B, A', B'$  lie on circle  $\Omega$  with center  $O$ .

- a) Determine  $f_{AB,A'B'}$ ?
- b) Find the locus of fixed points of  $f_{AB,A'B'}$ .
- c) Find the 4-orbit of  $O$ .
- d) Prove that each 4-orbit is concyclic (or collinear);
- e) and the circles from the previous item are co-axis (have common radical axis).

**1.4. (\*PARALLELOGRAM\*)** Let  $ABA'B'$  be a parallelogram.

- a) Prove that  $f_{AB,A'B'} f_{AB',A'B}$  is a central symmetry.
- b) Prove that each 4-orbit ia a parallelogram  $XYX'Y'$  whose angles are equal to the angles of  $ABA'B'$ .
- c) Let  $P$  be a point, and let  $O_1, O_2, O_3, O_4$  be centers of circles  $ABP, BA'P, A'B'P, B'AP$ . Prove that the angle between  $O_1O_3$  and  $O_2O_4$  is constant (independent of the choice of  $P$ ).

d) Let parallelogram  $ABA'B'$  is a pedal quadrilateral for a quadrilateral  $CDC'D'$  and a point  $P$ . Prove that  $f_{CD,C'D'}f_{CD',C'D}(P)$  is a intersection point of diagonals of  $CDC'D'$ .

## 8-orbits and quartets

For four given points  $A, B, A', B'$ , consider (pairwise commuting) involutions  $f_{AB,CD}$ ,  $f_{AC,BD}$ ,  $f_{AD,BC}$  (more precisely, a group  $G$  of 8 transformations generated by them). These transformations define the partition of all «regular» points into *8-orbits* (each 8-orbit could be obtained as a union of two 4-orbits).

Note that involution  $g_{A,B,C,D} = f_{AB,CD}f_{AC,BD}f_{AD,BC}$  does not depend of ordering points  $A, B, C, D$ .

One may consider a subset  $H \subset G$  of transformations that could be obtained as a product of an even number of isocyclic involutions. There are 4 such transformations (including *Id*), and, as we will see in section 2, all these transformations are cyclic. We call the orbits under the action of  $H$  by *quartets*. Quadruple  $A, B, C, D$  is one of quartets. Each 8-orbit could be obtained as a union of two quartets, one of which is the image of the other by  $g_{A,B,C,D}$ .

We continue to study this interesting construction in section 6.

## 2 Inversion+reflection

**2.1.** Prove that

a) the circumcircles of four triangles formed by lines  $AB$ ,  $AB'$ ,  $A'B$ ,  $A'B'$ , have a common point (*Miquel point*);

b) Miquel point is the center of similitude taking  $\vec{XY}$  to  $\vec{X'Y'}$ .

**Definition.** By *inversion+reflection* with center  $O$  we mean the product of an inversion in a circle  $\omega$  centered at  $O$  and a symmetry about some line  $\ell$  passing through  $O$ .

For given points  $X, X', Y, Y'$  by  $\varphi_{XYX'Y'}$  denote a unique circular transformation (= a Möbius transformation of the complex plane), interchanging points  $X \leftrightarrow X'$ ,  $Y \leftrightarrow Y'$ .

If the midpoints of  $XX'$  and  $YY'$  coincide (further we call this case centrally-symmetric, or the case of PARALLELOGRAM), then  $\varphi_{XYX'Y'}$  is a central symmetry. Otherwise (regular case)  $\varphi_{XYX'Y'}$  is an inversion+reflection with center at Miquel point  $M = M_{XYX'Y'}$ .

A fixed inversion+reflection lets «to observe» all regular quadruples. The following precise claim about this:

**2.2.** (universality of  $\varphi$ ) Let  $\varphi$  be a fixed inversion+reflection with center  $O$ . Prove that for each regular quadruple  $(X, X'; Y, Y')$  there exist exactly two (symmetric in  $O$ ) quadruples of the form  $(A, \varphi(A); B, \varphi(B))$ , similar (with same orientation) to  $(X, X'; Y, Y')$ .

The next problems shows an important connection with isocyclic involutions.

**2.3.** (split) Prove that

$$\varphi_{ABCD} = f_{AB,CD} f_{BC,AD}.$$

**2.4.**

a) Prove that  $\varphi_{ABCD} \varphi_{ACBD} = \varphi_{ACBD} \varphi_{ABCD}$ .

b) Find the transformation that equals to this product.

Further for Miquel point (=centers of inversion+reflection) and corresponding inversions+symmetries use also the following short notation (as in [13]):  $X = M_{ABDC}$ ,  $Y = M_{ABCD}$ ,  $Z = M_{ACBD}$ ,  $\varphi_X = \varphi_{ABDC}$ ,  $\varphi_Y = \varphi_{ABCD}$ ,  $\varphi_Z = \varphi_{ACBD}$ . Also set  $P_X = AD \cap BC$ ,  $P_Y = BD \cap AC$ ,  $P_Z = CD \cap AB$ .

**2.5.** Prove that  $\varphi_X(P_Y) = P_Z$ .

(Note that this fact is in accordance with theorem on isogonals.)

**2.6.** Prove that  $\varphi_X(Y) = Z$ .

We see that one could fix  $\varphi_X$ ,  $\varphi_Y$ ,  $\varphi_Z$  and vary quartets  $A, B, C, D$  — further see section 6.

### 3 Harmonic sextets

In the plane (accomplished by the point  $\infty$ ) consider ordered sextets (more precisely, triples of unordered pairs) of points  $(A, A'; B, B'; C, C')$ . Here allow coincidence inside pairs  $A$  and  $A'$ ,  $B$  and  $B'$ ,  $C$  and  $C'$ .

**Definition.** We call sextet  $(A, A'; B, B'; C, C')$  *harmonic*, if

$$\frac{a - b'}{b' - c} \cdot \frac{c - a'}{a' - b} \cdot \frac{b - c'}{c' - a} = -1, \quad (1)$$

where  $a, a'$ , etc. are complex numbers corresponding to points  $A, A'$ , etc.

**3.1.** Prove that the property of  $(A, A'; B, B'; C, C')$  «to be harmonic» is invariant under

- a) transpositions of pairs  $(A, A') \leftrightarrow (B, B')$ ,  $(B, B') \leftrightarrow (C, C')$ ,  $(C, C') \leftrightarrow (A, A')$ ;
- b) transpositions inside  $(A, A')$ ,  $(B, B')$ ,  $(C, C')$ ;
- c) the choose of complex coordinates in the plane;
- d) under circular transformations (see, e.g., [6]).

**3.2.** For five points  $A, A', B, B', C$  there exists a unique  $C'$  such that  $(A, A'; B, B'; C, C')$  is harmonic.

**3.3.**

a) Sextet  $(A, A'; B, B'; C, C')$  is harmonic iff  $C' = \varphi_{ABA'B'}(C)$ , or  $\varphi_{ACA'C'} = \varphi_{ABA'B'}$ .

b) Let  $A, A'; B, B'; C, C'; D, D'$  be 8 points (coincidence allowed inside pairs  $A, A'$ , etc., only) Suppose that  $(A, A'; B, B'; C, C')$  and  $(A, A'; B, B'; D, D')$  are harmonic. Prove that  $(A, A'; C, C'; D, D')$  is also harmonic.

Moreover, note that if  $\varphi_{ACA'C'} = \varphi_{ABA'B'} = \varphi$  is a central symmetry, then the midpoints of  $AA'$ ,  $BB'$ ,  $CC'$  coincide, and harmonic sextet  $(A, A'; B, B'; C, C')$  is symmetric (about a point). Otherwise (if  $\varphi$  is an inversion+reflection), then the midpoints of  $AA'$ ,  $BB'$ ,  $CC'$  are distinct, and we call such harmonic sextet  $(A, A'; B, B'; C, C')$  *rugular*. A fixed inversion+reflection lets «to obsevre» all regular harmonic sextets as a «similar copy» of the form  $(A, \varphi(A); B, \varphi(B); C, \varphi(C))$ .

**3.4.** Let  $(A, A'; B, B'; C, C')$  be a harmonic sextet. Prove that

$$\angle(AB, AC) + \angle(AB', AC') = \angle(A'B, A'C) + \angle(A'B', A'C').$$

### Harmonicity and products of similitudes

Let us denote by  $h_{X,Y \rightarrow Z}$  the similitude with center  $X$  taking  $Y$  to  $Z$ .

Consider the following relations (here  $R$  and  $L$  are choosen to label relations on angles (rotation) and lengths (lengths); further the cyclic sequence like  $A'B'C'$  determines the cyclic order (in the sextet)  $BA'CB'AC'$  uniquely):

$$\angle(\overrightarrow{A'B}, \overrightarrow{A'C}) + \angle(\overrightarrow{B'C}, \overrightarrow{B'A}) + \angle(\overrightarrow{C'A}, \overrightarrow{C'B}) = 0, \quad (R - A'B'C')$$

where by  $(\vec{a}, \vec{b})$  we mean the measure of the angle of counterclockwise rotation from  $\vec{a}$  to  $\vec{b}$  taking modulo  $2\pi$ .

$$\frac{BA'}{A'C} \cdot \frac{CB'}{B'A} \cdot \frac{AC'}{C'B} = 1. \quad (L - A'B'C')$$

### 3.5.

- a) Prove that sextet  $(A, A'; B, B'; C, C')$  is harmonic iff the conditions  $(R - A'B'C')$  and  $(L - A'B'C')$  are fulfilled.
- b) Prove that sextet  $(A, A'; B, B'; C, C')$  is harmonic iff  $h_{B', C \rightarrow A} h_{A', B \rightarrow C} h_{C', A \rightarrow B} = Id$ .
- c) (generalized Napoleon theorem) From  $(R - A'B'C')$  and  $(L - A'B'C')$  derive  $(L - C'AB')$ .
- d) Find the way to construt the center of the product of two similitudes.
- e) Among all conditions of the form  $(R - \dots)$ ,  $(L - \dots)$  find pairs of conditions which imply all the other conditions.

