

# Дистанционные графы и теорема Турана

А. М. Райгородский

Задачу представляют Л. Неустроева, А.М. Райгородский, О. В. Бурсиан, К. П. Кохась

## 1 Базовые определения

Пусть  $G = (V, E)$  — граф без петель, кратных ребер и ориентации. Назовем *кликой* в этом графе любой его полный подграф. Одна вершина и одно ребро — это тоже клики. Назовем, далее, *кликовым числом* графа  $G$  величину  $\omega(G)$ , равную максимальному такому  $k$ , что в графе  $G$  есть клика на  $k$  вершинах. В то же время назовем *независимым множеством* такое множество вершин графа  $G$ , что ни одна пара вершин в нем не образует ребра. В своем роде это “антиклика”. Одна вершина является не только кликой, но и независимым множеством вершин. Соответственно, *число независимости* графа  $G$  — это максимальное  $k$ , при котором в  $G$  есть независимое множество вершин мощности  $k$ . Обозначается это число  $\alpha(G)$ . Наконец, *хроматическое число* графа  $G$  — это минимальное число  $\chi(G)$  цветов, в которые можно так покрасить все вершины графа, чтобы концы каждого ребра имели разные цвета.

## 2 Задачи до промежуточного финиша

### 2.1 Простые упражнения

**Задача 1.** Докажите, что  $\chi(G) \geq \omega(G)$ .

**Задача 2.** Докажите, что  $\chi(G) \geq \frac{|V|}{\alpha(G)}$ .

**Задача 3.** Пусть  $\Delta(G)$  — максимальная степень вершины графа  $G$ . Докажите, что  $\chi(G) \leq \Delta(G) + 1$ .

**Теорема Брукса (без доказательства).** Если граф  $G$  связан и не является ни полным графом, ни простым (несамопересекающимся) циклом нечетной длины, то  $\chi(G) \leq \Delta(G)$ .

### 2.2 Теорема Турана

**Задача 4.** Пусть  $G = (V, E)$  и  $|V| = n$ . Докажите, что если  $\omega(G) < 3$  (или, иначе говоря, в графе нет треугольников), то число ребер в  $G$  не больше, чем  $\left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil$ . Докажите также, что эта оценка неумлучшаема.

**Задача 5.** Докажите, что утверждение задачи 4 равносильно следующему: пусть  $G = (V, E)$  и  $|V| = n$ ; если  $\alpha(G) < 3$ , то число ребер в  $G$  не меньше, чем

$$C_n^2 - \left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil,$$

и эта оценка неумлучшаема.

**Задача 6 (теорема Турана).** Пусть  $G = (V, E)$  и  $|V| = n$ . Докажите, что если  $\alpha(G) \leq k$ , то число ребер в  $G$  не меньше, чем

$$n \cdot \left\lfloor \frac{n}{k} \right\rfloor - k \cdot \frac{\left\lfloor \frac{n}{k} \right\rfloor \left( \left\lfloor \frac{n}{k} \right\rfloor + 1 \right)}{2},$$

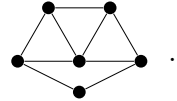
и эта оценка неумлучшаема.

## 2.3 Дистанционные графы на плоскости

Назовем *дистанционным графом на плоскости* (или *графом расстояний на плоскости*) такой граф, вершины которого — это точки плоскости, а ребра — все пары точек, расстояние между которыми равно 1.

**Задача 7.** Докажите, что в дистанционном графе нет подграфов  $K_4$  (полных графов на 4-х вершинах).

**Задача 8.** Докажите, что в дистанционном графе нет подграфов  $K_{2,3}$  (полных двудольных графов с долями размера 2 и 3).

**Задача 9.** Докажите, что в дистанционном графе нет подграфов  $W =$  .

**Задача 10.** Дистанционный граф не стоит путать с планарным графом (графом, который можно так изобразить на плоскости, чтобы ребра на рисунке пересекались только по вершинам). Приведите пример непланарного графа расстояний и планарного графа, не являющегося дистанционным. (Критерий Куратовского можно использовать без доказательства. Я его напому.)

## 2.4 Теорема Турана для дистанционных графов на плоскости

**Задача 11.** Пусть в дистанционном графе  $G = (V, E)$  на плоскости  $4n$  вершин, а  $\alpha(G) \leq n$ . Согласно теореме Турана  $|E| \geq 6n$ . Докажите, что в текущем случае (когда граф  $G$  дистанционный) имеет место более сильная оценка  $|E| \geq 7n$ . Воспользуйтесь результатом задачи 7.

Дальнейшая серия задач посвящена уточнению результата задачи 11. При этом по-прежнему мы используем только задачу 7.

**Задача 12.** Докажите, что если у графа  $G = (V, E)$  (не обязательно дистанционного!)  $4n$  вершин,  $\alpha(G) \leq n$ ,  $\omega(G) \leq 3$  (граф не содержит  $K_4$ ) и *минимальная* степень вершины  $G$  не больше трех, то из графа можно так удалить не более четырех вершин со всеми примыкающими к ним ребрами, чтобы в новом графе  $G' = (V', E')$  было  $\alpha(G') \leq \alpha(G) - 1$ ,  $|E'| \leq |E| - 8$  (удалив не более четырех вершин, избавимся от не менее восьми ребер).

Для решения задачи 12 можно действовать так. Пусть  $A$  — вершина минимальной степени в  $G$ . Рассмотрите по отдельности все 4 случая значения степени от 0 до 3. В первых трех случаях удаляйте вершину  $A$  со всеми соседями и используйте задачу 2 в сочетании с теоремой Брукса для доказательства существования вершины большой степени в остающемся графе. В последнем случае проведите небольшой перебор возможных ситуаций.

**Задача 13.** С помощью индукции выведите из задачи 12 оценку  $|E| \geq 8n$  в условиях задачи 11.

**Задача 14.** Докажите, что для графов (не обязательно дистанционных!), у которых  $4n$  вершин,  $\alpha(G) \leq n$  и  $\omega(G) \leq 3$ , оценка  $|E| \geq 8n$  неулучшаема.

И еще большие усиления за счет дополнительных “запрещенных” подграфов.

**Задача 15\*.** С помощью результатов задач 7, 8 и 9 докажите, что если у дистанционного графа на плоскости  $4n$  вершин и  $\alpha(G) \leq n$ , то  $|E| \geq \frac{26}{3}n$ .

**Задача 16 (открытая проблема).** Улучшите оценку задачи 15.

## 2.5 Дистанционные графы в пространствах большей размерности

Если Вы знаете, что такое  $n$ -мерное пространство, обозначаемое традиционно  $\mathbb{R}^n$ , то Вы молодец, но прямо сейчас это знание не является обязательным. Позже мы дадим определения, достаточные для решения соответствующих задач. Однако пока можно обойтись без слова “пространство”. Рассмотрим граф  $G(n, 3, 1)$ . Его вершинами служат все возможные  $C_n^3$  трехэлементные подмножества множества  $\{1, 2, \dots, n\}$ . А ребрами в нем соединяются те и только те вершины, которым отвечают трехэлементные подмножества, пересекающиеся ровно по одному элементу. На рисунке 2 изображен пример графа  $G(5, 3, 1)$ .

**Задача 17.** Найдите число ребер в графе  $G(n, 3, 1)$ .

**Задача 18.** Найдите число треугольников в графе  $G(n, 3, 1)$ .

**Задача 19.** Докажите, что  $\alpha(G(n, 3, 1)) = n, n - 1$  или  $n - 2$  в зависимости от величины остатка от деления числа  $n$  на 4.

**Задача 20.** Найдите  $\omega(G(n, 3, 1))$ .

**Задача 21\*.** Докажите, что если  $n = 2^k$ , то  $\chi(G) = \frac{|V|}{\alpha(G)} = \frac{(n-1)(n-2)}{6}$ .

Напомним, что две функции  $f$  и  $g$  натурального аргумента  $n$ , не принимающие нулевых значений, называются *асимптотически равными* (или *эквивалентными*), если  $\frac{f(n)}{g(n)} \rightarrow 1$  при  $n \rightarrow \infty$ . Например, асимптотически равны функции  $n^4$  и  $n^4 + 100n^2$ . Пишут  $f \sim g$ . Далее, функция  $f$  *бесконечно мала* по сравнению с  $g$ , если  $\frac{f(n)}{g(n)} \rightarrow 0$  при  $n \rightarrow \infty$ . В этом случае пишут  $f = o(g)$ . Например,  $n^3 = o(n^4)$ .

**Задача 22.** Пусть  $W_n$  — произвольное подмножество множества вершин графа  $G(n, 3, 1)$  (для каждого  $n$  рассматриваем свое множество  $W_n$ ). Обозначим  $r(W_n)$  число ребер, оба конца которых принадлежат  $W_n$ . Пусть  $n = o(|W_n|)$  при  $n \rightarrow \infty$ . Докажите, что обычная теорема Турана гарантирует тогда, что  $r(W_n) \geq f(n)$ , где  $f$  — некоторая функция, асимптотически равная величине  $\frac{|W_n|^2}{2\alpha(G(n, 3, 1))} \sim \frac{|W_n|^2}{2n}$ .

Вот теперь дадим формальное определение пространства  $\mathbb{R}^n$ . Это просто множество всех “точек”  $\mathbf{x}$ , каждая из которых есть последовательность, состоящая из  $n$  действительных чисел:  $\mathbf{x} = (x_1, \dots, x_n)$ . При этом между любыми двумя точками  $\mathbf{x} = (x_1, \dots, x_n)$  и  $\mathbf{y} = (y_1, \dots, y_n)$  можно померить расстояние по формуле

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

В частности, при  $n = 1$  получаем обычную прямую, при  $n = 2$  — обычную плоскость, при  $n = 3$  — обычное пространство.

Далее, скалярное произведение векторов  $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n)$  в  $\mathbb{R}^n$  — это выражение

$$(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \dots + x_n y_n.$$

Нетрудно проверить, что всегда

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}).$$

**Задача 23.** Докажите, что граф  $G(n, 3, 1)$  изоморфен следующему графу в  $\mathbb{R}^n$ :

$$V = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = 3\}, \quad E = \{(\mathbf{x}, \mathbf{y}) : (\mathbf{x}, \mathbf{y}) = 1\}.$$

Таким образом, этот граф дистанционный, т.е. его вершины — точки в пространстве, а ребра — пары точек на заданном наперед расстоянии.

**Задача 24.** Пусть  $K_{l_1, \dots, l_r}$  — полный  $r$ -дольный граф с размерами долей  $l_1, \dots, l_r$ . Докажите, что дистанционный граф в  $\mathbb{R}^n$  не содержит в качестве подграфа граф  $K_{3, \dots, 3}$  с числом долей  $[n/2] + 1$ .

### 3 Задачи после промежуточного финиша

**Задача 25.** Докажите, что если в условиях задачи 22 дополнительно потребовать выполнение условия  $|W_n| = o(n^2)$ , то оценка из задачи 22 (т.е. обычная турановская оценка) асимптотически неулучшаема. Иными словами, для любой функции  $g$ , удовлетворяющей условиям  $g(n) = o(n^2)$  и  $h = o(g(n))$  при  $n \rightarrow +\infty$ , существует последовательность  $W_n$ , такая что  $|W_n| \sim g(n)$  и  $r(W_n) \sim \frac{|W_n|^2}{2n}$ .

**Задача 26-27.** Назовем *вершинами правильного симплекса* в  $\mathbb{R}^n$  любой набор из  $k$  точек, попарные расстояния между которыми равны 1. Докажите, что такие множества существуют при всех  $k \leq n+1$  (задача 26) и не существуют ни при каких  $k \geq n+2$  (задача 27).

**Задача 28.** Пусть  $G_n = (V_n, E_n)$ ,  $n = 1, 2, \dots$ , — дистанционные графы в  $\mathbb{R}^n$ . Обозначим их числа независимости  $\alpha_n$ . Пусть  $W_n$  — произвольное подмножество множества вершин графа  $G_n$  (как обычно, для каждого  $n$  рассматриваем свое множество  $W_n$ ). Обозначим  $r(W_n)$  число ребер, оба конца которых принадлежат  $W_n$ . Пусть  $n\alpha_n = o(|W_n|)$  при  $n \rightarrow \infty$ . С помощью задачи 26-27 докажите, что  $r(W_n) \geq f(n)$ , где  $f$  — некоторая функция, асимптотически равная величине  $\frac{|W_n|^2}{\alpha_n}$ .

Применив утверждение задачи 28 к последовательности графов  $G_n = G(n, 3, 1)$  мы получим оценку примерно в 2 раза лучше, чем в задачах 22 и 25 (вдвое лучшая турановской). Здесь нет противоречия, потому что в этих задачах сформулированы разные (практически противоположные) требования к числу вершин  $|W_n|$ :  $|W_n| = o(n^2)$  в задаче 25 и (проверьте!)  $n^2 = o(|W_n|)$  в задаче 28. Оказывается, для графов  $G(n, 3, 1)$ , как ни странно, можно получить еще более сильные оценки турановского типа, временно отказавшись от использования в них числа независимости. Идея состоит в том, чтобы посмотреть вершины, содержащие тот или иной элемент множества  $\{1, \dots, n\}$ , оценить соответствующие количества ребер и воспользоваться некоторыми стандартными неравенствами.

**Задача 29.** Пусть  $W_n$  — произвольное подмножество множества вершин графа  $G(n, 3, 1)$ . Пусть  $n^2 = o(|W_n|)$  при  $n \rightarrow \infty$ . Докажите, что  $r(W_n) \geq f(n)$ , где  $f$  — некоторая функция, асимптотически равная величине  $4.5 \cdot \frac{|W_n|^2}{n}$ . Иными словами, получается примерно в 4.5 раза лучшая оценка, чем в задаче 28!

**Задача 30.** Докажите, что оценка из задачи 29 в стандартном смысле асимптотически неулучшаема.

Само обозначение “ $G(n, 3, 1)$ ” подсказывает, что у этого графа есть обобщение. Это граф  $G(n, r, s)$ . У него вершинами служат все  $r$ -элементные подмножества множества  $\{1, \dots, n\}$ , а ребрами соединяются две вершины, если и только если соответствующие множества пересекаются ровно по  $s$  элементам. Иными словами, вершины —  $n$ -мерные точки с “координатами” 0 или 1, причем в каждой точке ровно  $r$  единиц. Ребро проводится тогда и только тогда, когда скалярное произведение вершин равно  $s$ . Графы  $G(n, r, s)$  называются *графами Джонсона*, а их частный случай — графы  $G(n, r, 0)$  — называются *кнезеровскими графами*.

**Задача 31.** Найдите число ребер в графе  $G(n, r, s)$ .

**Задача 32.** Найдите число треугольников в графе  $G(n, r, s)$ .

**Задача 33\*.** Докажите, что аналогом результатов из задач 29 и 30 служит асимптотически неулучшаемая оценка величиной  $\frac{|W_n|^2}{n^s} \cdot \frac{C_r^s \cdot r!}{2 \cdot (r-s)!}$ . Здесь надо требовать, чтобы  $n^{r-1} = o(|W_n|)$ .

Следующий результат можно использовать без доказательства.

**Теорема Эрдеша, Ко и Радо.** Пусть  $n \geq 2r$ . Тогда  $\alpha(G(n, r, 0)) = C_{n-1}^{r-1}$ .

**Задача 34.** Докажите, что если  $W_n$  — произвольное подмножество множества вершин графа  $G(n, r, 0)$  и  $l = |W_n| > \alpha(G(n, r, 0))$ , то

$$r(W_n) \geq \frac{l(l - (C_n^r - C_{n-r}^r))}{2}.$$

# Distance graphs and Turán's theorem

A. Raigorodsky

The project is proposed by O. Bursian, K. Kokhas, L. Neustroeva, A. Raigorodsky

## 1 Definitions

Let  $G = (V, E)$  be a graph without loops, multiple edges and orientation. A *clique* in  $G$  is any complete subgraph. Single vertex or single edge are also cliques. *The clique number* of graph  $G$  denoted by  $\omega(G)$  is the maximal integer  $k$  such that  $G$  contains a clique on  $k$  vertices. An *independent set* is a set of vertices in  $G$  such that no two of the vertices form an edge. It is an “anticlique” in a sense. Single vertex is not only a clique but an independent set too. Accordingly, *an independence number* of graph  $G$  is the maximal integer  $k$  such that  $G$  contains an independent set of  $k$  vertices. It is denoted by  $\alpha(G)$ . And finally, *the chromatic number* of graph  $G$  is the minimal number  $\chi(G)$  of colors for which one can color vertices of graph in these colors so that the endpoints of any edge have different colors.