Some constructions with conditions  $(R - A'B'C')$  and  $(L - A'B'C')$  are considered in [4], where these conditions are formulated as existence of a quadruple  $X, Y, Z, T$  such that  $AC'B \sim XTY$ ,  $BA'C \sim YTZ$ ,  $CB'A \sim ZTX$ . E.g., in [7] there examples of applying generalized Napoleon theorem to some constructions with «add-ons»  $BA'C$ ,  $CB'A$ ,  $AC'B$  constructed on the sides of a triangle  $ABC$ : if conditions  $(R - A'B'C')$  and  $(L - A'B'C')$  are given, then, by  $(L - C'AB')$ , the angles of triangle  $A'B'C'$  could be found in terms of the angles of add-ons only, regardless of the angles of  $ABC$ .

**3.6.** Establish the following description: sextet  $(A, A'; B, B'; C, C')$  with  $A \neq A'$  and  $B \neq B'$  is harmonic iff one of the two following conditions hold:

- 1) circles (lines)  $(ABC')$ ,  $(A'BC)$ ,  $(AB'C)$ ,  $(A'B'C')$  are pairwise distinct and they have a common point;
- 2)  $A, A', B, B', C, C'$  are concyclic and  $AA', BB', CC'$  are concurrent,  $A, A', B, B', C, C'$  are collinear points which could be transformed by a circular transformation to a concyclic configuration mentioned above.

### 3.7.

- a) Prove that the isogonal sextet  $(A, A'; B, B'; C, C')$  is harmonic.
- b) Prove that if  $Isog_A(BB', CC')$  holds, then the harmonic sextet  $(A, A'; B, B'; C, C')$  is isogonal.
- c) Prove that that if the midpoints of  $AA'$ ,  $BB'$ ,  $CC'$  are collinear, then the regular harmonic sextet  $(A, A'; B, B'; C, C')$  is isogonal.

## 4 Information about cubics

**Definition.** *Algebraic curve* is the set of points with (complex) coordinates  $(x, y)$  satisfying to  $F(x, y) = 0$ , where  $F(x, y)$  is a polynomial probably with complex coefficients. *Degree* of algebraic curve is the minimal degree of corresponding polynomials.

Algebraic curves of degree 2 and 3 are called also *conics* and *cubics* respectively.

**Definition.** A triple  $(x : y : z) \neq (0 : 0 : 0)$  of (complex) numbers defined apart from a common multiplicative (complex) constant is called *homogeneous coordinates* of the point on the (complex) projective plane. If  $z \neq 0$  we can identify the triple  $(x, y, z)$  with the point  $(x/z, y/z)$  of (complex) Euclidean plane. The triples with  $z = 0$  correspond to the infinite points.

Algebraic curves are often considered as subsets of (complex) projective plane. Then the equation  $F(x, y) = 0$  of degree  $n$  is rewrited in homogeneous coordinates as  $P(x : y : z) = 0$ , where  $P = z^n F(x/z, y/z)$  is *homogeneous* polynomial of degree  $n$  such that  $F(x, y) = P(x : y : 1)$  (for example if  $F(x, y) = x^3 - 2y^2 + 3xy - x + 1$ , then  $P(x, y, z) = x^3 - 2y^2z + 3xyz - xz^2 + z^3$ ).

**Definition.** Algebraic curve is *degenerated*, if any correspondent polynomial is reducible (i.e. equals to the product of polynomials with smaller degrees).

Partially a degenerated cubic is defined by equation  $QL = 0$ , where  $Q$  and  $L$  are polynomials of degrees 2 and 1 respectively; so it is the union of the line  $L = 0$  and the conic  $Q = 0$  (this conic also can be degenerated).

We will to consider the intersection of cubic  $\mathcal{C}$  and line  $\ell$ . To find  $\mathcal{C} \cap \ell$  we have to prove the system  $P(x, y, z) = 0$ ,  $L(x, y, z) = 0$  of homogeneous equations with degrees 3 and 1 respectively. Using  $L(x, y, z) = 0$  we can express one of coordinates through the remaining ones and substitute it in  $P(x, y, z) = 0$ . For example substituting  $z$  we obtain a homogeneous equation  $R(x, y) = 0$  of degree 3. In the degenerate case  $R \equiv 0$  polynomial  $P$  is divisible by  $L$  and  $\ell \subset \mathcal{C}$ . If  $R \neq 0$ , then  $R$  is a product of linear polynomials  $L_1 L_2 L_3$  ( $L_i$  in general case have complex coefficients). Each equation  $L_i = 0$  define a point  $A_i \in \mathcal{C} \cap \ell$  (probably infinite or non-real). Some of  $L_i$  can be proportional. If  $L_1 = \lambda L_2$ , then the point  $A_1 = A_2$  is a *multiple* common point: point of order 2 if  $L_3$  is not proportional to  $L_1$ , and point of order 3, if all  $L_i$ ,  $i = 1, 2, 3$ , are proportional. It can be proved that the order of common point does not depend on the coordinate system  $x, y, z$ . Thus a non-degenerated cubic  $\mathcal{C}$  meets an arbitrary line  $\ell$  exactly in three points taking into consideration their orders.

Several *special* cubics  $\mathcal{C}$  contain so called *singular* points (for example the point  $(0, 0)$  is a self-intersection point of curve  $y^2 = x^3 + x^2$  and cuspidal points of curve  $y^2 = x^3$ ; formally the point is especial if the partial derivatives of the polynomial equal zero). If the order of a non-singular common point  $A_1 \in \mathcal{C} \cap \ell$  is grater than 1, then  $\ell$  touches  $\mathcal{C}$  at  $A_1$ ; if the order of  $A_1$  is 3,  $A_1$  is called *an inflexion point* of  $\mathcal{C}$ . (Understand the geometrical sense of this.)

Since the cubic meets any line at three points we can define for an arbitrary non-singular point  $P \in \mathcal{C}$  *the projection* with center  $P$ : the involution  $s_P : \mathcal{C} \rightarrow \mathcal{C}$ , mapping point  $X \in \mathcal{C}$  to the third common point of  $PX$  with  $\mathcal{C}$  (if  $X = P$  the line

$PX$  is the tangent to  $\mathcal{C}$ ; for the inflection point  $O$  we have  $s_O(O) = O$ .

In general to find the common points of two curves with degrees  $m$  and  $n$  we have to solve an equation of degree  $mn$ . Thus by the *Besou theorem*:

Two algebraic curves with degrees  $m$  and  $n$  defined by relatively prime polynomials have exactly  $mn$  common points taking into consideration their orders.

We do not give strict definition of the order of common point because it is not necessary for the solution of the problems. Not only that the (non-singular) touching point  $A$  of two curves is their common point with order greater than 1. (For example understand that two concentric circles have two imaginary infinite touching point (the circular points defined below)).

By the Besou theorem we obtain that an arbitrary conic meets a nondegenerated cubic at 6 point taking into consideration their orders and two different cubics have exactly 9 common points taking into consideration their orders.

It is known that for any point  $X$  there exists 6 lines passing through  $X$  and touching the given non-special cubic  $\mathcal{C}$ . Also 6 touching points lie on the conic. If  $X \in \mathcal{C}$ , then two or three of these lines coincide with the tangent at  $X$ .

Mention another significant theorem:

*The Shales theorem (about 9 points on three cubics).* Let two cubics intersecting at 9 points (taking into consideration their orders) be given. Then any cubic passing through eight of these points passes also through the remaining one.

This theorem can be also used for degenerated cubics.

**Definition.** Let a cubic  $\mathcal{C}$  and a non-singular point  $O$  (zero) on it be given. For two arbitrary non-singular point  $A, B \in \mathcal{C}$  find third common point  $C$  of line  $AB$  with  $\mathcal{C}$ , after this find third common point of line  $OC$  and  $\mathcal{C}$ . Call this point the *sum*  $A + B$  of points  $A$  and  $B$ .

**4.1.** Prove that

- a) the addition of points of a cubic is associative:  $(A + B) + C = A + (B + C)$ ;
- b) for any (non-singular) points  $A, B$  there exists a unique point  $A - B$ , such that  $B + (A - B) = A$ .

**4.2.** Express the operation « $+$ » with zero at point  $O' \in \mathcal{C}$  through the operation « $+$ » with zero at point  $O \in \mathcal{C}$ .

**4.3.**

a) Prove that for any three non-singular points  $A, B, C$  of  $\mathcal{C}$  lying on a line  $\ell$  the sum  $A + B + C$  does not depend on  $\ell$ .

b) Let  $O$  be a suflection point. Prove that  $A + B + C = O$  if and only if  $A, B, C$  are collinear.

The assumption of problem 4.1. means that the addition of points on  $\mathcal{C}$  (without singular points) define the structure of Abelian group. It may be proved (see problem 4.2), that this structure does not depend on the choice of zero=point  $O$ . This group can be defined as a group of transformations

$\mathcal{C} \rightarrow \mathcal{C}$  having view  $X \mapsto X + C$ .

**4.4.** (the criterium of commutating projections). Let  $P, P' \in \mathcal{C}$  be non-singular points. Prove that  $s_P s_{P'} = s_{P'} s_P$  if and only if

- a) for any  $X \in \mathcal{C}$  we have the closing condition:  $s_P s_{P'} s_{P'} s_P(X) = X$ ;
- b) the tangents to  $\mathcal{C}$  at  $P$  and  $P'$  meet on  $\mathcal{C}$ .

The condition (a) allows to define in case  $s_P s_{P'} = s_{P'} s_P$  the following bijection between the pairs  $(X, X'), (Y, Y')$  of points on  $\mathcal{C}$ :  $Y = s_P(X)$ ,  $X' = s_{P'}(Y)$ ,  $Y' = s_P(X') = s_{P'}(X)$  (so  $XX'$ ,  $YY'$ ,  $PP'$  — are the diagonals of the quadrangle inscribed into  $\mathcal{C}$ ).

**4.5.** (Points of order 2 and the translation involutions.) Let  $C \in \mathcal{C}$  be such point that  $C \neq O$  and  $C + C = O$ . (I.e  $C$  is the point of Abelian group with order 2.) Then the translation  $X \mapsto X + C$  is an involution  $X \leftrightarrow X'$ .

- a) Choosing an inflection point as  $O$  describe the points of order 2 and the corresponding involutions. How many points of order 2 may be on the cubic?
- b) Prove that the tangents to  $\mathcal{C}$  at  $X$  and  $X'$  meet on  $\mathcal{C}$ ; and inversely the pair of points  $P, P' \in \mathcal{C}$  such that the tangents to  $\mathcal{C}$  at these point meet on  $\mathcal{C}$  defines the translation involution  $X \mapsto X + P' - P$ .

**4.6.** Let  $\mathcal{C}$  be a non-special cubic and  $O$  be an inflection point. Prove that the sum of six points equals  $O$  if and only if they lie on the conic.

**4.7.**

- a) Fix  $A, B, C, D \in \mathcal{C}$ . For any point  $X$  find the sixth common point (taking into consideration their orders)  $Y$  of the conic passing through  $A, B, C, D, X$  with  $\mathcal{C}$ . Prove that all lines  $XY$  concur.
- b) Fix  $P, C, D \in \mathcal{C}$ . For an arbitrary line passing through  $P$  find the points  $X \in \mathcal{C}$  and  $Y = s_P(X)$ . Consider a conic passing through  $C, D, X, Y$  and meeting  $\mathcal{C}$  also at points  $Z, T$ . Prove that all lines  $ZT$  pass through a fixed point  $Q \in \mathcal{C}$ .

## Circular cubics

**Definition.** Points (imaginary) with homogeneous coordinates  $(1, i, 0)$  and  $(1, -i, 0)$  are called *circular points*.

**Definition.** A cubic passing through two circular points is called *circular cubic*.

**4.8.** Prove that any circle (i.e a line with equation  $(x - a)^2 + (y - b)^2 = r^2$ , where  $a, b, r$  are complex numbers) passes through circular points.

**4.9.** Let  $X \leftrightarrow X'$  be a translation involution on circular cubic  $\mathcal{C}$ :  $X' = X + C$ , where  $C + C = O$ . For non-singular points  $A, B, X \in \mathcal{C}$  distinct from the circular points prove that the second non-circular common point of circles  $(ABX)$  and  $(A'B'X)$  lies on  $\mathcal{C}$ .

**4.10.** (pencils of «antiparallels») Let  $P$  and  $Q$  lie on a circular cubic  $\mathcal{C}$ . Passing lines through  $P$  we obtain pairs of points  $X, Y$  on  $\mathcal{C}$ . Passing lines through  $Q$  we obtain pairs of points  $Z, T$ .

- a) Prove that if  $X, Y, Z, T$  are concyclic for several lines, then this is true for arbitrary lines.

- b) The assumption of the previous item is true if and only if  $PQ$  is parallel to *the asymptote* (i.e the line passing through the infinite point of cubic distinct from the circular points).

## 5 Cubics of foci

Further (in sections 5 and 6), when we deal with an equation of a cubic, we assume that its coefficients are real (though we can substitute complex coordinates of points in this equation).

### Properties of cubics of foci

#### 5.1.

- a) Prove that if  $X \in ISO(ABA'B')$ , then  $Y = f_{AB,A'B'}(X) \in ISO(ABA'B')$ ;
- b) all such lines  $XY$  have a common point.

**5.2.** Prove that  $\varphi = \varphi_{ABA'B'}$  maps any point  $X \in ISO(ABA'B')$  to the isogonally conjugated point  $X'$ .

**5.3.** Prove that  $ISO(ABA'B')$  is a circular cubic.

**5.4.** Prove that (in regular case)  $ISO(ABA'B')$  contains the following points:

- a)  $A, B, A', B'$ ;
- b)  $P = AB \cap A'B', P' = AB' \cap A'B$ ;
- c) the Mickel point  $M = M_{ABA'B'}$ ;
- d) the projection of a common point of  $AA'$  and  $BB'$  to the line  $PP'$ ;
- e) point  $T = T_{AB',A'B}$  such that triangles  $TAB'$  and  $TA'B$  are similar and oppositely oriented (and point  $T_{AB,A'B'}$  defined similarly).

**5.5.** For all points indicated in the previous problem find

- a) isogonally conjugated points
- b) and corresponding 4-orbit.

**5.6.** (Asymptote and Newton-Gauss line) Prove that the asymptote of  $ISO(ABA'B')$

- a) is parallel to the Newton-Gauss line;
- b) passes through the reflection of  $M$  about the Newton-Gauss line.

**c)** Prove that for any  $X \in ISO(ABA'B')$  the midpoint of segment between  $X$  and  $s_M(X)$  lies on the Newton-Gauss line.

#### 5.7.

- a) (S.Berlov) Prove that all lines  $XY$  (see problem 5.1) pass through  $T_{AB',A'B}$ .
- b) Prove that line  $PT_{AB',A'B}$ , where  $P = AB \cap A'B'$ , is parallel to the Newton-Gauss line.

**5.8.** Let  $(C, C')$  and  $(D, D')$  be two pairs of isogonally conjugated points of  $ISO(ABA'B')$ . Prove that the cubic of foci  $ISO(CDC'D')$  coincide with  $ISO(ABA'B')$ , and the pairs of isogonally conjugated points are the same for both cubics.

**5.9.** Let  $X, X'$  be isogonally conjugated points on a cubic of foci. Prove that  $X - X' = K$  is the point of order 2 not depending on  $X$  (i.e.  $K + K = O$ ).

**5.10.** (\*CYCLIC\*) Let points  $A, B, A', B'$  lie on a circle  $\Omega$  centered at  $O$ . Let  $X, Y, X', Y'$  be the 4-orbit of a point  $X \in ISO(ABA'B')$ . Prove that the conics with foci  $X, X'$  and  $Y, Y'$  inscribed into  $ABA'B'$  are similar.

**5.11.** (\*HARMONIC\*) Let  $ABA'B'$  be a harmonic quadrilateral (i.e. inscribed with equal products of opposite sides).

- a) Prove that the midpoints  $M_A$  and  $M_B$  of segments  $AA'$  and  $BB'$  lie on  $ISO(ABA'B')$ .
- b) (Brocard points) Prove that  $M_A$  and  $M_B$  form a 4-orbit with Brocard points  $Br_1, Br_2$ .
- c) Let  $AA' \cap PP' = W$ , and  $\omega$  be circle  $(M_A Br_1 M_B Br_2)$ . Prove that the central projection  $\omega \rightarrow \omega$  with center  $W$  maps the 4-orbit  $M_A Br_1 M_B Br_2$  to the 4-orbit of  $O$ .

**5.12.** (\*PARALLELOGRAM\*) Let  $ABA'B'$  be a parallelogram.

- a) Prove that  $X \in ISO(ABA'B')$  if and only if  $\angle(BA, AX) = \angle(A'X, A'B)$ .
- b) Prove that  $X \in ISO(ABA'B')$  if and only if circles  $(XAB), (XAB'), (XA'B'), (XA'B')$  are congruent.
- c) Prove that  $ISO(ABA'B')$  is the union of the infinite line and the hyperbola passing through  $A, B, A', B'$ ;
- d) and this hyperbola is equilateral and has the asymptotes parallel to the bisectors of angles of  $ABA'B'$ .

**5.13.** (\*CIRCUMSCRIBED + DEGENERATED  $A = A'$ \*)

- a) Let  $ABA'B'$  be a quadrilateral which is non-parallelogram, and let  $I$  be its degenerate 4-orbit (i.e., such 4-orbit that all 4 its points coincide). Determine if the following implications are true:  $I \in ISO(ABA'B') \Leftrightarrow AB, BA', A'B', B'A$  are tangents to a circle.
- b) In this case  $M_{ABA'B'}$  coincide with the projection of the center of circle  $(AIA')$  to the symmedian of triangle  $AIA'$  from  $I$ .
- 5.14.** (\*ac=bd\*) Let  $C$  be the third common point of  $AA'$  and  $ISO(ABA'B')$ , and  $D$  be the third common point of  $BB'$  and  $ISO(ABA'B')$ .
- a) When  $C = D$ ?
- b) When  $D = C'$ ?
- c) (semiBrocard). Call  $P$  a (first/second) semiBrocard point if  $\angle(PA, AB) = \angle(PA', A'B')$  and  $\angle(PB, BA') = \angle(PB', B'A)$ . Prove that two of four points of 4-orbit of semiBrocard point lie on  $AA'$  and  $BB'$ .
- d) (IMO2018) Let  $ABCD$  be a convex quadrilateral such that  $AB \cdot CD = BC \cdot DA$ . Point  $X$  inside  $ABCD$  is such that  $\angle XAB = \angle XCD$  and  $\angle XBC = \angle XDA$ . Prove that  $\angle BXA + \angle DXC = 180^\circ$ .