## 2 Problems, I

### 2.1 Exercises

**Problem 1.** Prove that  $\chi(G) \geq \omega(G)$ .

**Problem 2.** Prove that  $\chi(G) \geq \frac{|V|}{\alpha(G)}$ .

**Problem 3.** Let  $\Delta(G)$  be the maximum degree of vertices of graph  $G$ . Prove that  $\chi(G) \leq \Delta(G) + 1$ .

**Brooks' theorem (without proof).** *If connected graph  $G$  is neither a complete graph nor a simple cycle (non self-intersecting) of odd length, then  $\chi(G) \leq \Delta(G)$ .*

### 2.2 Turán's theorem

**Problem 4.** Let  $G = (V, E)$  and  $|V| = n$ . Prove that if  $\omega(G) < 3$  (in other words, the graph does not contain triangles) then the number of edges in  $G$  is at most  $\lfloor \frac{n}{2} \rfloor \cdot \lceil \frac{n}{2} \rceil$ . Prove that this upper bound is sharp (i.e. can not be increased).

**Problem 5.** Prove that problem 4 is equivalent to the following statement. Let  $G = (V, E)$  and  $|V| = n$ . Prove that if  $\alpha(G) < 3$  then the number of edges in  $G$  is at least

$$C_n^2 - \left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil,$$

and this lower bound is sharp.

**Problem 6 (Turán's theorem).** Let  $G = (V, E)$  and  $|V| = n$ . Prove that if  $\alpha(G) \leq k$  then the number of edges in  $G$  is at least

$$n \cdot \left\lfloor \frac{n}{k} \right\rfloor - k \cdot \frac{\left\lfloor \frac{n}{k} \right\rfloor \left( \left\lfloor \frac{n}{k} \right\rfloor + 1 \right)}{2},$$

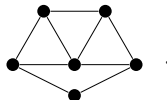
and this lower bound is sharp.

## 2.3 Distance graphs in the plane

A *distance graph on the plane* or *graph of distances on the plane* is a graph such that its vertices are some points of the plane and edges are all pairs of points at distance 1.

**Problem 7.** Prove that distance graphs do not contain subgraphs  $K_4$  (complete graphs on 4 vertices).

**Problem 8.** Prove that distance graphs do not contain subgraphs  $K_{2,3}$  (complete bipartite graphs with parts of 2 and 3 vertices).

**Problem 9.** Prove that distance graphs do not contain subgraphs  $W =$   .

**Problem 10.** Do not confuse distance graphs and planar graphs (the latter can be drawn on the plane in such a way that its edges intersect only at their endpoints). Give examples of non-planar distance graph and planar but non-distance graph. You may use Kuratowski's criterion without proof.

## 2.4 Turán's theorem for distance graphs on the plane

**Problem 11.** Let  $G = (V, E)$  have  $4n$  vertices and  $\alpha(G) \leq n$ . In this case  $|E| \geq 6n$  by Turán's theorem. Prove that if  $G$  is a distance graph on the plane then the stronger inequality  $|E| \geq 7n$  holds. Use the result of problem 7.

Next problems strengthen the inequality of problem 11 by applying the result of problem 7 only.

**Problem 12.** Let graph  $G = (V, E)$  (not necessarily being a distance graph) has  $4n$  vertices. Assume that  $\alpha(G) \leq n$ ,  $\omega(G) \leq 3$  (that means  $G$  does not contain  $K_4$ ) and *minimum* vertex degree in  $G$  is at most 3. Prove that it is possible to remove at most 4 vertices with all its edges from  $G$  in such a way that in the new graph  $G' = (V', E')$  we have  $\alpha(G') \leq \alpha(G) - 1$  and  $|E'| \leq |E| - 8$  (by removing of at most 4 vertices we delete at least 8 edges).

You may use the following approach to problem 12. Let  $A$  be a vertex of minimal degree in  $G$ . The possible values of this degree are from 0 to 3. For the first three values apply problem 2 plus Brooks' theorem in order to prove that the remaining graph has a vertex of big degree. For the last value investigate possible cases.

**Problem 13.** Let  $G = (V, E)$  be a distance graphs on the plane,  $|V| = 4n$  and  $\alpha(G) \leq n$ . Using induction and problem 12 prove that  $|E| \geq 8n$ .

**Problem 14.** Let graph  $G = (V, E)$  (not necessarily being a distance graph) have  $4n$  vertices,  $\alpha(G) \leq n$  and  $\omega(G) \leq 3$ . Prove that the estimation  $|E| \geq 8n$  can not be strengthened.

We can improve the bound better by using additional “forbidden” subgraphs.

**Problem 15\*.** Applying results of problems 7, 8 and 9 prove that if a distance graph has  $4n$  vertices and  $\alpha(G) \leq n$ , then  $|E| \geq \frac{26}{3}n$ .

**Problem 16 (open problem).** Improve the bound of problem 15.

## 2.5 Distance graphs in high-dimensional spaces

If you already know what is  $n$ -dimensional space usually denoted by  $\mathbb{R}^n$ , you are extremely smart, but this knowledge is not obligatory right now. We will give all necessary definitions later. And now we tend to avoid the word “space”. Consider graph  $G(n, 3, 1)$ . Its vertices are all 3-element subsets of the set  $\{1, 2, \dots, n\}$ , so it has  $\binom{n}{3}$  vertices. And the edges correspond to the pairs of subsets which has 1-element intersection. See example of graph  $G(5, 3, 1)$  in fig. 2.

**Problem 17.** Find the number of edges in graph  $G(n, 3, 1)$ .

**Problem 18.** Find the number of triangles in graph  $G(n, 3, 1)$ .

**Problem 19.** Prove that  $\alpha(G(n, 3, 1)) = n, n - 1$  or  $n - 2$  depending on the remainder  $n \bmod 4$ .

**Problem 20.** Find  $\omega(G(n, 3, 1))$ .

**Problem 21\*.** Prove that if  $n = 2^k$ , then  $\chi(G) = \frac{|V|}{\alpha(G)} = \frac{(n-1)(n-2)}{6}$ .

Let  $f$  and  $g$  be two functions defined on the set of non negative integers and having no zero values. We remind that  $f$  and  $g$  are called *asymptotically equal* (or *equivalent*) if  $\frac{f(n)}{g(n)} \rightarrow 1$  for  $n \rightarrow \infty$ . It is written as  $f \sim g$ . For example  $n^4 \sim n^4 + 100n^2$ . Function  $f$  is said to be *infinitesimal* with respect to  $g$  if  $\frac{f(n)}{g(n)} \rightarrow 0$  for  $n \rightarrow \infty$ . It is denoted as  $f = o(g)$ . For example  $n^3 = o(n^4)$ .

**Problem 22.** For each integer  $n \geq 3$  let  $W_n$  be a subset of the set of vertices of graph  $G(n, 3, 1)$ . Denote by  $r(W_n)$  the number of edges with both endpoints in  $W_n$ . Let  $n = o(|W_n|)$  for  $n \rightarrow \infty$ . Prove that Turán’s theorem implies that  $r(W_n) \geq f(n)$ , where  $f$  is a function that is asymptotically equal to  $\frac{|W_n|^2}{2\alpha(G(n, 3, 1))} \sim \frac{|W_n|^2}{2n}$ .

Now we will give a formal definition of the space  $\mathbb{R}^n$ . It is just a set of “points”  $\mathbf{x}$ , where each of points is a sequence of  $n$  real numbers:  $\mathbf{x} = (x_1, \dots, x_n)$ . For any two points  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_n)$  we define a distance between them by formula

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}.$$

In particular, for  $n = 1$  this definition gives us the usual line, for  $n = 2$  the usual plane and for  $n = 3$  the usual space.

Further, the *scalar product* of vectors  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_n)$  in  $\mathbb{R}^n$  is the expression

$$(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \dots + x_n y_n.$$

It easy to check that for all  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}).$$

**Problem 23.** Prove that graph  $G(n, 3, 1)$  is isomorphic to graph  $(V, E)$

$$V = \{\mathbf{x} = (x_1, \dots, x_n) : x_i \in \{0, 1\}, x_1 + \dots + x_n = 3\}, \quad E = \{\{\mathbf{x}, \mathbf{y}\} : (\mathbf{x}, \mathbf{y}) = 1\}.$$

Thus, this is a distance graph in  $\mathbb{R}^n$ : its vertices are points in  $\mathbb{R}^n$ , and edges are the pairs of points at distance 2.

**Problem 24.** Let  $K_{l_1, \dots, l_r}$  be the complete  $r$ -partite graphs, with parts of sizes  $l_1, \dots, l_r$ . Prove that distance graphs in  $\mathbb{R}^n$  do not contain subgraphs of the form  $K_{\underbrace{3, \dots, 3}_{[n/2]+1}}$ .



### 3 Problems after intermediate finish

**Problem 25.** Prove that if in the statement of problem 22 to impose additionally the condition  $|W_n| = o(n^2)$ , then the estimation of problem 22 (i. e. usual Turán's estimation) cannot be asymptotically improved. In other words, for every function  $g$  such that  $g(n) = o(n^2)$ ,  $h = o(g(n))$  there exists sequence  $W_n$  such that  $|W_n| \sim g(n)$  and  $r(W_n) \sim \frac{|W_n|^2}{2n}$ .

**Problem 26-27.** We say that any  $k$  points in  $\mathbb{R}^n$  are the *vertices of right simplex*, if all the pairwise distances between them are equal to 1. Prove such sets exist for all  $k \leq n + 1$  (problem 26) and do not exist for all  $k \geq n + 2$  (problem 27).

**Problem 28.** Let  $G_n = (V_n, E_n)$ ,  $n = 1, 2, \dots$  be unit distance graphs in  $\mathbb{R}^n$ . Denote their independence numbers by  $\alpha_n$ . Let  $W_n$  be an arbitrary subset of the set of vertices of graph  $G_n$  (as usual, for each  $n$  we consider its own set  $W_n$ ). Denote by  $r(W_n)$  the number of the edges, both ends of which belong to  $W_n$ . Let  $n\alpha_n = o(|W_n|)$  as  $n \rightarrow \infty$ . With the help of problem 26-27 prove that  $r(W_n) \geq f(n)$ , where  $f$  is some function asymptotically equal to the value  $\frac{|W_n|^2}{\alpha_n}$ .

For sequence  $G_n = G(n, 3, 1)$  problem 28 give the estimation that is approximately 2 times better than the estimation in problems 22 and 25 (twice better than Turán's estimation). There are no contradiction here, because these problems have different (in fact opposite) limitations for the number of vertices  $|W_n|$ : in problem 25  $|W_n| = o(n^2)$  and in problem 28 (check!)  $n^2 = o(|W_n|)$ . It turns out that for graphs  $G(n, 3, 1)$  even stronger estimations of Turán's kind can be obtained, by temporary refuse of using the independence number. The idea is to consider the vertices containing an element of set  $\{1, \dots, n\}$ , to estimate the corresponding numbers of edges and to apply some standard inequalities.

**Problem 29.** Let  $W_n$  be an arbitrary subset of the set vertices of graph  $G(n, 3, 1)$ . Let  $n^2 = o(|W_n|)$  as  $n \rightarrow \infty$ . Prove that  $r(W_n) \geq f(n)$ , where  $f$  is some function asymptotically equal to the value  $4.5 \cdot \frac{|W_n|^2}{n}$ . By the other words, we have obtained the estimation, approximately 4.5 times better than in problem 28!

**Problem 30.** Prove that the estimation of problem 29 in the standard sense cannot be asymptotically improved.

The notation " $G(n, 3, 1)$ " itself prompts that this graph has the generalization. It is graph  $G(n, r, s)$ . Its vertices are all  $r$ -element subsets of set  $\{1, \dots, n\}$ , and two vertices are connected by edge, if and only if the intersection of the corresponding sets contains exactly  $s$  elements. In other words, the vertices are  $n$ -dimensional points with "coordinates" 0 or 1, where the number of 1's is exactly  $r$ . Edge is drawn if and only if the scalar product of the vertices equals  $s$ . Graphs  $G(n, r, s)$  are called *Johnson graphs*, and the particular case of them, graphs  $G(n, r, 0)$ , are called *Kneser graph*.

**Problem 31.** Find the number of the edges of graph  $G(n, r, s)$ .

**Problem 32.** Find the number of the triangles of graph  $G(n, r, s)$ .

**Problem 33\*.** Prove that the analogue for the results from problems 29 and 30 is the estimation of the form  $\frac{|W_n|^2}{n^s} \cdot \frac{C_r^s \cdot r!}{2 \cdot (r-s)!}$  that asymptotically cannot be improved. Here we have to demand  $n^{r-1} = o(|W_n|)$ .

The following result you can apply without proof.

**Erdős–Ko–Rado theorem.** Let  $n \geq 2r$ . Then  $\alpha(G(n, r, 0)) = C_{n-1}^{r-1}$ .

**Problem 34.** Prove that if  $W_n$  is an arbitrary subset of the set of vertices of graph  $G(n, r, 0)$  and  $l = |W_n| > \alpha(G(n, r, 0))$ , then

$$r(W_n) \geq \frac{l(l - (C_n^r - C_{n-r}^r))}{2}.$$



---

On Sets of Distances of  $n$  Points

Author(s): P. Erdos

Source: *The American Mathematical Monthly*, Vol. 53, No. 5 (May, 1946), pp. 248-250

Published by: Mathematical Association of America

Stable URL: <http://www.jstor.org/stable/2305092>

Accessed: 19/08/2009 11:17

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit organization founded in 1995 to build trusted digital archives for scholarship. We work with the scholarly community to preserve their work and the materials they rely upon, and to build a common research platform that promotes the discovery and use of these resources. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

# ON SETS OF DISTANCES OF $n$ POINTS

P. ERDÖS, Stanford University

**1. The function  $f(n)$ .** Let  $[P_n]$  be the class of all planar subsets  $P_n$  of  $n$  points and denote by  $f(n)$  the minimum number of different distances determined by its  $n$  points for  $P_n$  an element of  $\{P_n\}$ . Clearly,  $f(3)=1$  (with the three points forming the vertices of an equilateral triangle)  $f(4)=2$ ,  $f(5)=2$ . The following theorem establishes rough bounds for arbitrary  $n$ . Though I have sought to improve this result for many years, I have not been able to do so.

**THEOREM 1.** *The minimum number  $f(n)$  of distances determined by  $n$  points of a plane satisfies the inequalities*

$$(n - 3/4)^{1/2} - 1/2 \leq f(n) \leq cn/(\log n)^{1/2}.$$

*Proof.* Let  $P_1$  be an arbitrary vertex of the least convex polygon determined by the  $n$  points, and denote by  $K$  the number of different distances occurring among the distances  $P_1P_i$  ( $i=2, 3, \dots, n$ ). If  $N$  is the maximum number of times the same distance occurs, then clearly  $KN \geq n-1$ .

If  $r$  is a distance that occurs  $N$  times then there are  $N$  points on the circle with center  $P_1$  and radius  $r$ , which all lie on the same semi-circle (since  $P_1$  is a vertex of the least convex polygon). Denoting these points by  $Q_1, Q_2, \dots, Q_N$ , we have  $Q_1Q_2 < Q_1Q_3 < \dots < Q_1Q_N$ , and these  $N-1$  distances are pairwise distinct. Thus  $f(n) \geq \max(N-1, (n-1)/N)$ , which is a minimum when  $N(N-1) = n-1$ . This yields the first part of the theorem.

Considering now the points  $(x, y)$  with integer coordinates for  $0 \leq x, y \leq n^{1/2}$ , we obtain at least  $n$  points  $P_i$  which pairwise have distances of the form  $(u^2+v^2)^{1/2}$ ,  $0 \leq u \leq n^{1/2}$ ,  $0 \leq v \leq n^{1/2}$ . Now it is well-known that the number of different integers not exceeding  $2n$  which are of the form  $u^2+v^2$  is less than  $cn/(\log n)^{1/2}$ , and the proof is complete.\*

For  $n$  points in  $k$ -dimensional space the same method yields  $c_1 n^{1/k} < f(n) < c_2 n^{2/k}$ .

**2. Some conjectures concerning  $f(n)$ .** Let us assume that our  $n$  points form a convex polygon. Then I conjecture that  $f(n) \geq [n/2]$ , with the equality sign valid when the  $n$  points are vertices of a regular  $n$ -gon. I am unfortunately unable to prove this. The following conjecture is stronger: In every convex polygon there is at least one vertex with the property that no three vertices of the polygon are equally distant from it. If this is the case, then clearly we would obtain  $[n/2]$  different distances by considering all the distances from such a vertex.

A still stronger conjecture is that on every convex curve there exists a point  $P$  such that every circle with center  $P$  intersects the curve in at most 2 points.

**3. The function  $g(n; r)$ .** Denoting by  $g(n; r)$  the maximum number of times a given distance  $r$  can occur among  $n$  points of a plane we establish

\* Landau, Verteilung der Primzahlen, vol. 2.

THEOREM 2.  $n^{1+\epsilon/\log \log n} < g(n; r) < n^{3/2}$ .