## Another descriptions of cubics of foci

**5.15.** Let Miquel point  $M$  be the origin of the coordinate system, and let its isogonally conjugated point be the infinite point of axis  $y$ . Prove that the cubic of foci has equation  $(x^2 + y^2)(x + A) = Bx + Cy$ .

**5.16.** Prove that

- a) a circular cubic is a cubic of foci if and only if the tangents at circular points meet on the cubic;
- b) in this case the tangents meet at the Mickel point  $M$ .

**5.17.** (touching points of circles of a pencil) Let  $L, L'$  be two non-circular points of a cubic of foci  $\mathcal{C}$  such that the tangents at these points pass through  $M$ . Take an

arbitrary circle passing through  $L$  and  $L'$ , and the tangents  $MX, MY$  to it. Prove that

- a)  $X, Y \in \mathcal{C}$ ;
- b) all lines  $XY$  meet  $\mathcal{C}$  at the same point.
- c) Let a pencil of circles and an arbitrary point  $M$  be given. Prove that the locus of points  $X, Y$ , where  $MX, MY$  are the tangents to an arbitrary circle of the pencil is a cubic of foci.
- d) How the view of the cubic depend on the type of the pencil.

**5.18.** (Universality of  $\varphi$  or the collection of all cubics of foci) Let  $\varphi$  be a given inversion and symmetry with center  $M$ .

- a) Let a line  $m$  be given. Prove that the locus of points  $X$  such that the midpoint of  $X\varphi(X)$  lies on  $m$  is a cubic of foci.
- b) Find the correspondence between lines  $m$  and cubics of foci.
- c) Descript the sets of common points of different cubics of foci.

## 6 Quartets and isogonal cubics

**6.1.** Let a triangle  $ABC$  and a point  $J$  be given. Prove that

a) the locus of such points  $P$  that  $P$ , isogonally conjugated point  $P'$ , and  $J$  are collinear is a cubic passing through the vertices of triangle, its incenter, excenters,  $J$ , and isogonally conjugated point  $J'$ ;

b) this cubic is circular if and only if  $J$  is an infinite point.

Let a triangle  $XYZ$  be given. As in section 2 denote as  $\varphi_X$  the composition of inversion centered at  $X$  with the reflection about the bisector of angle  $X$ , transposing  $Y$  and  $Z$ . Define  $\varphi_Y, \varphi_Z$  similarly.

**6.2.** Prove that these maps commute each other and commute with isogonal conjugation.

Let  $A$  be an arbitrary point,  $B = \varphi_Z(A)$ ,  $C = \varphi_Y(A)$ ,  $D = \varphi_X(A)$ . The quadruple  $\{A, B, C, D\}$  is called a *quartet* with respect to triangle  $XYZ$ .

**6.3.** Prove that

a) the quadruple of isogonally conjugated points  $\{A', B', C', D'\}$  is also a quartet;

b) the lines  $AA', BB', CC', DD'$  are parallel;

c) the points  $A, B, C, D, A', B', C', D', X, Y, Z$  lie on a circular cubic (call it the *quartets cubic*);

d)  $A + A = B + B = C + C = D + D$ , i.e. the tangents to the quartets cubic at  $A, B, C, D$  meet the cubic at the same point.

The properties of quartets were considered in the project of XXII Summer Conference [13]. In partial, the following problem was proposed there, but the participants did not solve it.

**6.4.** Let  $A, B, C, D$  be a quartet,  $A', B', C', D'$  be isogonally conjugated quartet;  $P_X$  be the common point of  $AD$  and  $BC$ ,  $P_Y$  be the common point of  $AC$  and  $BD$ ,  $P_Z$  be the common point of  $AB$  and  $CD$ . points  $Q_X, Q_Y, Q_Z$  are defined similarly using points  $A', B', C', D'$ . Prove that

a) the lines  $P_XQ_X, P_YQ_Y, P_ZQ_Z$  concur at a point lying on the circumcircle of  $XYZ$ ;

b) the lines  $P_XQ_Y, P_YQ_X$  and  $XY$  concur at a point  $Z'$ ;

c)  $ZZ'$  is parallel to  $AA', BB', CC', DD'$ .

**6.5.** Let  $D_1, D'_1$  and  $D_2, D'_2$  be two pairs of isogonally conjugated points such that  $D_1D'_1 \parallel D_2D'_2$ . Prove that the lines  $A_1A_2, B_1B_2, C_1C_2, D_1D_2$  concur ( $A_1, B_1, C_1, D_1$  and  $A_2, B_2, C_2, D_2$  are quartets).

**6.6.** Let the tangents to a quartets cubic at  $X$  and  $Y$  meet at  $P$ , and the tangents at circular points meet at  $Q$ . Prove that  $PQ$  is a diameter of circle  $XYZ$ .

**6.7.** Where a quartets cubic is a cubic of foci?

**6.8.** Let  $\mathcal{C}$  be a circular cubic,  $J$  be its infinite point distinct from circular points,  $X, Y, Z$  be such points that  $X + X = Y + Y = Z + Z = J + J$ . Prove that  $\mathcal{C}$  is a quartets cubic with respect to triangle  $XYZ$ .

### Once more about 8-orbits

**6.9.** Let  $A, B, C, D, A^* = g_{A,B,C,D}(A), B^*, C^*, D^*$  be a 8-orbit with respect to

$X, Y, Z, T$ .

- a) Prove that the circles  $(TAA^*)$ ,  $(TBB^*)$ ,  $(TCC^*)$ ,  $(TDD^*)$  touch each other;
- b) Prove that the circles  $(TAD)$ ,  $(TA^*DA^*)$ ,  $(TYZ)$  are coaxial (where  $D = \varphi_{XYZT}(A)$ ).

## 7 Once more

### Isogonal conjugation of circles

**7.1.** (F. Nilov) Let a quadrilateral  $ABCD$  be given. Let  $l_a, l_b, l_c, l_d$  be the internal bisectors of angles  $A, B, C, D$  respectively. Let  $a, b, c, d$  be lines passing through  $A, B, C, D$  respectively in such a way that the common points of  $a$  and  $b$ ,  $b$  and  $c$ ,  $c$  and  $d$ ,  $d$  and  $a$  lie on a circle  $\alpha$ . Let  $a', b', c', d'$  be the reflections of  $a, b, c, d$  about  $l_a, l_b, l_c, l_d$  respectively.

- a) Prove that the common points of  $a'$  and  $b'$ ,  $b'$  and  $c'$ ,  $c'$  and  $d'$ ,  $d'$  and  $a'$  lie on a circle  $\alpha'$ ;
- b) and  $\alpha' = \varphi_{ABCD}(\alpha)$ .

## Список литературы

- [1] A. Akopyan. Geometry in figures. Edition 2, 2017.
- [2] A. Akopyan, A. Zaslavsky. Geometry of conics. Amer. Math. Soc., Providence, RI, 2007. (edition 2 in Russian)
- [3] A. Akopyan, A. Zaslavsky. Different views on isogonal conjugation. (in Russian) Матем. просв., сер. 3, 11, Изд-во МЦНМО, М., 2007, 61–78.
- [4] N. Beluhov. On some pairs of perspective triangles. (in Russian). Матем. просв., сер. 3, 14, Изд-во МЦНМО, М., 2010, , 256–259.
- [5] N. Vasilyev. Pascal hexagrams and cubic curves. (in Russian) Квант, 1987, 8, 2–8.
- [6] A. Zaslavsky. Geometrical transformations. (in Russian) Изд-во МЦНМО, М., 2004.
- [7] P. Kozhevnikov. Generalized Napoleon theorem. Сборник «Элементы математики в задачах. Через олимпиады и кружки к профессии.» Изд-во МЦНМО, М., 2018, 196–202.
- [8] A. Kulikova, D. Prokopenko. Theorem on isogonals. (in Russian) Квант, 2018, 4, 41–44, 5, 34–37.
- [9] V. Ostrik, M. Tsfasman. Algebraic geometry and number theory: rational and elliptic curves. (in Russian) Изд-во МЦНМО, М., 2005.
- [10] V. Prasolov, Yu. Solovyev. Elliptic functions and algebraic equations. (in Russian) М.: Факториал, 1997.
- [11] Yu. Solovyev. Arithmetic of elliptic curves. (in Russian) Квант, 1987, 7, 2–8.
- [12] A. Utkin. Isogonal conjugation in a quadrilateral. (in Russian) Квант, 2019, 2, 37–42.
- [13] <https://www.turgor.ru/lktg/2010/1/index.htm>

# **Focal and circular cubics**

Solutions and hints (preliminary version)

# 0 Isogonal conjugation in polygons

## Isogonal conjugation in a quadrilateral

**0.10.** Use the assumption of 0.1d.

**0.11.** Use the assumption of 0.14a.

**0.12.**

a) Follows from the previous problem.

b) There are two different combinatory cases which follow from 0.10 and 0.11 respectively.

**0.13.** Using 0.7, 0.8 we obtain that if  $X$  and  $X'$  are isogonally conjugated with respect to pairs  $a, b$  and  $b, c$ , then  $X$  and  $X'$  are isogonally conjugated with respect to  $c, a$ .

Also we can assert: if  $X$  and  $X'$  are isogonally conjugated with respect to some polygon, then they are isogonally conjugated with respect to any two its sidelines.

**0.14.**

a) 1) Let  $X \in ISO(ABA'B')$ . Then by 0.1e the projections of  $X$  and  $X'$  to  $AB, AB'$  lie on a circle  $\omega$ , the projections of its center  $O$  bisect the projections of segment  $XX'$ , thus  $O$  is the midpoint of  $XX'$ . Similarly the projections of  $X$  and  $X'$  to  $A'B', A'B$  lie on a circle with center  $O$  and radius  $R = OX_{AB'}$  (where  $X_{AB'}$  is the projection of  $X$  to  $AB'$ ), i.e. on  $\omega$ . Finally repeat this reasoning for  $A'B, A'B'$ .

1') Let the projections of  $X$  to  $AB, AB', A'B, A'B'$  lie on a circle  $\omega$  centered at  $O$ . Then the point isogonally conjugated to  $X$  with respect to the triangle formed by lines  $AB, AB', A'B$  coincide with the reflection  $X'$  of  $X$  about  $O$ . The same point is isogonally conjugated to  $X$  with respect to the triangle formed by lines  $A'B', AB', A'B$ . Hence by 0.13,  $X$  and  $X'$  are isogonally conjugated with respect to  $ABA'B'$ .

2) The assumption  $Isog_X(AA', BB')$  is true if and only if the projections  $X_{AB}, X_{BA'}, X_{A'B'}, X_{B'A}$  are concyclic. In fact, using  $\angle(X_{AB}X_{BA'}, X_{BA'}X_{A'B'}) = \angle(X_{AB}X_{BA'}, X_{BA'}X) + \angle(XX_{BA'}, X_{BA'}X_{A'B'}) = \angle(AB, BX) + \angle(XA', A'B')$  and similar equalities we obtain that  $\angle(X_{AB}X_{BA'}, X_{BA'}X_{A'B'}) = \angle(X_{AB}X_{B'A}, X_{B'A}X_{A'B'}) \Leftrightarrow \angle(BX, AX) = \angle(B'A, A')$ .

b) The following reasoning yields that b) and  $X \in ISO(ABA'B')$  are equivalent. Let  $R = OX_{AB} = OX'_{AB}$ . Let  $X_0$  be the reflection of  $X$  about  $AB$ ,  $T = X'X_0 \cap AB$ . Then  $XT$  and  $X'T$  are symmetric with respect to  $AB$  and  $XT \pm X'T = \pm 2R$ , i.e.  $OX_{AB}$  is a medial line of triangle  $OX'X_0$  and  $XT = X_0T$ . A conic with foci  $X, X'$  and (major) semiaxis  $\pm 2R$  touches  $AB$ .

*Remark.* Note that this conic twice touches a (pedal) circle with center  $O$  and radius  $R$ . It is the Brocard conic of point  $X$  corresponding to angle  $90^\circ$ . (This remark can be generated for *skew-pedal circle*).

c) Let such pyramid with insphere  $\omega$  exist. Then the cone  $K$  with vertex circumscribed around  $\omega$  is also inscribed into the pyramid. Inscribe into  $K$  another sphere  $\omega'$  touching  $ABA'B'$  at  $X'$ . This is a known construction of Dandelin spheres, and points  $X, X'$  are the foci of a conic inscribed into  $ABA'B'$  (this conic is the section of  $K$  by the plane  $ABA'B'$ ).

*Remark.* For the circumscribed pyramid we have  $\angle ASB + \angle A'SB' = \angle BSA' +$

$\angle B'SA$ , which generates the equality  $\angle AXB + \angle A'XB' = \angle BXA' + \angle B'XA$  equivalent (for the point inside  $ABA'B'$ ) to  $Isog_X(AA', BB')$ .

**0.15.** The midpoints of  $XX'$  are centers of conics inscribed into  $ABA'B'$ . It is known that they lie on the Newton-Gauss line. Each point of the Gauss line corresponds to exactly one pair  $X, X'$  of points symmetric with respect to it. This can be obtained for example using complex coordinates (see. 3.7.).

**0.16.**

Let  $X$  does not lie on  $AA'BB'$ . Since the bisectors of angles  $AXA'$  and  $BXB'$  coincide, we obtain that  $X$  lies on the common Appolonius circle of pairs  $A, A'$  and  $B, B'$ . Such circle is unique (as the common circle of two pencils or such circle that  $A$  and  $A'$ ,  $B$  and  $B'$  are inverse about it). In problem a) the locus of  $X$  satisfying to  $Isog_X(AA', BB')$  is the union of  $AA'$  and the Appolonius circle  $\omega$  of points  $A$  and  $A'$  passing through  $B = B'$ .

*Remark.* This problem explains another name of  $ISO(ABA'B')$  — Apollonius cubic.

Problem b) was proposed by L.Emelyanov on the South tournament nearly 20 ago.

# 1 Isocyclic involutions

## 1.1.

a) Directed angles  $\angle(XB, XA)$  and  $\angle(XD, XC)$  do not change.

$$\angle(YC, YB) = \angle(YC, YX) + \angle(YX, YB) = \angle(DC, DX) + \angle(AX, AB) = \angle D + \angle(DA, XD) + \angle A + \angle(XA, DA) = \angle D + \angle A + \angle(XA, XD).$$

Similarly for angles  $\angle(YA, YD)$  and  $\angle(XB, XC)$ .

b) follows from the previous  $\angle(XA, XD)$  is constant, therefore  $\angle(YB, YC)$  is constant.

**1.2.** After an inversion with center  $A$  the assertion follows from the existence of a Mickel point.

Also we can obtain this assertion from the description of  $f_{AB,CD}f_{BC,DA}$  (as inversion+reflecton) given in section 2. This description allows also to define  $f_{AB,CD}f_{BC,DA}$  for «non-regular» points?

## 4-orbits

### 1.3.

a) Let  $P = AB \cap A'B'$ . Then  $P$  is the radical center of circles  $(ABXY)$ ,  $(A'B'XY)$  and  $\Omega$ , hence  $XY$  passes through  $P$ , also  $PX \cdot PY = \deg_\Omega P$ , thus  $f_{AB,A'B'}$  is the inversion with center  $P$  conserving  $\Omega$ .

b) By the previous the set of immobile points of  $f_{AB,A'B'}$  is the circle with center  $P$  and radius  $\sqrt{\deg_\Omega P}$ .

c) Let  $P' = AB' \cap A'B$ ,  $E = AA' \cap BB'$ ,  $L = P'E \cap PO$ ,  $L' = PE \cap P'O$ . It is known that  $P'E$  is the polar of  $P$  with respect to  $\Omega$ , hence  $P'E \perp PO$  and  $PO \cdot PL = \deg_\Omega P$ , thus  $L = f_{AB,A'B'}(O)$ . Similarly  $L' = f_{A'B,AB'}(O)$  and  $E = PL' \cap P'L$  — the fourth vertex of 4-orbit  $O, L, E, L'$ .

d) Since  $PX \cdot PY = PX' \cdot PY' = \deg_\Omega P$ , we obtain that  $X, Y, X', Y'$  are concyclic and the degrees of  $P$  with respect to circles  $(YXX'Y')$  are the same for all 4-orbit  $X, Y, X', Y'$ .

e) Similarly the degrees of  $P'$  with respect to circles  $(YXX'Y')$  are equal, therefore  $PP'$  is the radical axis of all  $(YXX'Y')$ .

### 1.4.

a) Let  $Y = f_{AB,A'B'}(X)$ . Then  $\angle(AY, YB') = \angle(AY, XY) + \angle(XY, YB') = \angle(AB, BX) + \angle(XA', A'B') = \angle(XA', AB) + \angle(AB, BX) = \angle(A'X, XB)$ . Let  $X', Y'$  are the reflections of  $X, Y$  about the center of the parallelogram. Then by the symmetry  $\angle(A'Y', Y'B) = \angle(AY, YB')$ , hence  $\angle(A'Y', Y'B) = \angle(A'X, XB)$ , and  $B, A'X, Y'$  are concyclic. Similarly  $B', AX, Y'$  are concyclic, hence  $Y' = f_{A'B,AB'}(X)$ . From similar reasoning about  $X'$  we obtain that  $X, Y, X', Y'$  is a 4-orbit (of  $X$ ).

b) We have  $\angle(XY, XY') = \angle(XY, XB) + \angle(XB, XY') = \angle(AY, AB) + \angle(A'B, A'Y')$ , by symmetry this is equal to  $\angle(AY, AB) + \angle(AB', AY) = \angle(AB', AB)$ .

c) Let  $X = P$  and  $X, Y, X', Y'$  be the 4-orbit of  $X$ . Then  $O_1O_3 \perp XY$  (the centers line is perpendicular to the common chord of circles  $(ABP)$  and  $(A'B'P)$ ), similarly  $O_2O_4 \perp XY'$ . Then by the previous the angle between  $O_1O_3$  and  $O_2O_4$  equals the angle between  $XY$  and  $XY'$  and equals to the angle of the parallelogram.