*Proof.* Assuming that there are  $x_i$  points at distance  $r$  from  $P_i$ , clearly  $g(n; r) = \max \frac{1}{2} \sum_{i=1}^n x_i$ . We suppose that  $x_1 \geq x_2 \geq \dots \geq x_n$ . Now the  $x_i$  points at distance  $r$  from  $P_i$  can contain at most two points with distance  $r$  from  $P_j$ . Hence

$$(1) \quad \sum_{i=1}^j (x_i - 2i + 2) \leq n \quad \text{for } j = 1, 2, \dots, n.$$

Put  $[n^{1/2}] = a$ ,  $n^{1/2} - a = \epsilon$ ,  $0 \leq \epsilon < 1$ . We have from (1)

$$(2) \quad x_1 + x_2 + \dots + x_a \leq n + 2 \binom{a}{2} = 2n - 2\epsilon n^{1/2} + \epsilon^2 - n^{1/2} + \epsilon \\ < 2n - 2\epsilon n^{1/2}$$

for  $n \geq 4$ . Thus

$$(3) \quad x_a < \frac{1}{a} (2n - 2\epsilon n^{1/2}) = 2n^{1/2}.$$

Hence from (2) and (3)

$$\sum_{i=1}^n x_i < 2n - 2\epsilon n^{1/2} + (n - a)2n^{1/2} = 2n^{3/2}$$

or

$$g(n; r) < n^{3/2}.$$

By again considering the set of points  $(x, y)$ ,  $0 \leq x, y \leq a$  we easily obtain (using well known theorems about the number of solutions of  $u^2 + v^2 = m$ )\*

$$g(n) > n^{1+\epsilon/\log \log n}$$

which completes the proof.

It seems likely that  $g(n) < n^{1+\epsilon}$ .

**4. Maximum and minimum distances.** If  $r$  is the diameter of the points  $P_i$ , it is well known that  $r$  can occur only  $n$  times.† This follows almost immediately from the fact that if  $\overline{P_1 P_2} = r$  and  $\overline{P_3 P_4} = r$  the lines  $P_1 P_2$  and  $P_3 P_4$  must intersect, for otherwise a simple argument shows that the diameter of  $P_1 P_2 P_3 P_4$  would be greater than  $r$ . Connect  $P_i$  with  $P_j$  if and only if their distance is  $r$ . We distinguish two cases. In Case 1, every  $P_i$  is connected with at most two other  $P$ 's. In this case the number of lines, *i.e.*, of pairs of points at distance  $r$  is clearly  $\leq n$ .

\* See *e.g.* P. Erdős, London Math. Soc. Journal, 1937, vol. 12, p. 133. The proof would depend on the prime number theorem for primes of the form  $4k+1$  (or on some weaker elementary result concerning the distribution of primes of the form  $4k+1$ ).

† Jahresbericht der Deutschen Math. Vereinigung, vol. 43, 1934, p. 114.

If  $P_1$  would be connected with three vertices say  $P_2, P_3, P_4$  where  $P_1P_3$  is between  $P_1P_2$  and  $P_1P_4$  then  $P_3$  can not be connected with any other  $P_i$ , since  $P_3P_i$  would have to intersect both  $P_1P_2$  and  $P_1P_4$  (the angle  $P_2P_1P_4$  is of course  $\leq \pi/3$ ), and thus be greater than  $r$ . Now we can just omit  $P_3$  and since both the number of points and the number of distances are reduced by 1, the proof can be completed by induction.

It would be interesting to have an analogous result for  $n$  points in  $k$  dimensional space. Vázsonyi\* conjectured that in three-dimensional space the maximum distance can not occur more than  $2n-2$  times.

If one could prove that in  $k$ -dimensional space the maximum distance can not occur more than  $kn$  times, the following conjecture of Borsuk would be established: *Each  $k$ -dimensional subset of diameter 1 can be decomposed into  $k+1$  summands each having diameter  $<1$ .*

Let now  $r'$  denote the minimal distance between any two  $P$ 's. First it is easy to see that  $r'$  can not occur more often than  $3n$  times. This is immediately clear from the fact that since  $r'$  was the minimal distance between any two  $P$ 's, there can be no more than 6  $P$ 's at distance  $r'$  from any given  $P$ .

Connect  $P_i$  with  $P_j$  if and only if their distance is  $r'$ . A simple argument shows that no two such lines  $P_1P_2$  and  $P_3P_4$  can intersect (otherwise there would be two  $P$ 's at distance  $<r'$ ). Thus the graph we obtain is planar, and from Euler's theorem it follows that the number of edges of such a graph is not greater than  $3n-6$ . Thus we have proved the following

**THEOREM 3.** *Let the maximum and minimum distances determined by  $n$  points in a plane be denoted by  $r$  and  $r'$ , respectively. Then  $r$  can occur at most  $n$  times and  $r'$  at most  $3n-6$  times.*

It is easy to give  $n$  points where the maximum distance occurs exactly  $n$  times. By more complicated arguments we can prove that the minimal distance  $r'$  can occur not more than  $3n-cn^{1/2}$  times, where  $c$  is a constant. On the other hand the example of the triangular lattice shows that  $r'$  can occur  $3n-c_1n^{1/2}$  times. I did not succeed in determining exactly how often  $r'$  can occur.

One could try to generalize Theorem 3 to higher dimensions. But already the case of three-dimensional space presents great difficulties. It would be of some interest to determine the maximum number of points on the unit sphere of  $k$  dimensions such that the distance of any two is  $\geq 1$ .

---

\* Oral communication.

# Turán type results for distance graphs<sup>\*</sup>

L.E. Shabanov,<sup>†</sup> A.M. Raigorodskii<sup>‡</sup>

## Abstract

The classical Turán theorem determines the minimum number of edges in a graph on  $n$  vertices with independence number  $\alpha$ . We consider unit-distance graphs on the Euclidean plane, i.e., graphs  $G = (V, E)$  with  $V \subset \mathbb{R}^2$  and  $E = \{\{\mathbf{x}, \mathbf{y}\} : |\mathbf{x} - \mathbf{y}| = 1\}$ , and show that the minimum number of edges in a unit-distance graph on  $n$  vertices with independence number  $\alpha \leq \lambda n$ ,  $\lambda \in [\frac{1}{4}, \frac{2}{7}]$ , is bounded from below by the quantity  $\frac{19-50\lambda}{3}n$ , which is several times larger than the general Turán bound and is tight at least for  $\lambda = \frac{2}{7}$ .

**Key words:** Turán theorem, independence number, distance graphs.

## 1 Introduction

The classical Turán theorem proved in [8] can be formulated as follows.

**Theorem 1.** *The minimum number of edges in a graph on  $n$  vertices with independence number  $\alpha$  is attained on a graph consisting of  $\alpha$  pairwise disjoint cliques whose sizes differ at most by one.*

One of the most important classes of graphs arising from combinatorial geometry is that consisting of *distance graphs*  $G = (V, E)$ , where

$$V \subset \mathbb{R}^n, \quad E = \{\{\mathbf{x}, \mathbf{y}\} : |\mathbf{x} - \mathbf{y}| = 1\}.$$

On the one hand, distance graphs are naturally related to the famous Nelson–Hadwiger problem on the chromatic numbers of spaces, and so their chromatic numbers and their independence numbers are intensively studied (see [1], [6], [7]). On the other hand, multiple questions concerning the edge numbers in distance graphs go back to Erdős (see [1], [3], [6]).

In this paper, we study distance graphs on the plane. Our main goal is to prove a Turán type result for such graphs, that is to find a lower bound for the minimum number of edges in a distance graph in  $\mathbb{R}^2$  given a number  $n$  of vertices and an independence number  $\alpha$ . Before stating our main result it is worth noting that for distance graphs with  $n$  vertices,  $\alpha$  cannot be arbitrary. It is definitely at least  $0.2293n$  (see [2], [4], [5]). Moreover, a strong belief is that it is greater than or equal to  $0.25n$ . Anyway, given a sequence of graphs with growing sets of vertices, the independence numbers of these graphs are quite far from being constant: they are proportional to the numbers of vertices.

One of the main results of our paper is as follows.

---

<sup>\*</sup>This work is done under the financial support of the following grants: the grant 15-01-00350 of Russian Foundation for Basic Research, the grant NSh-2964.2014.1 supporting Leading scientific schools of Russia.

<sup>†</sup>Higher School of Economics, Mathematics Faculty.

<sup>‡</sup>Moscow State University, Mechanics and Mathematics Faculty, Department of Mathematical Statistics and Random Processes; Moscow Institute of Physics and Technology, Faculty of Innovations and High Technology, Department of Data Analysis; Buryat State University, Institute of Mathematics and Informatics.

**Theorem 2.** *The minimum number of edges in a distance graph on  $n$  vertices with independence number  $\alpha \leq \lambda n$ ,  $\lambda \in [\frac{1}{4}, \frac{2}{7}]$ , is bounded from below by the quantity  $\frac{19-50\lambda}{3}n$ .*

The result of Theorem 2 is much stronger than that of Theorem 1. If, for example,  $\lambda = \frac{1}{4}$ , then Theorem 1 gives  $1.5n$  edges. In the same case, Theorem 2 gives at least  $\frac{13}{6}n$  edges. If, in turn,  $\lambda = \frac{2}{7}$  and  $n$  is divisible by 7, then the classical bound is equal to  $\frac{9}{7}n$ , and our bound equals  $\frac{11}{7}n$ . Moreover, in this case, our bound is tight, since one can take disjoint copies of the so-called Moser spindle, which has 7 vertices, 11 edges and independence number 2 (see fig. 1).

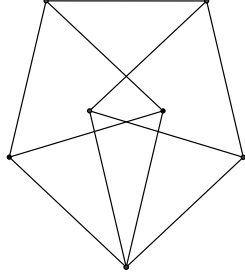


Figure 1: Moser's spindle

Finally, for  $\lambda \geq \frac{1}{3}$ , Turán's bound is trivially tight, since cliques on at most 3 vertices are distance graphs.

The paper is organized as follows. In Section 2, we give a more general setting of the problem and formulate another main result of the paper. In Section 3, we prove a “key lemma”. In Section 4, we prove both main theorems of the paper. In Section 5, we give some discussion.

## 2 More general setting

Consider a graph  $\Gamma = (W, E)$ . We call *the configuration* of  $\Gamma$  the vector  $(|W|, \alpha(\Gamma), |E|)$  and we denote it by  $\text{Config}(\Gamma)$ .

Let  $V$  be a set of vectors  $(a, b, c)$  with non-negative integer coordinates  $a, b, c$ . Then we call *an extension* of the set  $V$  the set of vectors  $(a, b+n, c+k)$ , where  $(a, b, c) \in V$  and  $n, k$  are again non-negative integers.

We say that a vector  $(a, b, c)$  is *good*, if it belongs to the extension of the set of all linear combinations with non-negative integer coefficients of the following vectors:  $(1, 1, 0)$ ,  $(2, 1, 1)$ ,  $(3, 1, 3)$ ,  $(4, 1, 9)$ ,  $(5, 1, 15)$ ,  $(6, 1, 22)$ ,  $(7, 2, 11)$ ,  $(n+1, 1, n(n-1))$ , where  $n \geq 6$ .

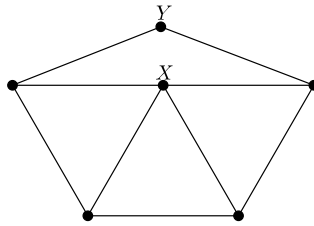


Figure 2: Semi-star graph



We call the graph, which is drawn on Figure 2, *semi-star* graph with *center*  $X$  and *top vertex*  $Y$ .  
The following proposition is quite simple, and we omit its proof here.

**Proposition 1.** *Any distance graph is free of  $K_4$  (complete graphs with four vertices),  $K_{3,2}$  (complete bipartite graphs with part sizes 2 and 3), and semi-star graphs.*

We say that a graph is *correct*, if it does not contain either  $K_4$  or  $K_{3,2}$ , or a semi-star graph as subgraphs. In particular, as we have just mentioned, every distance graph is correct. The second main result of our paper is given below.

**Theorem 3.** *The configuration of a correct graph is a good vector.*

The proof of Theorem 3 is based on

**Key Lemma.** *From any correct graph  $\Gamma$ , one can delete several vertices together with all the adjacent edges in such a way that for the remaining graph  $\Gamma'$ , the vector  $\text{Config}(\Gamma) - \text{Config}(\Gamma')$  is good.*

In the next section, we prove Key Lemma. In Section 4, we deduce Theorems 2 and 3 from Key Lemma.

## 3 Proof of Key Lemma

### 3.1 Some preliminaries

We say that a vector  $v = (v_1, v_2, v_3)$  *exceeds* a vector  $w = (w_1, w_2, w_3)$ , if  $v_1 = w_1, v_2 \geq w_2, v_3 \geq w_3$ , and we denote this relation by  $v \succeq w$ .

**Proposition 2.** *If  $u, v$  are vectors of dimension 3 such that  $u \succeq v$  and  $v$  is good, then  $u$  is also good.*

The proposition is straightforward, and thus we prove Key Lemma, provided we show that the vector  $\text{Config}(\Gamma) - \text{Config}(\Gamma')$ , with an appropriate  $\Gamma'$ , exceeds some good vector.

**Proposition 3.** *The vectors  $(1, 1, 0)$ ,  $(2, 1, 1)$ ,  $(3, 1, 3)$ ,  $(4, 1, 9)$ ,  $(5, 1, 15)$ ,  $(7, 2, 11)$ ,  $(8, 2, 18)$ ,  $(6, 1, 22)$ ,  $(12, 3, 26)$ ,  $(6, 2, 9)$ ,  $(10, 2, 30)$ ,  $(4n, n, 10n)$ ,  $(4m+1, m, 10m+3)$ ,  $(k+1, 1, k(k-1))$  ( $n, m, k \in \mathbb{Z}; n, m \geq 3; k \geq 6$ ) are good.*

*Proof.* The vectors

$$(1, 1, 0), (2, 1, 1), (3, 1, 3), (4, 1, 9), (5, 1, 15), (7, 2, 11), (6, 1, 22), (k+1, 1, k(k-1)) \text{ for } k \geq 6$$

are good by definition. Now, we briefly explain what happens with the other vectors:

- $(8, 2, 18) = 2(4, 1, 9)$ ;
- $(12, 3, 26) = (5, 1, 15) + (7, 2, 11)$ ;
- $(6, 2, 9) \succeq (6, 2, 6) = 2(3, 1, 3)$ ;
- $(10, 2, 30) = 2(5, 1, 15)$ ;
- $(4n, n, 10n) \succeq (4n, n, 9n) = n(4, 1, 9)$ ;
- $(4m+1, m, 10m+3) \succeq (4m+1, m, 9m+6) = (m-1)(4, 1, 9) + (5, 1, 15)$  for  $m \geq 3$ .

□

Let  $A$  be a vertex of the minimum degree in  $\Gamma$ . Consider several cases depending on the value of  $\deg A$ .

### 3.2 Case of $\deg A = 0$

Remove the vertex  $A$  from  $\Gamma$ . Since  $A$  had no neighbours, we get  $\text{Config}(\Gamma) - \text{Config}(\Gamma') = (1, 1, 0)$ .

### 3.3 Case of $\deg A = 1$

Remove from  $\Gamma$  the vertex  $A$  and its unique neighbour  $B$ . Obviously the independence number is reduced by 1 and the number of edges is reduced at least by 1. Therefore,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (2, 1, 1)$ .

### 3.4 Case of $\deg A = 2$

Remove from  $\Gamma$  the vertex  $A$  and both its neighbours  $B$  and  $C$ . Note that the number of edges is reduced at least by 3, since  $AB, AC$  are removed and also some edge adjacent to  $B$  and different from  $AB$  is removed (2 is the minimum degree in this case). Now it is clear that  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (3, 1, 3)$ .

### 3.5 Case of $\deg A = 3$

#### 3.5.1 Preliminaries

Let  $B, C, D$  be the neighbours of  $A$ . Since  $G$  does not contain  $K_4$ , we may assume that the vertices  $B$  and  $D$  are not adjacent. Below we consider several variants of subgraphs induced on  $A, B, C, D$ :

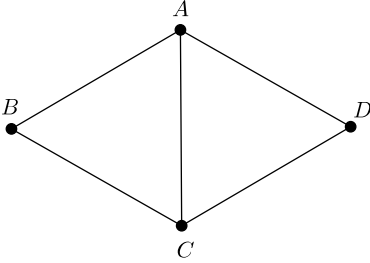


Figure 3: First variant

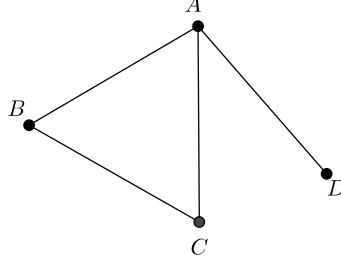


Figure 4: Second variant

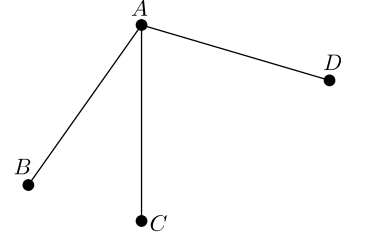


Figure 5: Third variant

#### 3.5.2 Graph from Figure 3

Let us calculate possible total numbers of edges adjacent to  $B$  or  $D$ . If the number of such edges is 6 or 7, then we remove the vertices  $B$  and  $D$  and all the vertices adjacent to them. Since the vertices  $B$  and  $D$  are not adjacent and also they are not adjacent to any of the vertices of the remaining graph  $\Gamma'$ , the independence number is reduced at least by 2. Moreover, since  $\Gamma$  is free of  $K_{3,2}$ , the vertices  $B$  and  $D$  do not have common neighbours different from  $A$  and  $C$ . Therefore, the number of vertices that have been removed is 6 or 7. Finally, since the degree of each vertex is at least 3, the total number of edges adjacent to the removed vertices is not less than 9 or 11, respectively. Thus, the vector  $\text{Config}(\Gamma) - \text{Config}(\Gamma')$  exceeds the vectors  $(6, 2, 9), (7, 2, 11)$ , respectively.

If the number of edges adjacent to  $B$  or  $D$  is at least 8, then we remove the vertices  $A, B, C, D$ . The independence number is reduced at least by 1, since the vertex  $A$  is not adjacent to any of the remaining vertices. The number of edges is reduced, in turn, at least by 9, for at least 8 edges adjacent to  $B$  or  $D$  are removed and also the edge  $AC$  is deleted. Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (4, 1, 9)$ .

### 3.5.3 Graph from Figure 4

Let us look at possible total numbers of edges adjacent to  $B$  or  $D$ . If the number of such edges is 6, then we remove the vertices  $B$  and  $D$  and all the vertices adjacent to them. Since the vertices  $B$  and  $D$  are not adjacent and also they are not adjacent to any of the vertices of the remaining graph  $\Gamma'$ , the independence number is reduced at least by 2. The number of vertices that have been removed is 6 or 7. Since the degree of any vertex is at least 3, the total number of edges adjacent to the removed vertices is at least 9 or 11, respectively. Thus, the vector  $\text{Config}(\Gamma) - \text{Config}(\Gamma')$  exceeds the vectors  $(6, 2, 9)$ ,  $(7, 2, 11)$ , respectively.

If the number of edges adjacent to  $B$  or  $D$  is 7 or larger, then we remove the vertices  $A, B, C, D$ . The independence number is reduced at least by 1, since the vertex  $A$  is not adjacent to any of the remaining vertices. The number of edges is reduced, in turn, at least by 9, for at least 7 edges adjacent to  $B$  or  $D$  are removed and also at least two more edges adjacent to  $C$  are deleted. Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (4, 1, 9)$ .

### 3.5.4 Graph from Figure 5

Just remove the vertices  $A, B, C, D$ . Since the degree of each vertex  $B, C, D$  is at least 3 and these vertices are pairwise non-adjacent, the number of removed edges is at least 9. As usual, the independence number is reduced at least by 1, and therefore  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (4, 1, 9)$ .

## 3.6 Case of $\deg A = 4$

### 3.6.1 Preliminaries

Let  $B, C, D, E$  be the vertices adjacent to  $A$ . Consider a subgraph induced on  $B, C, D, E$ . Note that it cannot have a vertex of degree 3, since otherwise by adding the vertex  $A$  we get  $K_{3,2}$ , which is forbidden. Also, the absence of  $K_{3,2}$  yields that among  $B, C, D, E$ , there are no 4-cycles. Finally, the absence of  $K_4$  yields, in turn, that among  $B, C, D, E$ , there are no 3-cycles (triangles). Thus, only the following 5 variants are possible for a graph on the vertices  $A, B, C, D, E$  (see fig. 6–10).

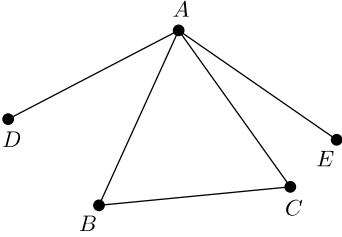


Figure 6: First variant

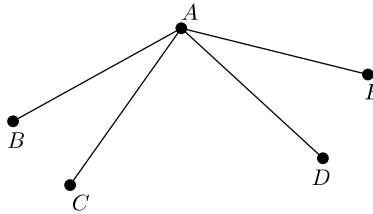


Figure 7: Second variant

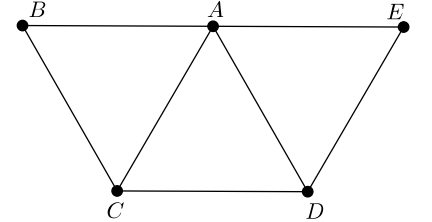


Figure 8: Third variant

### 3.6.2 Graphs from Figures 6 and 7

Remove the vertices  $A, B, C, D, E$ . The independence number is reduced at least by 1. The number of edges is reduced at least by 15, since any vertex among  $B, C, D, E$  is of degree at least 4 and at most 1 edge is calculated twice. Therefore,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (5, 1, 15)$ .

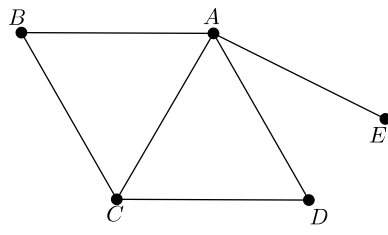


Figure 9: Fourth variant

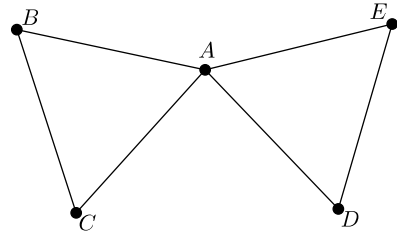


Figure 10: Fifth variant

### 3.6.3 Graph from Figure 8

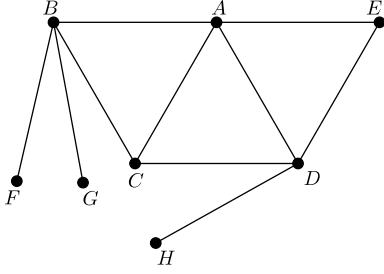


Figure 11:

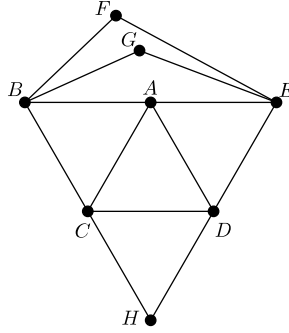


Figure 12:

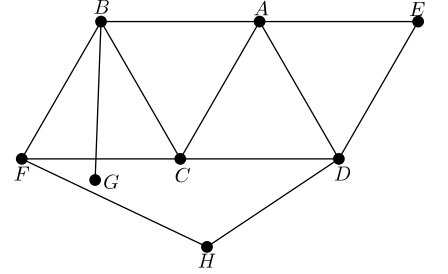


Figure 13:

First, assume that the vertices  $B, D$  are both of degree 4. Denote by  $F, G$  the vertices adjacent to  $B$  and different from  $A$  and  $C$ . Also, denote by  $H$  the fourth vertex adjacent to  $D$ . The vertex  $H$  does not coincide either with  $F$  or with  $G$ , since otherwise  $B$  and  $D$  share three neighbours and we obtain a  $K_{3,2}$ . Remove the 8 vertices  $A, B, C, D, E, F, G, H$  (see fig. 11). The independence number is reduced at least by 2, since the vertices  $B$  and  $D$  are neither adjacent one to the other, nor adjacent to any of the remaining vertices.

Let us prove that the number of removed edges is greater than or equal to 18. The sum of the degrees of the vertices  $A, B, C, D, E, F, G, H$  is at least 32. If we show that the number of edges in a subgraph on the vertices  $A, B, C, D, E, F, G, H$  is at most 14, then we are done.

Some 10 edges are drawn on fig. 11. Moreover, all the edges adjacent to  $A, B, D$  are indicated there. Let us prove that among the vertices  $C, E, F, G, H$ , there are at most 4 edges. Since the vertices  $B, C$  have no more than 2 common neighbours, the edges  $CF, CG$  cannot appear simultaneously. Without loss of generality, assume that there is no  $CG$ .

Since  $C$  and  $E$  have at most 2 common neighbours, the edges  $CH$  and  $EH$  cannot appear simultaneously.

If the edge  $EF(EG)$  is present as on fig. 12, then the vertices  $A, B, C, D, E, F(G)$  form a semi-star graph with center  $A$  and top vertex  $F(G)$ . Therefore, the graph  $\Gamma$  does not have edges  $EF$  and  $EG$ .

If in  $\Gamma$ , the edges  $CF$  and  $FH$  appear simultaneously (see fig. 13), then the vertices  $A, B, C, D, F, H$  form a semi-star graph with center  $C$  and top vertex  $H$ .

The edge  $CE$  is absent due to the construction of the subgraph on the vertices  $A, B, C, D, E$ . So only the pairs of vertices  $(F, G), (G, H)$  remain, which can form the third and the fourth edges of the subgraph

on the vertices  $C, E, F, G, H$ . Thus, we really get the bound 14 for the number of edges in the subgraph on the vertices  $A, B, C, D, E, F, G, H$ , and we eventually have that  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (8, 2, 18)$ .

Recall that we assumed that the vertices  $B, D$  were both of degree 4. Of course, if the same is true for  $C, E$ , then again  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (8, 2, 18)$ .

Thus, assume that there exists a vertex of degree at least 5 both among  $B, D$  and  $C, E$ . In this case, remove the vertices  $A, B, C, D, E$ . The independence number is reduced at least by 1. The number of edges is, in turn, reduced at least by 15, since the sum of the degrees of the vertices  $B, C, D, E$  is at least 18 and there are only 3 edges between these vertices. Finally,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (5, 1, 15)$ .

### 3.6.4 Graph from Figure 9

Divide the argument into two parts roughly in the same way as it was done in the previous case. Namely, either the degrees of both  $B$  and  $D$  equal 4, or at least one among  $B, D$  has at least 5 neighbours. The second situation is much simpler, as before, so let us start here with it. Indeed, remove the vertices  $A, B, C, D, E$ . The independence number is reduced at least by 1. The number of edges is, in turn, reduced at least by 15, since the total number of edges adjacent to the vertices  $B, C, D, E$  is not less than 17 and only 2 of them were calculated twice. Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (5, 1, 15)$ .

Now, assume that both  $B, D$  are of degree 4. We proceed like in Subsection 3.6.3. Since the vertices  $B$  and  $D$  cannot have 3 common neighbours (due to the absence of  $K_{3,2}$ ), they have exactly 2 such neighbours —  $A$  and  $C$ . So we can denote by  $F, G$  the two other vertices adjacent to  $B$  and by  $H, I$  — the two other vertices adjacent to  $D$  (see fig. 14).

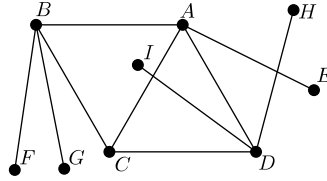


Figure 14:

Let us prove, as in Subsection 3.6.3, that removing some 8 vertices (namely,  $A, B, C, D, F, G, H, I$ ) gives us the bound  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (8, 2, 18)$ . Of course, we just need to show that here again the number of edges is reduced at least by 18, and to this end we need to analyze the structure of a subgraph on the vertices  $A, B, C, D, F, G, H, I$  and to see that the number of edges in this subgraph is at most 14. This seems to be very similar to what was done earlier. However, there are important subtleties: actually, either that is true, or we come back to a previously considered situation.

Since the graph  $\Gamma$  is free of  $K_{3,2}$ , among  $CF, CG$  as well as among  $CH, CI$ , at most one edge is present in  $\Gamma$ . Without loss of generality, assume that the edges  $CG, CI$  are absent.

If among  $CF, FG$  both edges are drawn, then we come back to the situation from fig. 8 with the vertices  $B, A, C, F, G$ . Analogously, if among  $CH, HI$  both edges are drawn, then we come back to the situation from fig. 8 with the vertices  $D, A, C, H, I$ . Therefore, we may assume that among  $CF, FG, CH, HI$  at most two edges are present.

Furthermore,  $\Gamma$  is free of  $K_{3,2}$  and thus among  $FH, FI, GH, GI$  we have at most 3 edges.

Summing up all the above inequalities, we see that a subgraph on the vertices  $C, F, G, H, I$  has at most 5 edges, which means that we do really have the bound by 14 for the number of edges in a subgraph on the vertices  $A, B, C, D, F, G, H, I$ . The case is complete.

### 3.6.5 Graph from Figure 10

If the degree of a vertex among  $B, C, D, E$  is at least 5, then we remove  $A, B, C, D, E$ . It is already clear that  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (5, 1, 15)$ . Let us discuss the opposite case.

We need some new definitions. Let a vertex of a graph satisfy the three following conditions: it is of degree 4; each of its neighbours is of degree 4; the configuration of the neighbours is the same as the one of the vertex  $A$  on fig. 10. We call such vertex a *key vertex*. If all the vertices of a graph are key vertices, then we call *key graph* the graph itself.

**Proposition 4.** *If in a connected graph, there is a vertex of degree 4 and all the vertices of degree 4 are key ones, then the graph is key.*

All the cases, in which a graph  $\Gamma$  has a non-key vertex of degree 4, are already considered. Thus, it remains to analyze the case of a key graph.

**Lemma 1.** *Any key graph contains a cycle of length at least 4.*

*Proof.* Take a vertex  $A$  in a key graph and suspend the graph on  $A$ . Let the level of  $A$  be 0. Let  $U$  be a vertex of the maximum level and  $V$  be a vertex of the previous level adjacent to  $U$ . Let  $W$  be a common neighbour of  $U$  and  $V$ . Let  $X$  be a vertex adjacent to  $V$  and different from  $U$  and  $W$ . Consider paths from  $U$  to  $A$  and from  $X$  to  $A$ , in which the level of any vertex is by 1 smaller than the level of the preceeding vertex. Since obviously the level of  $V$  is greater than 1, the vertices  $U$  and  $X$  do not coincide with  $A$ . Let  $B$  be the first common point of the paths  $UA, XA$ . Then since  $U$  and  $X$  are not adjacent and their levels differ at most by 1, they do not coincide with  $B$ . Therefore, the cycle  $UBXV$  ( $UB, BX$  denote paths, whereas  $UV, VX$  denote edges) consists of at least 4 edges, which completes the proof.  $\square$

Take a key graph  $\Gamma$ . Consider its shortest cycle of length greater than 3. Note that if two vertices in the cycle are not consecutive, then they cannot be adjacent. Indeed, otherwise, if the length of the cycle exceeds 4, then we would get a cycle, which is shorter than the initial one, although its length would be still greater than 3; if the length of the initial cycle is, in turn, exactly 4, then the existence of an edge inside the cycle would contradict our assumption that all the vertices are key ones.

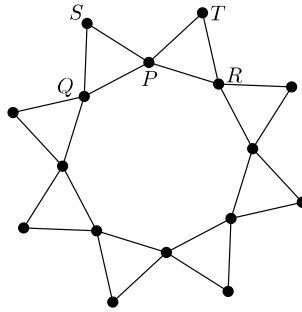


Figure 15: A minimum cycle of length greater than 3 in a key graph

Let us analyze the vertices, which are adjacent to the cycle. Let  $P$  be a vertex of the cycle. Denote by  $Q$  and  $R$  its neighbours in the cycle. Let  $S, T$  be the two other neighbours of  $P$ . Clearly among  $Q, R, S, T$  we have two pairs of adjacent vertices and they are not among  $(Q, R), (S, T)$ . Without loss of generality, we assume that they are  $(Q, S), (R, T)$ . Now, consider the vertices adjacent to  $Q$ . These are of course  $P, S$  and two more vertices that are also adjacent one to the other, but not adjacent to  $P, S$ : one of these vertices belongs to the cycle. Taking the next vertex of the cycle and proceeding the same way we see that all the edges coming out from the vertices of the cycle look like on fig. 15 (an example with 8 vertices). Here any two vertices adjacent to some two different vertices of the cycle do not coincide, since otherwise either they are not key ones, or there is a shorter cycle of length exceeding 3.

Consider different cases as on fig. 16–19.