*Remark.* This problem was proposed by P.Kozhevnikov for the South Tournament in 2017.

d) Let  $A, B, A', B'$  be the projections of  $P$  to  $CD, DC', C'D', D'C$  respectively,  $Q = f_{CD', C'D}(P)$ ,  $K = CC' \cap DD'$ . Then  $\angle(DQ, QC) = \angle(DQ, QP) + \angle(PQ, QC) = \angle(DC', C'P) + \angle(PD', D'C) = \angle(BA', A'P) + \angle(PA', A'B) = \angle(BA', A'B)$ . By the previous (since  $D, C', D', C$  are the homothetic images of  $O_1, O_2, O_3, O_4$  with center  $P$  and coefficient 2),  $\angle(DK, KC) = \angle(BA', A'B)$ , hence  $C, D, Q, K$  are concyclic. Similarly  $C', D', Q, K$  are concyclic, therefore  $K = f_{CD, C'D'}(Q)$ , q.e.d.

*Remark.* If  $CDC'D'$  is cyclic this fact corresponds to 1.3c.

## 2 Inversion+reflection

**2.1.** This is well known.

**2.2.** If  $ABA'B'$  is given then the center, the axis and the radius of inversion+reflection are defined by the following way: the center is the Mickel point  $M$  if  $ABA'B'$ , the axis bisects the angle between  $MA$  and  $MA'$ , the radius equals  $\sqrt{MA \cdot MA'}$ . A similarity maps  $(X, X'; Y, Y')$  to  $(A, \varphi(A); B, \varphi(B))$  if and only if it maps the center, the axis and the inversion circle for  $(X, X'; Y, Y')$  to the center, the radius, and the inversion circle for  $(A, \varphi(A); B, \varphi(B))$ .

Next problem indicate important connection with isocyclic involutions.

**2.3.** (split) For the central symmetric case see problem 1.4.

Let  $\varphi = \varphi_{ABA'B'}$  — is the inversion+reflection centered at  $M$ .

For an arbitrary point  $C$  define  $D = f_{AB,A'B'}(C)$  and  $C' = \varphi(C)$ . Prove that  $A, B', D, C'$  are concyclic which is equivalent to  $\angle(AD, DB') = \angle(AC', C'B')$ . This will be sufficient because similarly we obtain that  $A', B, D, C'$  are concyclic an hence  $C' = f_{AB',A'B}(D)$ .

We have  $\angle(AD, DB') = \angle(AD, DC) + \angle(DC, DB') = \angle(AB, BC) + \angle(CA', A'B')$  as inscribed angles. From inversion+reflection  $\angle(AC', C'B') = \angle(AC', C'M) + \angle(MC', C'B') = \angle(CA', A'M) + \angle(MB, BC)$ . Hence  $\angle(AD, DB') - \angle(AC', C'B') = \angle(AB, BC) + \angle(CA', A'B') + \angle(A'M, CA') + \angle(BC, MB) = \angle(AB, MB) + \angle(A'M, A'B') = 0$ .

**2.4.** Prove that  $\varphi_{ABCD}\varphi_{ACBD} = \varphi_{ABDC}$  (and similarly  $\varphi_{ACBD}\varphi_{ABCD} = \varphi_{ABDC}$ ). Left and right expressions are circular maps of I type transposing  $A$  with  $D$  and  $B$  with  $C$ . Such map is unique.

Also we can obtain the solution from the previous problem:  $\varphi_{ABCD} = f_{AB,CD}f_{BC,AD} = f_{BC,AD}f_{AB,CD}$ . Then  $\varphi_{ACBD}\varphi_{ABCD} = (f_{AC,BD}f_{BC,AD})(f_{BC,AD}f_{AB,CD}) = f_{AC,BD}f_{BC,AD}^2f_{AB,CD} = f_{AC,BD}f_{AB,CD} = \varphi_{ABDC}$ .

(How the requirement of regularity for  $f_{AB,CD}, \dots$  can be avoided?)

**2.5.** Follows from  $\varphi_X(BD) = (XAC)$ ,  $\varphi_X(AC) = (XBD)$ , and since  $X$  is a Mickel point the circles  $(XAC)$  and  $(XBD)$  pass through  $P_Z = AB \cap CD$ .

*Remark: this fact corresponds with the isogonals theorem.*

**2.6.** Follows from  $\varphi_X((BCZ)) = (CBY)$  and  $\varphi_X((ADZ)) = (DAY)$ , because  $P_Y$  lies on the circles  $(BCZ)$ ,  $(ADZ)$ , and  $P_Z$  lies on the circles  $(CBY)$  and  $(DAY)$ .

### 3 Harmonic sextets

#### 3.1.

- a) Immediate check.
- b) Immediate check.
- c) Translation  $z \rightarrow z + c$ , multiplying by constant  $z \rightarrow cz$ ,  $c \neq 0$ , and conjugation  $z \rightarrow \bar{z}$  conserve (1).
- d) By immediate check we obtain that the map  $z \rightarrow 1/z$  conserve (1). This and the previous result yield that all fractionally-linear maps (circular maps of type I) conserve (1), also the composition of fractionally-linear maps and the conjugation (circular maps of type II) conserve (1).

**3.2.** If left part of (1) and five points are fixed, then the sixth point (probably infinite) is defined uniquely from linear equation.

#### 3.3.

a) Let  $ABA'B'$  be regular, i.e.  $\varphi = \varphi_{ABA'B'}$  is inversion+reflection. Take complex coordinates in such a way that  $\varphi(z) = 1/z$ , so  $A(a)$ ,  $A'(1/a)$ ,  $B(b)$ ,  $B'(1/b)$ ,  $C(c)$ . Take  $C''(1/c)$ . By immediate check of (1) we obtain that  $(A, A'; B, B'; C, C'')$  is harmonic. This and the previous problem yield the required.

If  $ABA'B'$  is central symmetric, i.e.  $\varphi = \varphi_{ABA'B'}$  is central symmetry, take such coordinates that  $\varphi(z) = -z$  and repeat the reasoning.

b) Follows from the previous: we have  $\varphi_{ACA'C'} = \varphi_{ABA'B'}$  and  $\varphi_{ADA'D'} = \varphi_{ABA'B'}$ , hence  $\varphi_{ACA'C'} = \varphi_{ADA'D'}$ , and  $(A, A'; C, C'; D, D')$  is harmonic.

**3.4.** The angle  $\angle(AB, AC) - \angle(A'B, A'C)$  equals to (directed) angle between the circles  $(ABC)$  and  $(A'BC)$ . Since  $\varphi$  conserve the angles between circles, it equals the angle between  $(AB'C')$  and  $(A'B'C')$ , or  $\angle(A'B', A'C') - \angle(AB', AC')$ .

*Remark.* This (and similar) equality can be transformed to different forms, for example

$$\angle(BA, BA') + \angle(B'A, B'A') = \angle(CA, CA') + \angle(C'A, C'A').$$

If  $M$  the center of inversion+reflection  $\varphi$ , then  $\angle(BA, BA') + \angle(B'A, B'A')$  may be transformed to  $(\angle(BA, AM) + \angle(AM, A'M) + \angle(A'M, BA')) + (\angle(B'A, B'M) + \angle(B'M, B'A')) = \angle(AM, A'M) + (\angle(BA, AM) + \angle(B'M, B'A')) + (\angle(A'M, BA') + \angle(B'A, B'M)) = \angle(AM, A'M) + 0 + 0$ . Similarly  $\angle(CA, CA') + \angle(C'A, C'A')$

So if  $A, A' = \varphi(A)$  are fixed, then the sum

$$\angle(XA, XA') + \angle(X'A, X'A')$$

does not depend on the pair  $X, X' = \varphi(X)$ .

The last fact can be generated: the sum

$$\angle(XA, XB) + \angle(X'B', X'A')$$

does not depend on  $X, X' = \varphi(X)$  (if  $A, A' = \varphi(A)$ ,  $B, B' = \varphi(B)$  are fixed). This sum equals to  $\angle(MA, MB)$  — the proof is similar.

## Harmonicity and products of similitudes

### 3.5.

- a) Follows from the equalities of modulus and arguments of complex numbers in (1).
- b) The coefficients of rotational homotheties equal to modulus of fractions in the left part of (1), and the angles of rotations are opposite to their arguments.
- c) Since  $(A, A'; B, B'; C, C')$  is harmonic,  $(C, C'; A', A; B, B')$  is also harmonic, which yields  $(L - C'AB')$ .
- d) Let  $A'$  and  $B'$  be two centers of rotational homotheties. Then the angles of triangle  $A'B'C'$  are known (for example from general Napoleon theorem).
- e) to be added

### 3.6.

The assumptions  $(R - \dots)$  yield that the circles concur.

If all six points are concyclic, the assumptions  $(L - \dots)$  with  $(R - \dots)$  giving the appropriate order of points, yield that the circles concur.

### 3.7.

- a) It is easy to see that an isogonal sextet satisfies the assumptions  $(R - \dots)$ , which yield the concurrence (see the previous problem).
- b) Five points  $A, B, B', C, C'$  define unique isogonal sextet  $(A, A'; B, B'; C, C'')$  (the lines  $BA$  and  $B'A$  are defined from  $Isog_B(AA', CC')$ ,  $Isog_{B'}(AA', CC'')$ ). From the previous  $(A, A'; B, B'; C, C'')$  is harmonic and by problem 3.2 we obtain  $C'' = C'$ .  
The problem can also be solved in complex coordinates (see for example the following).
- c) Take such complex coordinates that  $A, A'; B, B'; C, C'$  correspond to  $a, 1/a, b, 1/b, c, 1/c$ . Then we can write  $Isog_A(BB', CC')$  (equivalent to the required by the previous) as  $\frac{1/c-a}{1/b-a} \cdot \frac{c-a}{b-a} \in \mathbb{R}$ , or  $\frac{1-a/c-ac+a^2}{1-a/b-ab+a^2} \in \mathbb{R} \Leftrightarrow \frac{1/a+a-1/c-c}{1/a+a-1/b-b} \in \mathbb{R}$ . but the last is equivalent to the collinearity of midpoints  $\frac{a+1/a}{2}, \dots$  of segments  $AA', \dots$ .