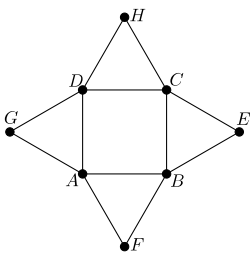


Figure 16:

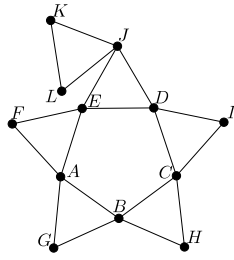


Figure 17:

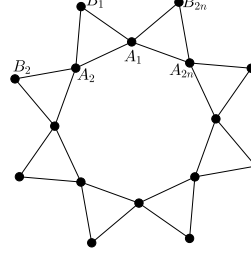


Figure 18:

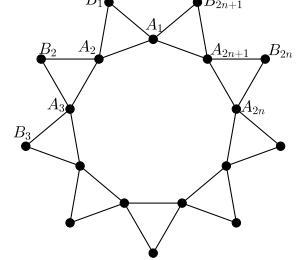


Figure 19:

**Cycle of length 4 (fig. 16)** Among the edges, which are not drawn on the picture, only the edges  $EG$  and  $FH$  might belong to the graph  $\Gamma$ . Therefore, the number of edges in a subgraph on the vertices  $A, B, C, D, E, F, G, H$  is at most 14. Remove the vertices  $A, B, C, D, E, F, G, H$ . The number of edges is reduced at least by 18, since, as usual, the total number of edges adjacent to the removed vertices is 32 and at most 14 edges are counted twice. The independence number is reduced at least by 2, since the vertices  $A$  and  $C$  are not adjacent one to the other as well as they are not adjacent to any of the remaining vertices. Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (8, 2, 18)$ .

**Cycle of length 5 (fig. 17)** Among the edges, which are not drawn on the picture, only some two edges from  $K$  and some two edges from  $L$  may belong to the graph, since otherwise a cycle of length 4 appears. Remove the 12 vertices  $A, B, C, D, E, F, G, H, I, J, K, L$ . The number of removed edges is at least  $48 - 22 = 26$ . The independence number is reduced at least by three due to the vertices  $A, C, J$ . Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (12, 3, 26)$ .

**Cycle of length  $2n$ ,  $n \geq 3$  (fig. 18)** Let the cycle consist of vertices  $A_1, \dots, A_{2n}$ , and let  $B_1, \dots, B_{2n}$  be the vertices outside the cycle adjacent to the vertices of the cycle. Note that all possible edges are drawn on the picture, since otherwise there is a cycle of length strictly greater than 3, but strictly smaller than  $2n$ . Remove the vertices  $A_1, \dots, A_{2n}, B_1, \dots, B_{2n}$ . The independence number is reduced at least by  $n$  due to the vertices  $A_2, A_4, \dots, A_{2n}$ . The number of edges is reduced at least by  $16n - 6n = 10n$ . Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (4n, n, 10n)$ .

**Cycle of length  $2n + 1$ ,  $n \geq 3$  (fig. 19)** Let the cycle consist of vertices  $A_1, \dots, A_{2n+1}$ , and let  $B_1, \dots, B_{2n+1}$  be the vertices outside the cycle adjacent to the vertices of the cycle. Note that, as in the previous case, all possible edges are drawn on the picture. Remove the vertices  $A_1, \dots, A_{2n+1}, B_1, \dots, B_{2n+1}$ . The independence number is reduced at least by  $n$  due to the vertices  $A_2, A_4, \dots, A_{2n}$ . The number of edges is reduced at least by  $(16n + 4) - (6n + 1) = 10n + 3$ . Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (4n + 1, n, 10n + 3)$ .

### 3.7 Case of $\deg A = 5$

Let  $B, C, D, E, F$  be the vertices adjacent to  $A$ . If a subgraph on the vertices  $B, C, D, E, F$  contains a 3-cycle, then, with the addition of the vertex  $A$ , a  $K_4$  appears. In case of a 4-cycle, we get a  $K_{3,2}$ . Finally, with a 5-cycle, we obtain a semi-star graph. Therefore, there are no cycles on the vertices  $B, C, D, E, F$ , which means that the number of edges in this subgraph is at most 4. Also, the absence of  $K_{3,2}$  yields that in the subgraph on the vertices  $B, C, D, E, F$  there are no vertices of degree 3. Thus, 4 edges can be drawn only as on fig. 20.

If the number of edges in a graph on the vertices  $B, C, D, E, F$  is bounded by 3, then the subgraph on the vertices  $A, B, C, D, E, F$  has at most 8 edges. Remove these vertices. As usual, the number of the removed edges is at least  $30 - 8 = 22$ . Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (6, 1, 22)$ .

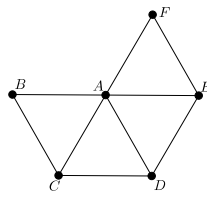


Figure 20:

If the number of edges in a graph on the vertices  $B, C, D, E, F$  is exactly 4, then the subgraph on the vertices  $A, B, C, D, E, F$  has 9 edges (see fig. 20). Call the vertex  $A$  a *support vertex*, if each of the vertices  $B, C, D, E, F$  is of degree 5.

If  $A$  is not a support vertex, then remove the vertices  $A, B, C, D, E, F$ . Clearly in this case, the sum of the degrees of the removed vertices is at least 31. Thus, the number of the removed edges is not less than 22 and we have  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (6, 1, 22)$ .

Let  $A$  be support. Since  $\Gamma$  is  $K_{3,2}$ -free, the vertices  $C$  and  $E$  have no other common neighbours than  $A$  and  $D$ . Since the vertices  $C, E$  are of degree 5, let  $G, H$  be the vertices adjacent to  $C$  and let  $I, J$  be the vertices adjacent to  $E$  (see fig. 21).

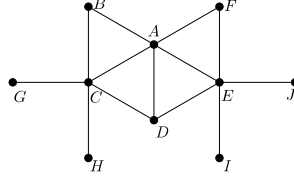


Figure 21:

Let us prove that the number of edges in a subgraph on the vertices on fig. 21 does not exceed 20.

On Figure 21, 13 edges are drawn. Moreover, for the vertices  $A, C, E$ , all the adjacent edges are indicated there. So it remains to show that a subgraph on the vertices  $B, D, F, G, H, I, J$  has at most 7 edges.

Since in the graph on fig. 20 all the edges between the vertices  $A, B, C, D, E, F$  are present, the edges  $BD, BF, DF$  do not belong to  $\Gamma$ . Furthermore, since  $\Gamma$  does not contain a semi-star, it does not have any of the edges  $BI, BJ, FG, FH$ . Also  $\Gamma$  is  $K_{3,2}$ -free, which means, in particular, that  $\Gamma$  cannot contain more than one edge in each of the following pairs:  $(BG, BH), (DG, DH), (DI, DJ), (FI, FJ)$ . Since the edges  $BG, DG$  cannot be present in  $\Gamma$  simultaneously, we may assume without loss of generality that  $\Gamma$  does not contain the edges  $BH$  and  $DG$ . Similarly, let us assume that  $\Gamma$  does not contain the edges  $DJ$  and  $FI$ .

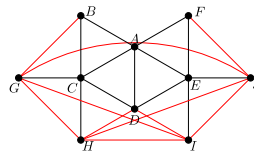


Figure 22:

Only 10 edges remain that are colored red on fig. 22. Suppose that, in contrast to what we want to



prove, one can keep some 8 red edges in such a way that the subgraph on the vertices

$$A, B, C, D, E, F, G, H, I, J$$

stay correct. Since  $\Gamma$  does not contain a semi-star graph, among the edges  $BG, GH, DH$ , only at most 2 can be drawn. Also, at most 2 edges are among  $DI, IJ, FJ$ . Therefore, if among the red edges, at least 8 are in  $\Gamma$ , then  $\Gamma$  contains the edge  $HI$ . If  $\Gamma$  contains the edge  $DH$ , then the vertices  $A, C, D, E, H, I$  form a semi-star graph with center  $D$  and top vertex  $I$ . Similarly, the edge  $DI$  is not in  $\Gamma$ . Once again, since we have at least 8 edges in  $\Gamma$ , we have in  $\Gamma$  the edges  $GH, GI, GJ, HJ, IJ$ . This eventually gives us a  $K_4$  on the vertices  $G, H, I, J$  leading to a contradiction.

Thus, we have finally shown that the number of edges on the vertices  $A, B, C, D, E, F, G, H, I, J$  is at most 20. Remove these vertices. The number of the removed edges is at least  $50 - 20 = 30$ . The independence number is reduced at least by 2, since the vertices  $C, E$  are not adjacent one to the other. So  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (10, 2, 30)$ .

### 3.8 Case of $\deg A = n \geq 6$

Let  $B_1, \dots, B_n$  be the vertices adjacent to  $A$ . If in a subgraph on the vertices  $B_1, \dots, B_n$ , there is a vertex of degree at least 3, then we obtain a  $K_{3,2}$ . Therefore, the maximum degree of a vertex in this subgraph is bounded by 2. So this subgraph has at most  $n$  edges. Then the number of edges in the subgraph on the vertices  $A, B_1, \dots, B_n$  does not exceed  $2n$ .

Remove the vertices  $A, B_1, \dots, B_n$ . Clearly the independence number is reduced at least by 1 and the number of edges is reduced at least by  $(n+1)n - 2n = n(n-1)$ . Thus,  $\text{Config}(\Gamma) - \text{Config}(\Gamma') \succeq (n+1, 1, n(n-1))$ .

## 4 Proofs of the two main theorems

### 4.1 Proof of Theorem 3

Let us proceed by induction in the number of vertices.

**Base of induction.** Note that in cases 3.6–3.8 of Key Lemma definitely not all the vertices were being removed from the corresponding graphs  $\Gamma$ . And in cases 3.2–3.5 at most 7 vertices were being removed. So we may consider here all the graphs on at most 7 vertices.

Let us call the graph from Theorem 1 the  $\alpha, n$ -Turán graph. Note that for  $\alpha \geq \frac{1}{3}n$ , the  $\alpha, n$ -Turán graph is the disjoint union of  $K_3, K_2$  and  $K_1$ , and so it is correct and its configuration is good.

Consider all possible pairs  $(\alpha, n)$ , where  $\alpha \leq n \leq 7$ . For all such pairs, but

$$(1, 4), (1, 5), (1, 6), (1, 7), (2, 7),$$

we have  $\alpha \geq n/3$ , which has been just discussed. For the pairs  $(1, 4), (1, 5), (1, 6), (1, 7)$ , the only corresponding graphs are the complete graphs on 4, 5, 6, 7 vertices. They are of course not correct.

Only one case of  $\alpha = 2, n = 7$  remains. Consider a vertex of the minimum degree in any such correct graph. Remove it and all its neighbours. The new graph is correct, and its independence number is at most 1. Therefore, it has no more than 3 vertices. This means that at least 4 vertices were removed, and so the above-considered vertex had at least 3 neighbours. Thus, each vertex in the graph has degree greater than or equal to 3, and consequently the number of edges is bounded from below by  $\frac{7 \cdot 3}{2}$ , that is, it is at least 11.

The base of induction is proved.

**Inductive step.** Apply Key Lemma and remove from graph  $\Gamma$  some of its vertices in such a way that the vector  $\text{Config}(\Gamma) - \text{Config}(\Gamma')$  is good. Then by the induction hypothesis, the vector  $\text{Config}(\Gamma')$  is good. Since the sum of good vectors is good, the vector  $\text{Config}(\Gamma) = (\text{Config}(\Gamma) - \text{Config}(\Gamma')) + \text{Config}(\Gamma')$  is good, too.  $\square$

## 4.2 Proof of Theorem 2

**Lemma 2.** *If a vector  $(u, v, w)$  is good, then it exceeds the vector  $(u, v, \frac{19}{3}u - \frac{50}{3}v)$*

*Proof.* Let us check the lemma for the “basis” vectors:

$$\begin{aligned} (1, 1, 0) &\succeq (1, 1, -31/3), (2, 1, 1) \succeq (2, 1, -12/3), (3, 1, 3) \succeq (3, 1, 7/3), \\ (4, 1, 9) &\succeq (4, 1, 26/3), (5, 1, 15) \succeq (5, 1, 15), (6, 1, 22) \succeq (6, 1, 64/3), \\ (7, 2, 11) &\succeq (7, 2, 11), (n+1, 1, n(n-1)) \succeq (n+1, 1, 19/3n - 31/3), \quad n \geq 6. \end{aligned}$$

The last series of inequalities holds true, since for  $n = 6$ , we have  $(7, 1, 30) \succeq (7, 1, 83/3)$  and if  $n$  increases by 1, then the third coordinate in the left-hand side increases by  $2n$  and the third coordinate in the right-hand side increases by  $19/3$ .

Suppose the lemma is true for some vectors  $u, v$ . Of course the relations  $a \succeq c, b \succeq d$  yield the relation  $a + b \succeq c + d$ . Then for  $u + v$ , the lemma is also true. The same type of argument can be used for any  $\lambda u$ , where  $\lambda$  is a positive constant. Finally, the relation “ $\succeq$ ” is transitive. Thus, the lemma is true for all good vectors.  $\square$

It follows from the lemma that the configuration of our graph  $\Gamma$  exceeds the vector  $(n, \lambda n, \frac{19-50\lambda}{3}n)$ , and, therefore, the number of edges in our graph is really greater than or equal to  $\frac{19-50\lambda}{3}n$ .

## 5 Some comments

In order to prove the main results, we used the fact that in any distance graph on the plane, there are no  $K_4$ ,  $K_{3,2}$  and semi-stars. A natural question arises: maybe one could use only one or two of these forbidden graphs and get the same result?

First, assume that only  $K_4$  and semi-stars are forbidden. In this case, one can prove the following result.

**Theorem 4.** *The minimum number of edges in a graph on  $n$  vertices with independence number  $\alpha \leq \lambda n$ ,  $\lambda \in [\frac{1}{4}, \frac{2}{7}]$ , and without  $K_4$  and semi-stars is bounded from below by the quantity  $\frac{17-43\lambda}{3}n$ .*

This result is a bit worse than the one of Theorem 2. For example, if  $\lambda = \frac{1}{4}$ , then Theorem 4 gives the bound by  $\frac{25}{12}n$  instead of  $\frac{26}{12}n$  following from Theorem 2.

The proof of Theorem 4 is very close to the proof of Theorem 2. We do not present it in this paper because of its complete similarity to the above-given argument. We only list here a set of “good” vectors, which plays, in a proof, the same role as it was in Proposition 3:

$$\begin{aligned} (1, 1, 0), (2, 1, 1), (3, 1, 3), (4, 1, 9), (5, 1, 14), (6, 1, 20), (7, 2, 11), (8, 2, 17), (n+1, 1, \frac{3n^2}{4}), \quad n \geq 6, \\ (5, 2, 8), (6, 2, 9), (6, 2, 12), (7, 2, 14), (7, 3, 14), (8, 3, 16), (9, 3, 18), (10, 3, 20), (11, 3, 22). \end{aligned}$$

Note that we do not claim that Theorem 4 cannot be improved further. However, for our proofs,  $K_{3,2}$  appears to be important.

Now, assume that only  $K_4$  is excluded. For simplicity, consider again the illustrative case of  $\alpha \leq n/4$ . We claim that in this case, the bound for the number of edges is  $2n$  and this bound is *tight* for  $n \equiv 0 \pmod{4}$ . If we are right, then of course semi-stars appear to be important as well:  $2n$  is smaller than  $\frac{25}{12}n$ . So let us prove the claim. On the one hand, the graphs on fig. 23 show that  $2n$  is the best possible bound under the current conditions.

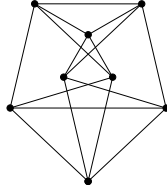


Figure 23: Graphs for the  $2n$  bound

It is worth noting that the graphs on fig. 23 are not only  $K_4$ -free, but also  $K_{3,2}$ -free. Thus,  $K_{3,2}$  is important only together with both  $K_4$  and the semi-star graph. Of course, we see a semi-star graph on fig. 23.

On the other hand, let us show that the lower bound for the number of edges in a  $K_4$ -free graph with independence number at most one fourth of the number  $n$  of vertices is indeed  $2n$ . For more transparency, let us switch to the case when the number of vertices is  $4n$  and the independence number is at most  $n$ . In this notation, we have to show that the number of edges is at least  $8n$ . As usual, we proceed by induction on  $n$ .

The case of  $n = 1$  is obviously impossible: there are no graphs on 4 vertices without  $K_4$ , but with  $\alpha = 1$ . So let  $n = 2$ . Either each of the 8 vertices of a given graph is of degree at least 4, in which case the number of edges is indeed at least 16 (and thus the base of induction is proved), or there is a vertex of degree at most 3, and we will show below that in this case, one can remove 4 vertices from the graph reducing the independence number at least by 1 and the number of edges at least by 8: for  $n = 2$ , that is impossible, as we would again obtain a graph on 4 vertices without  $K_4$ , but with independence number 1. Therefore, we get the base of induction. To make this argument complete and to provide the induction step, we need the following lemma.

**Lemma 3.** *Let  $\Gamma$  be a graph with  $4n$  vertices ( $n \geq 2$ ), without  $K_4$  and with  $\alpha(\Gamma) \leq n$ . Let  $A$  be a vertex of the minimum degree in  $\Gamma$ . Suppose  $\deg A \leq 3$ . Then one can remove 4 vertices from the graph reducing the independence number at least by 1 and the number of edges at least by 8.*

The induction step is obvious, so that it remains to prove the lemma.

*Proof.* Let us consider all possible values of  $\deg A$ .

**Case of  $\deg A = 0$ .** Remove the vertex  $A$  from  $\Gamma$ . Obviously in the new graph  $\Gamma'$  the independence number is smaller. However, we have not yet removed 8 or more edges. Consider  $\Gamma'$ . It has  $4n - 1$  vertices and  $\alpha(\Gamma') \leq n - 1$ . Consequently, the chromatic number  $\chi(\Gamma')$  is bounded from below by  $\frac{4n-1}{n-1} > 4$ . In other words,  $\chi(\Gamma') \geq 5$ . Of course this means that the maximum degree of a vertex in  $\Gamma'$  is greater than 3. It cannot be exactly equal to 4, since by Brook's theorem (we do not forget that  $\Gamma'$  is  $K_4$ -free) the chromatic number would be bounded by 4 from above. Thus, we have a vertex  $B$  of degree at least 5 in  $\Gamma'$ . Remove it. In the new graph  $\Gamma''$ , the number of vertices is  $4n - 2$ , the independence number is at most  $n - 1$ , and the number of edges is by at least 5 smaller than in the initial graph  $\Gamma$ . Since  $\frac{4n-2}{n-1} > 4$ , we apply once again the above argument and find a vertex  $C$  of degree at least 5. Removing  $C$ , we already get even more than we needed: the number of vertices is reduced by 3 (we promised 4). The number of edges is reduced by 10 (we promised 8). The independence number is reduced by 1 or more. The case is complete.

**Cases of  $\deg A \in \{1, 2\}$ .** Here the same procedure as in the first case applies. Let us consider only the case of degree 2. Remove the vertex  $A$  and both its neighbours  $B, C$ . We removed 3 vertices and at least 3 edges (2 is the *minimum* degree of a vertex). The independence number is already reduced. In the new graph, we have  $4n - 3$  vertices, and since  $\frac{4n-3}{n-1} > 4$ , we find a vertex  $D$  of degree 5. We remove it, and we are done.

**Case of  $\deg A = 3$ .** Let  $B, C, D$  be the neighbours of  $A$ . We do not forget that the degrees of these vertices are at least 3 each. Since  $K_4$  is forbidden, we may assume that  $BD$  is not in our graph. One can easily check that if in addition some of the edges  $BC, CD$  is absent or the degree of at least one vertex among  $B, C, D$  is strictly greater than 3, then the total amount of edges adjacent to  $A, B, C, D$  is at least 8. Thus, it suffices to remove the vertices  $A, B, C, D$ .

It remains to consider the case when the degrees of the vertices  $B, C, D$  are all exactly equal to 3 and both edges  $BC$  and  $CD$  are in the graph. In this case, the vertex  $B$  has one more neighbour  $E$ . Remove from the graph the vertices  $A, B, C, E$ , and we are done. □

## References

- [1] P. Brass, W. Moser, J. Pach, *Research problems in discrete geometry*, Springer, 2005.
- [2] H.T. Croft, *Incident incidents*, Eureka (Cambridge), 30 (1967), 22 - 26.
- [3] P. Erdős, *On sets of distances of  $n$  points*, Amer. Math. Monthly, 53 (1946), 248 - 250.
- [4] A.A. Kokotkin, *On large subgraphs of a distance graph which have small chromatic number*, Math. Notes, 96 (2014), N2, 298 - 300.
- [5] D.G. Larman, C.A. Rogers, *The realization of distances within sets in Euclidean space*, Mathematika, 19 (1972), 1 - 24.
- [6] A.M. Raigorodskii, *Cliques and cycles in distance graphs and graphs of diameters*, “Discrete Geometry and Algebraic Combinatorics”, AMS, Contemporary Mathematics, 625 (2014), 93 - 109.
- [7] A.M. Raigorodskii, *Coloring Distance Graphs and Graphs of Diameters*, Thirty Essays on Geometric Graph Theory, J. Pach ed., Springer, 2013, 429 - 460.
- [8] P. Turán, *On an extremal problem in graph theory*, Matematikai Fizikai Lapok, 48 (1941), 436 - 452 (in Hungarian).

## Некоторые свойства конструкций Микеля.

Проект представляет Константин Иванов при деятельном участии Ивана Фролова. Идея: Павел Долгирев. Отдельная благодарность Александру Скутину за формулировку задач 20-23.

При поддержке Алексея и Олега Заславских, а также Павла Кожевникова.

Значком  $^\circ$  обозначены некоторые общеизвестные факты, без которых, однако, решение дальнейших задач будет затруднительно. Звёздочкой  $*$  обозначены предположительно сложные задачи.

### Часть 1

**1 $^\circ$**  (*Теорема Микеля*) В треугольнике  $ABC$  на сторонах  $AB, BC, CA$  взяты точки  $C_1, A_1, B_1$  соответственно. Докажите, что окружности, описанные около  $\triangle AB_1C_1, \triangle A_1BC_1, \triangle A_1B_1C$ , имеют общую точку.

**2 $^\circ$**  (*Лемма о воробьях*) Дан угол  $ABC$ . По прямым  $AB, BC$  перемещаются с постоянными (необязательно равными) скоростями точки  $C_1, A_1$  соответственно. Докажите, что все окружности  $BC_1A_1$  проходят через другую точку, отличную от  $B$ . В каком случае это неверно?

**3 $^\circ$**  (*Теорема Чевы в форме синусов*) В треугольнике  $ABC$  на сторонах  $AB, BC, CA$  взяты точки  $C_1, A_1, B_1$  соответственно. Докажите, что прямые  $AA_1, BB_1, CC_1$  пересекаются в одной точке или все три параллельны тогда и только тогда, когда

$$\frac{\sin \angle \overrightarrow{ABB_1} \cdot \sin \angle \overrightarrow{BCC_1} \cdot \sin \angle \overrightarrow{CAA_1}}{\sin \angle \overrightarrow{B_1BC} \cdot \sin \angle \overrightarrow{C_1CA} \cdot \sin \angle \overrightarrow{A_1AB}} = 1$$

**4 $^\circ$**  (*Точка Микеля*) Пусть даны четыре прямые общего положения. Исключением одной прямой можно получить три прямые, образующие треугольник, всего четыре треугольника. Докажите, что описанные окружности этих четырёх треугольников пересекаются в одной точке.

**5 $^\circ$**  (*Окружность Микеля*) Пусть даны 5 прямых общего положения. Докажите, что точки Микеля всех пяти возможных четвёрок прямых лежат на одной окружности.

**6 $^\circ$**  Даны две окружности  $\mathcal{A}, \mathcal{B}$ . Докажите, что ГМТ точек  $X$  таких, что

$$\frac{\text{степень } X \text{ относительно } \mathcal{A}}{\text{степень } X \text{ относительно } \mathcal{B}} = \text{const}$$

является окружностью, в случае

a) когда  $\mathcal{A}, \mathcal{B}$  пересекаются

b) для произвольного положения  $\mathcal{A}$  и  $\mathcal{B}$ .

**7 $^\circ$**  В треугольнике  $ABC$  педальные окружности двух точек совпадают. Докажите, что точки изогонально сопряжены в  $\triangle ABC$ .

**8.** Внутри треугольника  $ABC$  выбрана точка  $M$ , а на сторонах  $AB, BC, CA$  взяты точки  $C_1, A_1, B_1$  соответственно. Прямые  $AM, BM, CM$  пересекают окружности, описанные около треугольников  $AB_1C_1, A_1BC_1, A_1B_1C$  в точках  $M_a, M_b, M_c$  соответственно. Докажите, что точки  $M, M_a, M_b, M_c$  лежат на одной окружности (в дальнейшем будем называть её окружностью  $\mathcal{M}$ ).

**9.** Пусть в обозначениях предыдущей задачи  $P$  – точка пересечения окружностей  $AB_1C_1, A_1BC_1, A_1B_1C$ . Пусть прямая  $PA_1$  пересекает  $\mathcal{M}$  в точке  $A'$ . Докажите, что  $MA' \parallel BC$ .

**10.** Докажите, что прямые  $M_aA', M_bB', M_cC'$  пересекаются в одной точке или параллельны.

**11\*** Докажите, что окружности, описанные около треугольников  $AM_aA', BM_bB', CM_cC'$ , соосны.

**12\*** Пусть есть четыре прямые  $a, b, c, d$  общего положения и их точки пересечения  $X_{ab}, X_{ac}, X_{ad}, X_{bc}, X_{bd}, X_{cd}$ . Есть окружность  $\mathcal{K}$  с выделенной точкой  $K$  на ней. Пусть  $Y_i$  – точка пересечения  $X_iK$  с  $\mathcal{K}$ . Докажите, что прямые  $Y_{ab}Y_{cd}, Y_{ac}Y_{bd}, Y_{ad}Y_{bc}$  пересекаются в одной точке или параллельны.

**13.** В треугольнике  $ABC$  выбираются произвольно точки  $C_1, C_2$  на стороне  $AB$ , точки  $A_1, A_2$  на стороне  $BC$ , точки  $B_1, B_2$  на стороне  $CA$ . Пара прямых  $A_1B_1$  и  $A_2B_2$  пересекается в точке  $L_c$ , точки  $L_a, L_b$  определяются аналогично. Окружности, описанные около  $\triangle A_1A_2L_c$  и  $\triangle B_1B_2L_c$  пересекаются в точках  $L_c$  и  $N_c$ , точки  $N_b$ , и  $N_a$  определяются аналогично.

а) Докажите, что прямые  $AN_a, BN_b, CN_c$  пересекаются в одной точке (назовём её  $N$ ).

б) Докажите, что  $N, N_a, N_b, N_c$  лежат на одной окружности (назовём её  $\mathcal{N}$ ).

Пусть окружности  $AB_1C_1, A_1BC_1, A_1B_1C$  пересекаются в точке  $P$ , а окружности  $AB_2C_2, A_2BC_2, A_2B_2C$  пересекаются в точке  $Q$ .

с) Докажите, что  $P$  и  $Q$  лежат на  $\mathcal{N}$ .

д) Докажите, что точка  $A'$  пересечения прямых  $PA_1$  и  $QA_2$  лежит на  $\mathcal{N}$ .

## Часть 2

В этом разделе значком гиперболы <sup>(1)</sup> обозначены задачи, в которых Вашей целью будет доказать исходное утверждение, а затем сформулировать и доказать аналогичное утверждение для гиперболы.

**14.** Даны две неподвижные точки  $A, B$  и точка  $X$ ,двигающаяся по прямой. Исследуйте на промежутки монотонности функцию  $f$ . Постройте циркулем и линейкой точку экстремума, если

а)  $f(X) = XA + XB$

б)  $f(X) = XA - XB$

**15°** (Задача Фаньяно) В треугольнике  $ABC$  на сторонах  $AB, BC, CA$  взяты точки  $C', A', B'$  соответственно, не совпадающие с вершинами  $\triangle ABC$ . Известно, что треугольник  $A'B'C'$  имеет минимальный возможный периметр из всех треугольников, вписанных в  $\triangle ABC$ . Докажите, что  $AA_1, BB_1$  и  $CC_1$  — высоты  $\triangle ABC$ .

**16<sup>(1)</sup>** (Оптическое свойство) Пусть  $A$  — точка на эллипсе с фокусами  $F_1$  и  $F_2$ . Докажите, что внешняя биссектриса угла  $F_1AF_2$  является касательной к эллипсу (имеет ровно одну общую точку с ним).

**17<sup>(1)</sup>** Эллипс с фокусами  $F_1$  и  $F_2$  касается сторон угла  $ABC$ . Докажите, что  $\angle ABF_1 = \angle CBF_2$ .

**18<sup>(1)</sup>** Фиксирован эллипс с фокусом  $F$ , прямая  $\ell$  его касается. Пусть  $P$  — проекция  $F$  на  $\ell$ . Докажите, что если  $\ell$  движется, то  $P$  движется по окружности, касающейся эллипса в двух точках.

**19.** Дан эллипс  $\mathcal{K}$  с фокусами  $F_1$  и  $F_2$ . Окружность  $\omega$  с центром  $O$  дважды касается его в точках  $X$  и  $Y$  (эллипс внутри окружности). Докажите, что

а)  $OF_1 = OF_2$ .

б)  $XF_1OF_2Y$  — вписанный пятиугольник.

с)<sup>(1)</sup> Пусть точка  $P$  движется по  $\omega$ . Тогда угол между  $PF_1$  и одной из касательных из  $P$  к эллипсу постоянен.

д) Дайте другое определение  $\omega$  так, чтоб  $\omega$  необязательно дважды касалась  $\mathcal{K}$ .

е) Прямая через  $O$  и центр  $\mathcal{K}$  пересекает  $\mathcal{K}$  в точке  $Z$ . Докажите, что окружность, описанная около  $\triangle OZF_1$ , касается  $\omega$ .

ф) Пусть окружности  $\alpha$  и  $\beta$  касаются  $\omega$  внутренним образом, проходят через  $F_1$  и второй раз пересекаются в точке  $E$ . Докажите, что из двух точек пересечения  $\alpha$  и  $\mathcal{K}$  можно выбрать точку  $I$ , а из двух точек пересечения  $\beta$  и  $\mathcal{K}$  можно выбрать точку  $J$ , так, что  $E$  будет лежать на прямой  $IJ$ .

г)<sup>\*</sup> Прямая через  $O$  и центр эллипса пересекает эллипс в точках  $Z$  и  $T$ , а окружность в точках  $A$  и  $B$ . На прямой  $ZT$  выбрана точка  $U$  так, что  $\angle UF_1O = 90^\circ$ . Докажите, что двойное отношение точек  $A, Z, U, B$  равно двойному отношению точек  $B, T, U, A$  (в указанном порядке).

h) Покажите, что, если принять  $\omega$  за абсолют модели Клейна плоскости Лобачевского, то  $\mathcal{K}$  будет окружностью или эквидистантой.

**20<sup>(1)</sup>** Даны две окружности  $\alpha$  и  $\beta$ , пересекающиеся в точках  $X$  и  $Y$ , в "дольку" их пересечения вписан эллипс, дважды касающийся каждой из окружностей. Прямая  $\ell_X$  касается эллипса, отделяет от него точку  $X$  и пересекает "дольку" в двух точках. Также прямая  $\ell_X$  пересекает окружность  $\alpha$  вне дольки в точке  $A_1$ , и пересекает окружность  $\beta$  вне дольки в точке  $B_1$ . Аналогично выберем прямую  $\ell_Y$  и определим точки  $A_2$  и  $B_2$ . Докажите, что  $A_1A_2 \parallel B_1B_2$ .

**21<sup>\*</sup>** По двум окружностям с одинаковыми угловыми скоростями движутся две точки  $N$  и  $M$ . Найдите огибающую (кривую, касающуюся всех) прямых  $NM$ .

**22<sup>\*</sup>** По двум прямым с постоянными скоростями движутся две точки  $N$  и  $M$ . Найдите огибающую прямых  $NM$ .

**23<sup>(1)</sup>** Даны две пересекающиеся окружности. В "дольку" их пересечения вписываются всевозможные эллипсы, дважды касающиеся каждой из окружностей. Найдите ГМТ их фокусов.

### Часть 3

**24°** (*Ортологичные треугольники*) Даны точки  $A, B, C, A_1, B_1, C_1$  общего положения. Пусть перпендикуляры из точки  $A$  на прямую  $B_1C_1$ , из  $B$  на  $A_1C_1$ , из  $C$  на  $A_1B_1$  пересекаются в одной точке. Докажите, что перпендикуляры из  $A_1$  на прямую  $BC$ , из  $B_1$  на  $AC$ , из  $C_1$  на  $AB$  тоже пересекаются в одной точке.

**25\*** Пусть в условиях предыдущей задачи вместо перпендикуляров из вершин  $\triangle ABC$  на стороны  $\triangle A_1B_1C_1$  опускаются наклонные под углом  $\alpha$ , а из вершин  $\triangle A_1B_1C_1$  на стороны  $\triangle ABC$  опускаются наклонные под углом  $180^\circ - \alpha$ .

Будем использовать обозначения задачи 13. Предположим дополнительно, что точки  $A_1, A_2, B_1, B_2, C_1, C_2$  лежат на одной окружности  $\mathcal{R}$  с центром  $R$ .