## 4 Information about cubics

### 4.1.

a) Let  $U, V$  be the third common points of the cubic with lines  $AB, BC$  respectively. Then  $P = A + B$  and  $Q = B + C$  are the third common points of the cubic with  $OU, OV$  respectively and we have to prove that the common point of lines  $CP$  and  $AQ$  lies on the cubic. Consider two degenerated cubics: one of them is the union of lines  $ABU, OVQ, CP$ , and the second one is the union of lines  $BCV, OUP, AQ$ . The given cubic passes through eight of their common points:  $A, B, C, O, U, V, P, Q$ ; Therefore it passes also through the remaining point.

b) Let  $OA$  meet the cubic for the third time at  $C$ . Then  $A - B$  is the third common point of the cubic with  $BC$ .

**4.2.** Denote  $A +' B = C$ . Then  $O' + C = A + B$ , i.e.  $C = A + B - O'$ .

### 4.3.

a) By the definition  $A + B + C$  is the third common point of the cubic and the line touching it at  $O$ .

b) If  $O$  is a suflexion point, then  $A + B + C = O$ . It is easy to see that for any  $P$   $P + O = P$ .

### 4.4.

a) Clearly follows from  $s_P s_P(X) = X$ .

b) By the previous problem  $P + X + s_P(X) = P' + s_P(X) + s_{P'} s_P(X)$ , i.e.  $s_P s_P(X) = X + P - P'$ . Then the commutativity is equivalent to  $P - P' = P' - P$  or  $2P = 2P'$ . But the last equality means that the tangents at  $P$  and  $P'$  meet the cubic in the same point.

### 4.5.

a) There exist three tangents to the cubic from the suflexion point  $O$  distinct from the tangent at  $O$ . The bases of these tangents are the points of degree 2.

b) Clearly follows from the previous problem.

**4.6.** Let  $A_1 + \dots + A_6 = 0$ . Find the third common points of the cubic with lines  $A_1A_2, A_3A_4, A_5A_6$ . The sum of these three points also equals to zero, therefore they are collinear, denote the corresponding line as  $\ell$ . Consider two degenerated cubics: the union of lines  $A_1A_2, A_3A_4, A_5A_6$  and the union of  $\ell$  with the conic passing through  $A_1, \dots, A_5$ . Eight of their common points lie on  $\mathcal{C}$ , thus the remaining point also lies on  $\mathcal{C}$ , i.e. coincides with  $A_6$ .

Inversely let  $A_1, \dots, A_6$  lie on a conic. Find the third common points  $B, C$  of  $\mathcal{C}$  with  $A_1A_2, A_3A_4$  respectively. The cubic which is the union of conic  $A_1 \dots A_6$  and line  $BC$  passes through eight common points of  $\mathcal{C}$  with the union of lines  $A_1A_2, A_3A_4, A_5A_6$ , thus  $BC$  and  $A_5A_6$  meet on  $\mathcal{C}$  which yields the required equality.

### 4.7.

a) By the previous problem  $X + Y$  does not depend on  $X$ .

b) Similarly  $Z + T$  does not depend on  $X$ .

## Circular cubics

**4.8.** Follows from right calculation.

**4.9.** Follows from  $A' + B' = A + B$ .

**4.10.**

a) The sum  $X + Y + Z + T$  depends only from  $P, Q$ . Hence if these points lie on a conic with two circular points for some section lines this is true for any section lines.

b) The line  $PQ$  is parallel to the asymptote if and only if  $P + Q$  equals to the sum of the circular points. Since  $P, Q, X, Y, Z, T$  lie on a (degenerated) conic, this means that  $X, Y, Z, T$  are concyclic.

## 5 Кубика фокусов

### Properties of cubics of foci

#### 5.1.

a)

Since  $\angle(AX, XB) = \angle(AY, YB)$  and  $\angle(A'X, XB') = \angle(A'Y, YB')$ , the assumptions  $Isog_X(AA', BB')$  and  $Isog_Y(AA', BB')$  are equivalent.

(Using that  $ISO(ABA'B')$  is an isocircular cubic): Let  $Y'$  be the sixth common point of the cubic with the circle  $(ABX)$ . Then  $Y' = -A - B - X - C_1 - C_2$ . Similarly for the sixth common point  $Y''$  of the cubic and the circle  $(A'B'X)$ . Since  $A' + B' = A + B$  (because  $A' = A + C$ ,  $B' = B + C$ , where  $C + C = O$ ), we obtain that  $Y' = Y''$ .

b)

(Using that  $ISO(ABA'B')$  is an isocircular cubic): The third common point of  $XY$  and the cubic is constant because  $X + Y = -A - B - C_1 - C_2 = const$ .

#### 5.2.

Follows from 3.7.

#### 5.3.

Follows from the equation (problem 4.15)

#### 5.4.

a)

b) By the description of  $ISO$  as the set of such  $X$  that the midpoints of  $AA'$ ,  $BB'$ , and  $XX'$  are collinear.

c) Because  $M$  is the center of rotational homothety mapping  $\vec{AB}$  to  $\vec{B'A'}$ .

d) The quadruple  $A, E = AA' \cap BB', A', AA' \cap PP'$  is harmonic, thus the quadruple of lines joining these points with the projection  $F$  of  $E$  to  $PP'$  is also harmonic. Since  $FE \perp PP'$ , we obtain that  $FA$  and  $FA'$  are isogonal with respect to  $FE$ . From the same reasoning for  $FB$  and  $FB'$  we obtain  $Isog_F(AA', BB')$ .

e) The assumption  $Isog_T(AA', BB')$  clearly follows from the definition.

5.5. By the definition of isocircular involutions  $P, M, P', \infty$  is an orbit.

Points  $T$  and  $T'$  are conjugated (see below).

#### 5.6.

a) Follows from the equation.

b) Follows from the equation because  $\infty$  and  $M$  are conjugated.

c) Since  $s_M(X) = s_\infty(X')$ , and the midpoint of  $XX'$  lies on the Gauss line.

#### 5.7.

a) (S.Berlov) Synthetic solution see in S.Berlov, F.Petrov. Solution of problem M2497. Kvant, 2018, 4, 13–15.

b) Follows from the orbit containing  $\infty$ .

5.8. Follows for example from problem 3.7.

5.9. Consider two pairs of conjugate points  $X, X'$  and  $Y, Y'$ . By the isogonals theorem points  $XY \cap X'Y'$  and  $XY' \cap X'Y$  are also isogonally conjugated, i.e. they

lie on the cubic. therefore  $X + Y = X' + Y'$  and  $X + Y' = X' + Y$  or  $X - X' = Y - Y' = Y' - Y$ .

**5.10.** (\*Cyclic\*) ?? If  $ABA'B'$  is cyclic the map  $f_{AB,A'B'}$  coincide with the inversion mapping  $A$  to  $B$ , and mapping  $A'$  to  $B'$ . This inversion is centered at the common point  $P$  of lines  $AB, A'B', XY, X'Y'$ , also we have  $\angle APX = \angle Y'PA'$ . Let  $X_1$  be the reflection of  $X$  about  $PA$  and  $Y'_1$  be the reflection of  $Y'$  about  $PA'$ . Then the similarity of triangles  $PXX'$  and  $PY'Y$  yields the equality  $X'X_1 : XX' = YY'_1 : YY'$  equivalent to the required.

**5.11.** (\*Harmonic\*) ??

a) Since  $AA'$  is a symmedian of triangles  $ABB'$ ,  $A'BB'$  and  $BB'$  is a symmedian of  $ABA'$ ,  $AB'A'$  we obtain that  $M_A$  and  $M_B$  are conjugated.

**5.12.** (\*Parallelogram\*)

a) This assumption is necessary, it is equivalent to  $isog_B(AA', XX')$  because by the symmetry  $\angle(A'X, A'B) = \angle(AX', AB')$ . By problem 3.7 this is sufficient for all remaining isogonality assumptions

b) It is easy to see that if two circles are congruent then two remaining circles have the same radius. Also if the circles  $XAB$  and  $XA'B'$  then the angles  $(XA, XB)$  and  $(XB', XA')$  corresponding to equal chords are congruent too.

c) When we change the radii of congruent circles  $ABX$  and  $A'BX$  the lines  $AX$  and  $A'X$  rotate with equal velocities in opposite directions. Hence their common point moves on an equilateral hyperbola.

**5.13.**

a) The inversion about the incircle maps  $AB, AB', A'B, A'B'$  to four congruent circles, therefore their common points form a parallelogram. Thus the circles  $ABI, A'B'I$  are tangent, and the circles  $AB'I, A'BI$  are tangent.

b)

c) Let  $T_1, T_2, T_3, T_4$  be the touching points of the incircle with  $AB, AB', A'B, A'B'$ . The midpoints of segments  $T_iT_j$ , the common points of diagonals and opposite sidelines of  $T_1T_2T_3T_4$  and the incenter  $I$  lie on an equilateral hyperbola, and the inversion images of these points lie on the cubic of foci.

**5.14.**

a) We have  $A + A' = B + B'$ , i.e.  $A + A = B + B$ . Thus the tangents to the cubic at  $A, B, A', B'$  meet it for the third time at the same point.