**26.** Докажите, что  $P$  и  $Q$  изогонально сопряжены в  $\triangle ABC$ .

**27.** Докажите, что:

- a)  $R \in \mathcal{N}$ .
- b)  $RN$  — диаметр  $\mathcal{N}$ .
- c)  $PR = QR$ .

**28.** Докажите, что в исходный треугольник можно вписать эллипс  $\mathcal{K}$  с фокусами  $P$  и  $Q$ .

**29.** Прямые  $PA'$  и  $QA'$  вторично пересекают  $\mathcal{R}$  в точках  $X$  и  $Y$ . Докажите, что  $XY$  касается  $\mathcal{K}$ .

**30.** Докажите, что  $\mathcal{K}$  касается  $\mathcal{R}$  тогда и только тогда, когда  $\mathcal{N}$  пересекается с  $\mathcal{R}$ , причем в этом случае точки касания совпадают с точками пересечения.

**31.** Докажите, что в треугольнике:

a) Точка Лемуана, две точки Брокара и центр описанной окружности образуют дельтоид с двумя прямыми углами.

b) Эллипс с фокусами в точках Брокара касается сторон в основаниях симедиан.

**32\*** Пусть прямые  $AA_1, BB_1, CC_1$  пересекаются в одной точке  $L$ . Докажите, что  $L$  лежит на радикальной оси  $\mathcal{N}$  и  $\mathcal{R}$ .

# Некоторые свойства конструкций Микеля.

## Решения

### Часть 1

1° Очевидно.

2° Пусть в один момент времени точки находятся в положениях  $A_1$  и  $C_1$ , а в другой — в положениях  $X$  и  $Y$  соответственно. Окружности  $(BC_1A_1)$  и  $(BXY)$  могут касаться или пересекаться вторично в точке  $G \neq B$ .

В первом случае существует гомотетия с центром  $B$ , переводящая окружность  $(BC_1A_1)$  в окружность  $(BXY)$ . Она переводит  $A_1$  в  $X$ , а  $C_1$  в  $Y$ . Следовательно,  $C_1A_1 \parallel XY$ . Рассмотрим третий момент, когда точки  $A_1$  и  $C_1$  находятся в положениях  $P$  и  $Q$  соответственно. Тогда  $\frac{A_1X}{A_1P} = \frac{C_1Y}{C_1Q}$ , значит,  $PQ \parallel A_1C_1$ . Следовательно, окружность  $(BPQ)$  касается окружности  $(BA_1C_1)$ , т.е. все окружности  $(BA_1C_1)$  касаются друг друга в точке  $B$ .

Во втором случае треугольники  $GXA_1$  и  $GYC_1$  подобны, поэтому  $\angle(GA_1, A_1B) = \angle(GC_1, C_1B)$  и  $\angle(GX, XB) = \angle(GY, YB)$ . Тогда существует поворотная гомотетия  $\phi$  с центром  $G$ , переводящая  $A_1$  в  $C_1$ , а  $X$  в  $Y$ . Вновь рассмотрим момент, когда точки  $A_1$  и  $C_1$  занимают положения  $P$  и  $Q$  соответственно. Тогда  $\phi(P) = Q$  и, значит,  $\angle(GP, PB) = \angle(GQ, QB)$ , т.е.  $G$  лежит на окружности  $(BPQ)$ .

3-4° Известные факты.

5° Обозначим точку пересечения прямых  $\ell_i$  и  $\ell_j$  через  $X_{ij}$ , а точку Микеля всех прямых, кроме  $\ell_i$ , через  $A_i$ . Достаточно доказать, что  $A_1, A_2, A_3$  и  $A_4$  лежат на одной окружности. Рассматривая окружности  $(A_1A_2X_{35}X_{45})$ ,  $(A_2A_3X_{15}X_{45})$ ,  $(A_3A_4X_{15}X_{25})$  и  $(A_4A_1X_{25}X_{35})$ , получаем:

$$\begin{aligned} \angle(A_1A_2, A_2A_3) &= \angle(A_1A_2, A_2X_{45}) + \angle(X_{45}A_2, A_2A_3) = \angle(A_1X_{35}, X_{35}X_{45}) + \angle(X_{45}X_{15}, X_{15}A_3) = \\ &= \angle(A_1X_{35}, X_{35}X_{25}) + \angle(X_{25}X_{15}, X_{15}A_3) = \angle(A_1A_4, A_4X_{25}) + \angle(X_{25}A_4, A_4A_3) = \angle(A_1A_4, A_4A_3). \end{aligned}$$

6° Приведем алгебраическое решение, годящееся для обоих пунктов. Геометрическое решение, в котором пункт а) проще пункта б), мы приведем после алгебраического.

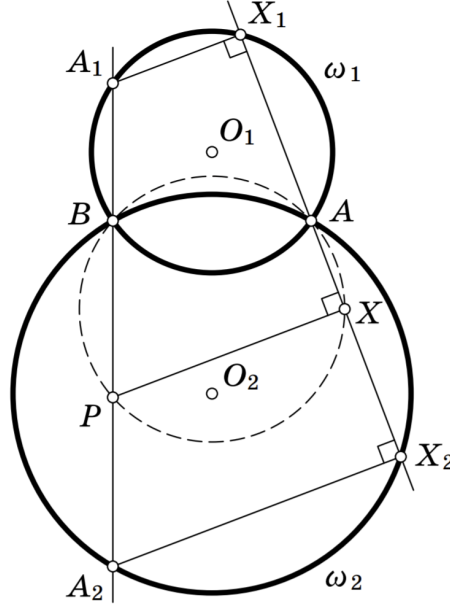
Пусть  $f(x, y) = 0$  и  $g(x, y) = 0$  — уравнения  $\mathcal{A}$  и  $\mathcal{B}$  соответственно в декартовых координатах, где  $f(x, y) = x^2 + y^2 + a_1x + a_2y + a_3$  и  $g(x, y) = x^2 + y^2 + b_1x + b_2y + b_3$ . Заметим, что степени точки  $(x, y)$  относительно  $\mathcal{A}$  и  $\mathcal{B}$  равны  $f(x, y)$  и  $g(x, y)$  соответственно. Поэтому искомое ГМТ задается уравнением  $f(x, y) = cg(x, y)$  для некоторой константы  $c$ . Легко видеть, что это уравнение задает прямую при  $c = 1$  и окружность  $\mathcal{C}$  при  $c \neq 1$ .

Пусть  $c \neq 1$ . Окружность  $\mathcal{C}$  задается уравнением  $\frac{f(x, y) - cg(x, y)}{1 - c} = 0$ . Пусть  $(p, q)$  — произвольная точка на радикальной оси окружностей  $\mathcal{A}$  и  $\mathcal{B}$ , т.е.  $f(p, q) = g(p, q)$ . Тогда степень точки  $(p, q)$  относительно окружности  $\mathcal{C}$  равна  $\frac{f(p, q) - cg(p, q)}{1 - c} = f(p, q) = g(p, q)$ . Следовательно,  $\mathcal{A}$ ,  $\mathcal{B}$  и  $\mathcal{C}$  соосны.

*Геометрическое решение, взятое из [1]:* Предположим, что окружности  $\mathcal{A}$  и  $\mathcal{B}$  пересекаются в точках  $A$  и  $B$ . Обозначим центры этих окружностей через  $O_1$  и  $O_2$  а их радиусы — через  $r_1$  и  $r_2$  соответственно. Точки, симметричные точке  $A$  относительно  $O_1$  и  $O_2$ , обозначим через  $A_1$  и  $A_2$ . Покажем, что множество таких точек  $X$ , что отношение их степеней относительно  $\omega_1$  и  $\omega_2$  равно  $k$ , — это окружность. Проведем прямую  $XA$ . Пусть она пересечет  $\omega_1$  и  $\omega_2$  в точках  $X_1$  и  $X_2$  соответственно. Тогда  $k$  будет равно  $\frac{XX_1}{XX_2}$  (взятому с нужным знаком). Поскольку  $AA_1$  и  $AA_2$  — диаметры соответствующих окружностей, углы  $AX_1A_1$  и  $AX_2A_2$  прямые, а значит,  $X_1$  и  $X_2$  — это проекции точек  $A_1$  и  $A_2$  на прямую  $AX$ . Возьмем на прямой  $A_1A_2$  такую точку  $P$ , что  $\frac{PA_1}{PA_2} = k$  (таких точек,



что это отношение равно  $|k|$ , будет две, надо выбрать ту, у которой «знак» соответствующий). Тогда по теореме Фалеса точка  $X$  будет проекцией точки  $P$  на прямую  $AX$ , а значит, она будет лежать на окружности с диаметром  $AP$ . Обратными рассуждениями легко показать, что для любой точки на этой окружности отношение степеней точек относительно  $\omega_1$  и  $\omega_2$  равно  $k$ .



Для того чтобы доказать это утверждение для непересекающихся окружностей, применим идею «выхода» в трехмерное пространство. Пусть даны две пересекающиеся сферы, пересекающие нашу плоскость по этим двум окружностям. Проводя аналогичные рассуждения, показываем, что геометрическим местом таких точек, что отношение их степеней относительно этих двух сфер равно  $k$ , есть сфера из этого пучка, то есть сфера, содержащая окружность пересечения этих двух сфер. Пересечение этой сферы с нашей плоскостью есть окружность из пучка, образованного окружностями  $\omega_1$  и  $\omega_2$ , а это и требовалось доказать.

**7°** Пусть  $X_b$  и  $Y_b$  — проекции  $X$  и  $Y$  соответственно на  $AC$ , а  $X_c$  и  $Y_c$  — проекции  $X$  и  $Y$  соответственно на  $AB$ . Так как  $X_b, Y_b, X_c$  и  $Y_c$  лежат на одной окружности,

$$\begin{aligned}\angle(BA, AX) &= \angle(X_cA, AX) = \angle(X_cX_b, X_bX) = \angle(X_cX_b, X_bY_b) + 90^\circ = \\ &= \angle(X_cY_c, Y_cY_b) + 90^\circ = \angle(YY_c, Y_cY_b) = \angle(YA, AY_b) = \angle(YA, AC)\end{aligned}$$

Аналогично  $\angle(AB, BX) = \angle(YB, BC)$ . Значит,  $X$  и  $Y$  изогонально сопряжены относительно  $\triangle ABC$ .

**8.** Пусть  $P$  — точка пересечения окружностей  $(AB_1C_1)$ ,  $(A_1BC_1)$ ,  $(A_1B_1C)$ . Заметим, что

$$\begin{aligned}\angle(MM_a, M_aP) &= \angle(AM_a, M_aP) = \angle(AB_1, B_1P) = \angle(CB_1, B_1P) = \\ &= \angle(CA_1, A_1P) = \angle(CM_c, M_cP) = \angle(MM_c, M_cP).\end{aligned}$$

Значит,  $M_c$  лежит на окружности  $(MPM_a)$ . Аналогично получаем, что  $M_b$  лежит на этой окружности.

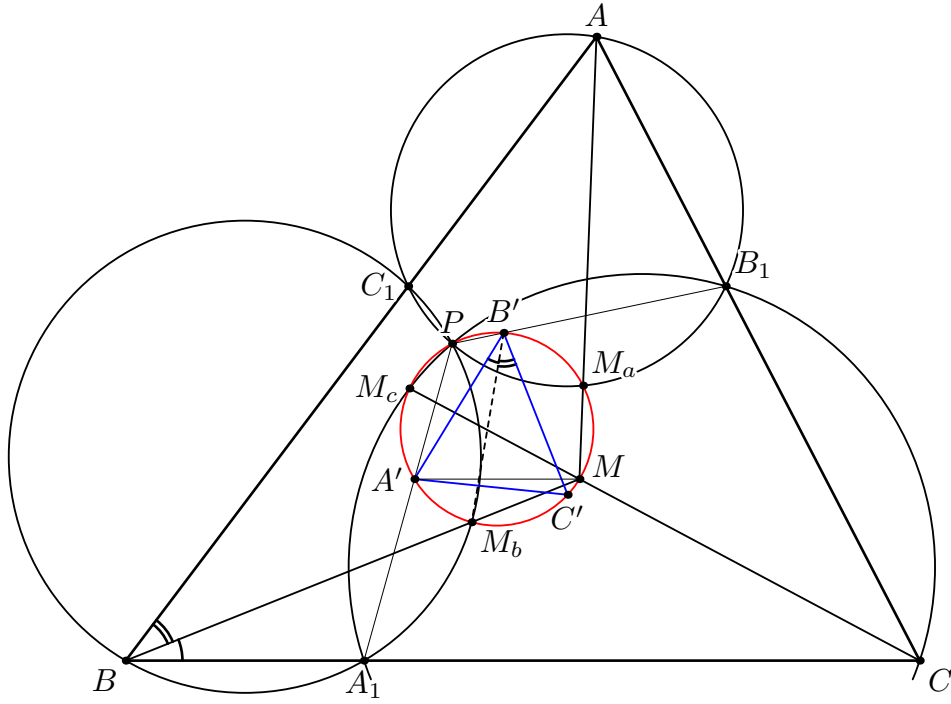
**9.** Из следующих равенств получаем, что  $MA' \parallel BC$ .

$$\angle(MA', A'P) = \angle(MM_c, M_cP) = \angle(CM_c, M_cP) = \angle(CA_1, A_1P) = \angle(BC, A'P),$$

**10.** Имеем

$$\angle(A'B', B'M_b) = \angle(A'M, MM_b) = \angle(CB, BM).$$

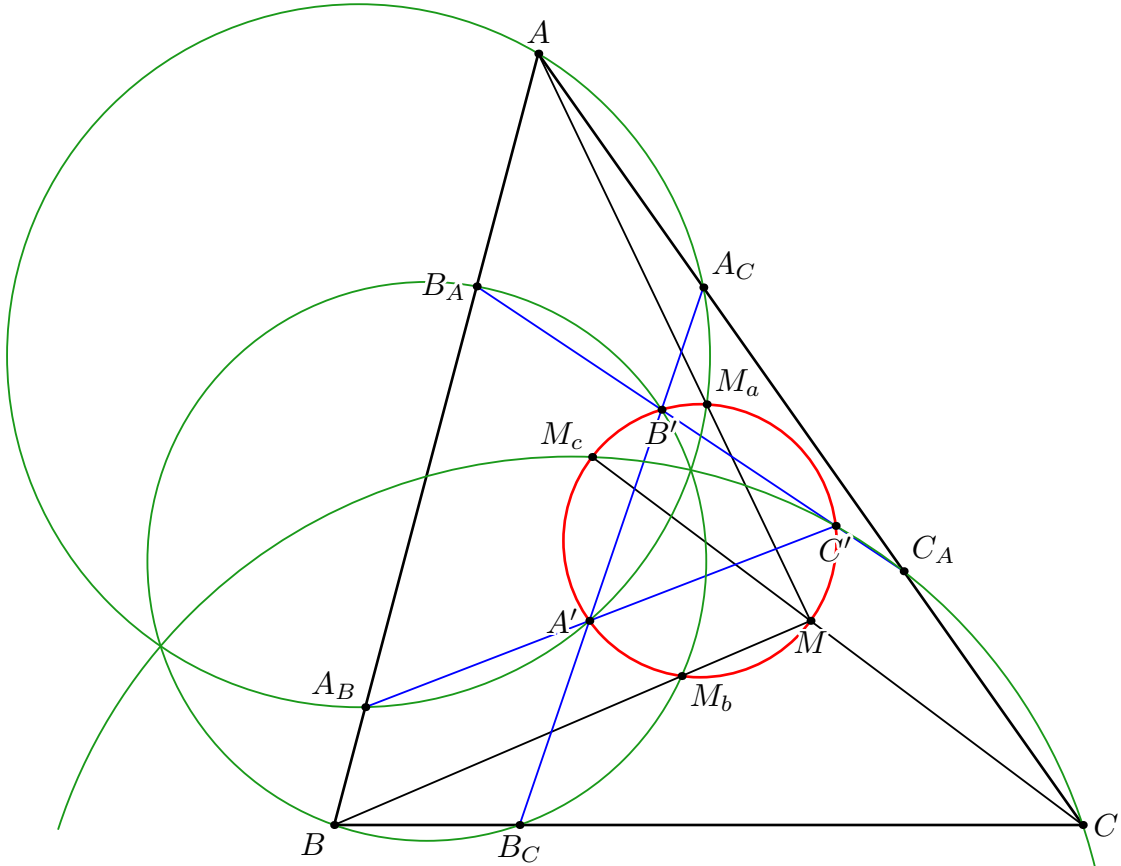
Аналогично  $\angle(C'B', B'M_b) = \angle(AB, BM)$  и т.д.. Поэтому треугольники  $ABC$  и  $A'B'C'$  подобны и противоположно ориентированы. Кроме того,  $A'M_a$ ,  $B'M_b$  и  $C'M_c$  проходят через точку, соответствующую изогонально сопряженной к  $M$  в  $\triangle ABC$ .