## Another descriptions of cubics of foci

**5.15.** Firstly find an equation for the case when  $\varphi$  with the complex conjugation:  $(x, y) \mapsto (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$ . using that the midpoints of segment  $XX'$  lie on the Gauss line  $2Ax + 2By = 1$  we obtain  $(Ax + By + 1)(x^2 + y^2) + Ax - By = 0$ . Now using the rotation mapping the Gauss line to a vertical line we obtain the required.

**5.16.**

a) Take such coordinate system that the infinite non-circular point of the cubic lie on the ordinate axis. Then the equation of the cubic is  $(x^2+y^2)(x+A) = Bx+Cy+D$ . It is easy to see that the tangents at the circular points pass through the origin.

b)  $M$  and  $M' = \infty$  (asymptote point) are conjugated, hence, the point  $O'_1 = O_2$  conjugated to circular point  $O_1$  is the result of projections from  $M'$  and  $M$ . But  $s_{M'}(O_1) = O_2$ , hence  $s_M(O_1) = O_2$ .

**5.17.**

a) By immediate check we obtain that the locus of  $X, Y$  is a cubic. This cubic coincides with  $\mathcal{C}$  because it passes through  $M, L, L'$  and the circular points and the tangents to it at  $L, L'$  and circular points pass through  $M$ .

b) The sum  $X + Y$  does not depend on the circle.

**5.18.** Follows from the equation of  $ISO(ABA'B')$ .

## 6 Quartets and isogonal cubics

### 6.1.

a) Let the barycentric coordinates of  $J$  and  $P$  be  $(x_0 : y_0 : z_0)$  and  $(x : y : z)$  respectively. Then the barycentric coordinates of  $P'$  are  $(a^2yz : b^2zx : c^2xy)$ , where  $a, b, c$  are the lengths of  $YZ, ZX, XY$  respectively and the collinearity of  $J, P, P'$  yields the equation of degree 3 about  $x, y, z$ .

b) Since the isogonal conjugation maps the infinite line to the circumcircle the circular points are conjugated.

**6.2.** Let  $P_1 = \varphi_X(P)$ ,  $P_2 = \varphi_Y(P_1)$ . Since  $XZ \cdot XY = XP \cdot XP_1$  and  $\angle ZXP = \angle P_1XY$ , the triangles  $XPZ$  and  $XYP_1$  similar. The triangles  $XYP_1$  and  $P_2YZ$  are also similar, thus  $P_2 = \varphi_Z(P)$ . Hence the composition of any two maps from  $\varphi_X, \varphi_Y, \varphi_Z$  is equal to the third map.

Let point  $Q$  be isogonally conjugated to  $P$ ,  $Q_1 = \varphi_X(Q)$ . Then  $X, P, Q_1$  are collinear and  $X, Q, P_1$  are collinear. Also  $\angle XYP_1 + \angle XYQ_1 = \angle XPZ + \angle XQZ + \pi + \angle Y$ , therefore the lines  $YQ_1$  and  $YP_1$  are symmetric with respect to the bisector of angle  $Y$  and  $P_1, Q_1$  are isogonally conjugated (fig. 6.1).

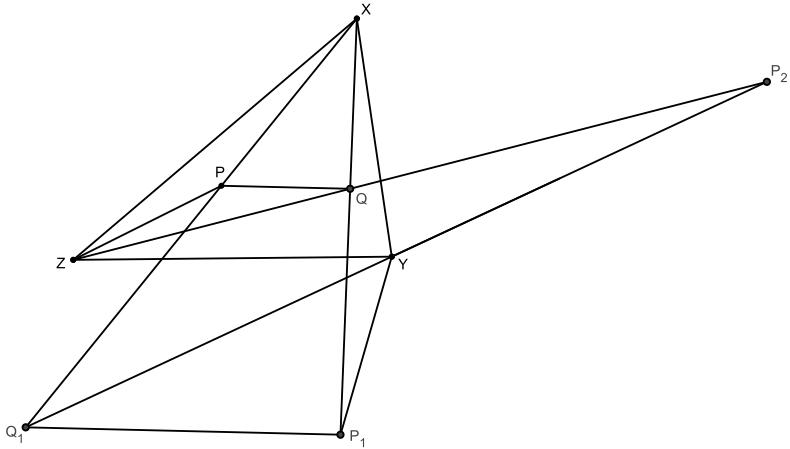


Fig. 6.1.

**Remarks.** 1. The commutation of  $\varphi_X$  with the isogonal conjugation can also be proved by the following way. Applying to  $P$  in an arbitrary order the isogonal conjugation and  $\varphi_x$  we obtain a point on  $XP$ . It is easy to see that both compositions are projective maps of this line, hence it is sufficient to prove that they coincide for three positions of  $P$ . But both compositions transpose  $X$  and the common point of  $XP$  with the circumcircle of  $XYZ$ , also they transpose the infinite point and the common point of  $XP$  with  $YZ$ .

2. The equality  $XP \cdot XP_1 = XQ \cdot XQ_1$  yields also  $PQ \parallel P_1Q_1$ .

### 6.3.

a) Follows from the previous problem.

b) Follows from remark 2 to the previous problem.

c) By the previous assertion these points lie on the cubic defined by infinite point of lines  $AA'$ ,  $BB'$ ,  $CC'$ ,  $DD'$ .

d) From the equalities  $A + D + X = A + C + Y = B + C + X = B + D + Y$  we obtain  $A + A = B + B$ .

#### 6.4.

a) From  $A + D' = B + C'$ ,  $D + D' = C + C'$  and  $D' + D' = C' + C'$  we obtain that  $A + D = B + C$ , i.e.  $P_X$  lies on the cubic. Similarly  $P_Y$ ,  $P_Z$ ,  $Q_X$ ,  $Q_Y$ ,  $Q_Z$  lie on the cubic. Then from  $A + D + P_X = A' + D' + Q_X = B + D + P_Y = B' + D' + Q_Y$  we obtain  $A + A' + P_X + Q_X = B + B' + P_Y + Q_Y$ . Since  $A + A' = B + B' = \infty$  (infinite point of the cubic) this yields that  $P_XQ_X$  and  $P_YQ_Y$  meet the cubic at the same point. This point is conjugated to the infinite one, thus it lies on the circumcircle. The line  $P_ZQ_Z$  also passes through this point.

b) From  $A + D + P_X = A' + D' + Q_X = B + D + P_Y = B' + D' + Q_Y = A + D' + X = B' + D + Y$  we obtain  $X + Y = P_X + Q_Y = P_Y + Q_X$ .

c) The common point  $Z'$  of the cubic and  $XY$  is conjugated to  $Z$ , therefore  $ZZ'$  passes through  $\infty$ .

**6.5.** The quartets  $A_1, B_1, C_1, D_1$  and  $A_2, B_2, C_2, D_2$  generate the same cubic. Also  $A_1 - B_1$  and  $A_2 - B_2$  is the same point of degree 2. Therefore,  $A_1 + A_2 = B_1 + B_2 = 2$ , i.e.  $A_1A_2$  and  $B_1B_2$  meet the cubic at the same point.

**6.6.** Since  $X, Y, Z, \infty$  is a quartet, the tangents at these points meet the cubic at the same point. This point is conjugated to the infinite one, thus it lies on the circumcircle.

All cubics of quartets pass through  $X, Y, Z$ , the incenter  $I$ , the excenters  $I_X, I_Y, I_Z$ , and the circular points. Hence these cubics form a pencil. The locus of common points of tangents to the cubics of this pencil at circular points is a conic because the correspondence between the tangent is projective. Consider a degenerated cubic which is the union of the bisector  $I_XI_Y$  of angle  $Z$  and the circle  $XYII_Z$ . The tangents to it at circular points meet at the center of this circle — the midpoint of arc  $XY$ . The cubic meets the circumcircle at the opposite point — the midpoint of arc  $XZY$ . Similarly the tangents at circular points meet at the point of the circumcircle opposite to its common point with the cubic for five other degenerated cubics of the pencil. Therefore this is correct for all cubics.

**6.7.** The tangents to a cubic of foci at circular points meet on the cubic. By the previous problem we obtain that the fourth common point of the cubic and the circumcircle is opposite to one of the vertices. The infinite point is conjugated to this point, thus it lies on an altitude of the triangle.

**Remark.** Let the infinite point of the cubic lie on the altitude from  $Z$ ; let  $A, B, C, D$  be an arbitrary quartet. Then the cubic is the cubic of foci for lines  $AC, BC, AD, CD$ . The vertex  $Z$  is the Mickel point of these lines, and the perpendicular bisector to segment  $XY$  is their Gauss line.

**6.8.** Let  $U$  be the common point of tangents to the cubic at  $X, Y, Z$ , and  $J$ . Form  $X + X + U = Y + Y + U = Z + Z + U = J + J + U = J_1 + J_2 + J = 0$ , where  $J_1, J_2$  are circular points we obtain that  $J_1 + J_2 + X + Y + Z + U = 0$ , i.e.  $U$  lies on the circle  $XYZ$ . Consider the cubic of quartets passing through  $U$ . It coincide with the given cubic because both cubics pass through  $X, Y, Z, U, J, J_1, J_2$ , and

the tangents to them at  $X, Y, Z$  coincide.

## Once more about 8-orbits

**6.9. Hint.** Let the inversion with center  $T$  map  $X, Y, Z$  to  $X', Y', Z'$  respectively. Then it maps a 8-orbit to two quartets isogonally conjugated with respect to  $X'Y'Z'$ .

If  $T, X, Y, Z$  are concyclic we can also consider an inversion mapping these points to the vertices of a rectangle. Then the map  $g_{T,X,Y,Z}$  corresponds to the inversion about the circumcircle of this rectangle.