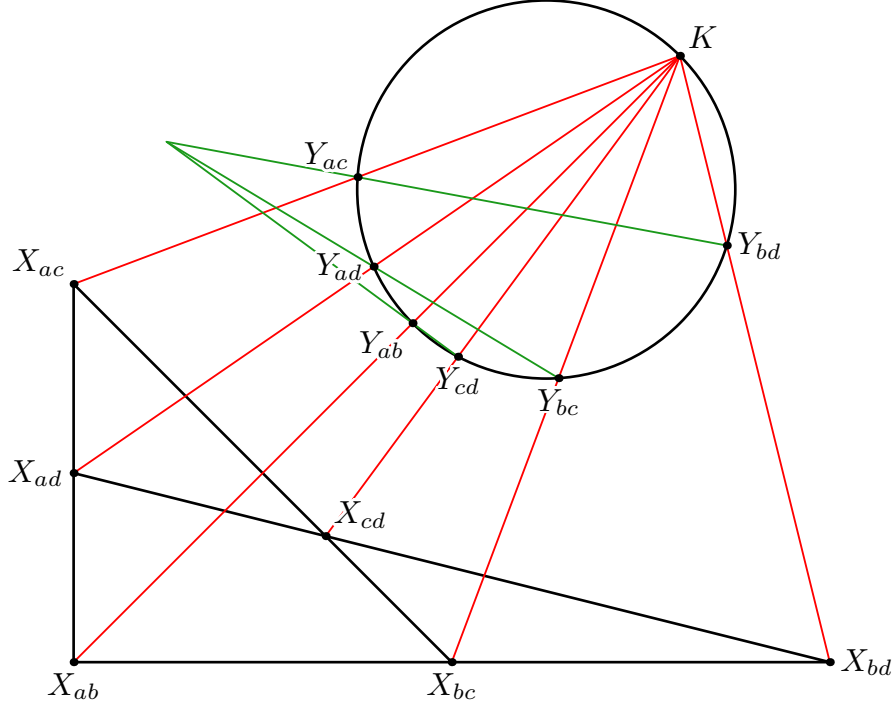
**11\*** Обозначим окружности  $(AM_aA')$ ,  $(BM_bB')$  и  $(CM_cC')$  через  $\omega_a$ ,  $\omega_b$  и  $\omega_c$  соответственно. Пусть  $A_B = AB \cap A'C'$ ,  $B_A = BA \cap B'C'$ ,  $A_C = AC \cap A'B'$ ,  $C_A = CA \cap C'B'$ ,  $B_C = BC \cap B'A'$ ,  $C_B = CB \cap C'A'$ . Подсчетом углов получаем, что  $\omega_a$  проходит через  $A_B$  и  $A_C$ . Аналогично  $B_A, B_C \in \omega_b$  и  $C_A, C_B \in \omega_c$ . Тогда

$$\frac{AB \cdot AB_A}{AC \cdot AC_A} = \frac{\sin \angle ACB \cdot \sin \angle AC_A B_A}{\sin \angle ABC \cdot \sin \angle AB_A C_A} = \frac{\sin \angle A_C C B_C \cdot \sin \angle A_C C_A B'}{\sin \angle A_C B' C_A \cdot \sin \angle A_C B_C C} = \frac{A_C B_C \cdot A_C B'}{A_C C_A \cdot A_C C},$$

значит, отношение степеней точки  $A$  относительно  $\omega_b$  и  $\omega_c$  равно отношению степеней точки  $A_C$  относительно этих окружностей. Такое же отношение степеней получаем для точки  $A_B$ . Осталось применить утверждение задачи 6.



**12\*** *Первое решение:* По теореме Дезарга об инволюции существует инволюция пучка прямых, проходящих через  $K$ , которая переставляет  $KY_{ab}$  с  $KY_{cd}$ ,  $KY_{ac}$  с  $KY_{bd}$  и  $KY_{ad}$  с  $KY_{bc}$ . Значит, существует инволюция на  $\mathcal{K}$ , переставляющая  $Y_{ab}$  с  $Y_{cd}$ ,  $Y_{ac}$  с  $Y_{bd}$  и  $Y_{ad}$  с  $Y_{bc}$ . Эта инволюция переводит каждую точку  $P \in \mathcal{K}$  во вторую точку пересечения прямой  $PU$  с  $\mathcal{K}$ , где  $U = Y_{ab}Y_{cd} \cap Y_{ac}Y_{bd}$ . Следовательно,  $Y_{ab}Y_{cd}$ ,  $Y_{ac}Y_{bd}$ ,  $Y_{ad}Y_{bc}$  пересекаются в одной точке.



*Второе решение:* (Мы игнорируем трудности, связанные с расположением точек.) Имеем

$$\begin{aligned} \frac{Y_{ab}Y_{ad}}{Y_{ad}Y_{ac}} \cdot \frac{Y_{ac}Y_{cd}}{Y_{cd}Y_{bc}} \cdot \frac{Y_{bc}Y_{bd}}{Y_{bd}Y_{ab}} &= \frac{\sin \angle Y_{ab}KY_{ad}}{\sin \angle Y_{ad}KY_{ac}} \cdot \frac{\sin \angle Y_{ac}KY_{cd}}{\sin \angle Y_{cd}KY_{bc}} \cdot \frac{\sin \angle Y_{bc}KY_{bd}}{\sin \angle Y_{bd}KY_{ab}} = \\ &= \frac{\sin \angle X_{ab}KX_{ad}}{\sin \angle X_{ad}KX_{ac}} \cdot \frac{\sin \angle X_{ac}KX_{cd}}{\sin \angle X_{cd}KX_{bc}} \cdot \frac{\sin \angle X_{bc}KX_{bd}}{\sin \angle X_{bd}KX_{ab}} = \frac{X_{ab}X_{ad}/KX_{ab}}{X_{ad}X_{ac}/KX_{ac}} \cdot \frac{X_{ac}X_{cd}/KX_{ac}}{X_{cd}X_{bc}/KX_{bc}} \cdot \frac{X_{bc}X_{bd}/KX_{bc}}{X_{bd}X_{ab}/KX_{ab}} = \\ &= \frac{X_{ab}X_{ad}}{X_{ad}X_{ac}} \cdot \frac{X_{ac}X_{cd}}{X_{cd}X_{bc}} \cdot \frac{X_{bc}X_{bd}}{X_{bd}X_{ab}} = 1 \end{aligned}$$

Утверждение задачи теперь следует из тригонометрической теоремы Чевы для треугольника  $Y_{ab}Y_{ac}Y_{ad}$ .

**13.** Заметим, что  $N_c$  является точкой Микеля для  $AC$ ,  $BC$ ,  $A_1B_1$  и  $A_2B_2$ , а значит является второй точкой пересечения окружностей  $(A_1B_1C)$  и  $(A_2B_2C)$ .

a) Следует из тригонометрической теоремы Чевы для треугольника  $ABC$ , поскольку

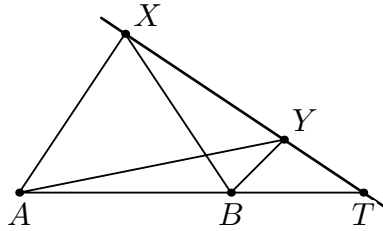
$$\frac{\sin \angle BCN_c}{\sin \angle ACN_c} = \frac{A_1A_2}{B_1B_2}, \quad \frac{\sin \angle CAN_a}{\sin \angle BAN_a} = \frac{B_1B_2}{C_1C_2}, \quad \frac{\sin \angle ABN_b}{\sin \angle CBN_b} = \frac{C_1C_2}{A_1A_2}.$$

b) Следует из задачи 8 для треугольника  $ABC$ , точек  $A_1$ ,  $B_1$ ,  $C_1$  на сторонах и точки  $N$ .

c) В решении задачи 8 доказано, что точка  $P$  пересечения трёх окружностей также лежит на окружности  $\mathcal{N}$ . Отсюда следует утверждение задачи.

d) Пусть  $A'$  — точка на  $\mathcal{N}$ , такая что  $NA' \parallel BC$ . Из задачи 9 следует, что  $PA_1$  и  $QA_2$  пересекаются в  $A'$ .

14. а) Можно считать, что точки  $A$  и  $B$  лежат по разные стороны от прямой (в противном случае отразим точку  $B$  относительно прямой). Теперь очевидно, что минимум достигается когда  $X$ ,  $A$  и  $B$  лежат на одной прямой. А на двух лучах функция  $f$  монотонно возрастает, что следует из неравенства треугольника.



б) Можно считать, что точки  $A$  и  $B$  лежат по одну сторону от прямой (в противном случае отразим точку  $B$  относительно прямой). Из неравенства треугольника следует, что экстремум достигается когда точки  $A$ ,  $B$  и  $X$  лежат на одной прямой (это положение точки  $X$  обозначим через  $T$ ). Чтобы доказать, что на двух лучах функция монотонно убывает, сделаем следующее. Пусть точка  $A$  дальше от прямой чем  $B$ . Рассмотрим две разных точки  $X$  и  $Y$  на прямой (см. рис.). Для того, чтобы доказать монотонность функции  $f$ , надо доказать, что  $XA - XB < YA - YB$ . Перепишем это как  $XA + YB < XB + YA$ , а это верно, потому что сумма диагоналей в четырехугольнике больше чем сумма двух противоположных сторон.

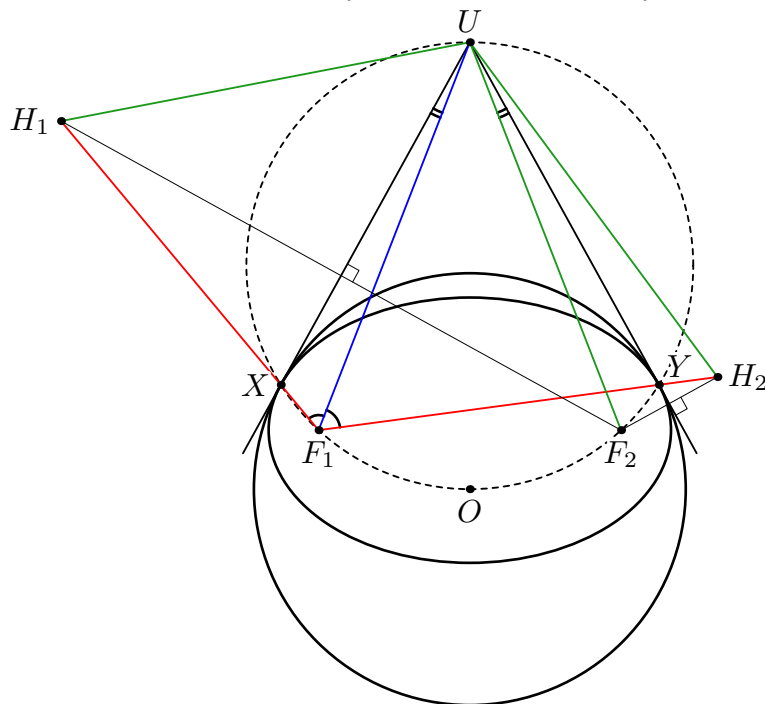
15° Зафиксируем  $B'$ ,  $C'$  и будем двигать  $A'$ . Так как сумма  $B'A' + A'C'$  минимальна,  $BC$  — внешняя биссектриса угла  $B'A'C'$ . Аналогично  $AC$  и  $AB$  — внешние биссектрисы углов  $A'B'C'$  и  $A'C'B'$  соответственно. Поэтому  $A$ ,  $B$  и  $C$  — центры вневписанных окружностей треугольника  $A'B'C'$ , а  $AA'$ ,  $BB'$ ,  $CC'$  — высоты треугольника  $ABC$ .

16)<sup>(</sup> См. [1], Теорема 1.1 и обсуждение после ее доказательства.

17)<sup>(</sup> См. [1], Теорема 1.3 и обсуждение после ее доказательства.

18)<sup>(</sup> Пусть  $\mathcal{K}$  — эллипс,  $G$  — его второй фокус, а  $M$  — середина  $FG$ . Пусть точка  $A$  симметрична  $F$  относительно  $\ell$ , а  $B = \ell \cap \mathcal{K}$ . Тогда  $MP = GA/2 = (FB + BG)/2$  постоянно, т.е.  $P$  движется по окружности с центром  $M$ , касающейся  $\mathcal{K}$ .

19. а) б) Проведем касательные к эллипсу в точках  $X$  и  $Y$ . Пусть они пересеклись в точке  $U$ .



Давайте докажем вспомогательный факт — биссектриса угла  $XF_1Y$  проходит через точку  $U$ . Для этого отражаем точку  $F_2$  относительно обеих касательных и получаем точки  $H_1$  и  $H_2$ . Тогда треугольники  $UH_1F_1$  и  $UH_2F_1$  равны по трем сторонам. Отсюда  $\angle XF_1U = \angle YF_1U$ .

Мы получаем, что через точку  $U$  проходит и биссектриса угла  $XF_1Y$  (и аналогично угла  $XF_2Y$ ), а также серединный перпендикуляр к  $XY$  (т.к. касательные равны). Тогда точки  $X, F_1, F_2, Y$  и  $U$  лежат на одной окружности. Так как  $XOYU$  вписан, то точка  $O$  тоже лежит на этой окружности.  $XO$  является биссектрисой угла  $F_1XF_2$  (так как это перпендикуляр к касательной к эллипсу), а значит  $F_1O = OF_2$ .

с)<sup>1)</sup> По задаче 18 ГМТ проекций фокуса  $F_1$  на касательные к эллипсу — окружность. Применяя поворотную гомотеию с центром  $F_1$ , углом поворота  $\pi/2 - \alpha$  и коэффициентом  $1/\sin \alpha$ , получаем, что ГМТ  $P$  таких, что направленный угол между  $PF_1$  и касательной к эллипсу из  $P$  равен  $\alpha$ , тоже будет окружностью. При  $\alpha = \angle YXU$  это ГМТ будет окружностью  $\omega$ .

д) В соответствии с предыдущим пунктом  $\omega$  можно определить как ГМТ  $P$  таких, что направленный угол между  $PF_1$  и касательной к эллипсу из  $P$  равен данному углу  $\alpha$ .

**Примечание.** Если окружности  $OF_1F_2$  и  $\omega$  не пересекаются, точки касания  $\mathcal{K}$  и  $\omega$  не будут существовать на обычной плоскости (при желании можно рассмотреть комплексные точки касания).

е) Пусть перпендикуляр к  $OF_1$  в точке  $F_1$  пересекает  $\omega$  в точке  $U_1$ ,  $Z'$  — проекция  $U_1$  на прямую  $OZ$ . Тогда точки  $F_1$  и  $Z'$  лежат на окружности с диаметром  $OU_1$ , касающейся  $\omega$ . При этом  $\angle(F_1U_1, U_1Z') = \angle(F_1O, OU) = \angle(F_1X, XU)$ , поскольку  $U_1Z'OF_1$  и  $F_1XOU$  вписаны. Следовательно,  $U_1Z$  касается  $\mathcal{K}$  (так как окружность  $\omega$  — геометрическое место точек, таких что угол между касательной и отрезком в фокус постоянен) и  $Z'$  совпадает с  $Z$ .

ф) Вытекает из следующей леммы, обобщающей утверждение предыдущего пункта (с помощью поворотной гомотеии с центром в точке  $F_1$ ).

**Лемма.** Пусть  $P$  — произвольная точка эллипса  $\mathcal{K}$ , касательная к  $\mathcal{K}$  в точке  $P$  пересекает  $\omega$  в точках  $A$  и  $B$ . Тогда окружность  $APF_1$  касается  $\omega$ .

g)<sup>\*</sup> Из п. е) следует, что точки  $Z$  и  $T$  являются проекциями на прямую  $AB$  концов хорды  $\omega$  с серединой  $F_1$ . Поэтому можно в двойных отношениях заменить  $Z$  и  $T$  на концы этой хорды, а  $A$  и  $B$  на точки пересечения касательных в этих точках с прямой  $UF_1$ . Если  $U$  лежит вне окружности, сделаем проективное преобразование, сохраняющее окружность переводящее  $U$  в бесконечную точку. Если же  $U$  внутри окружности, сделаем проективное преобразование, переводящее  $U$  в центр. В обоих случаях утверждение задачи станет очевидно.

h) Непосредственно следует из предыдущего. (Про модели плоскости Лобачевского можно прочитать в [2].)

20)<sup>1)</sup> Пусть  $F_1$  и  $F_2$  — фокусы эллипса, причем  $F_1$  ближе к  $Y$ , чем  $F_2$ . Из задачи 19с следует, что треугольники  $F_1A_1B_1$  и  $F_2A_2B_2$  подобны по двум углам. Пусть  $S = A_1B_1 \cap A_2B_2$ . Из оптического свойства эллипса  $\angle A_1SF_1 = \angle A_2SF_2$ . Поэтому существует композиция гомотеии с центром  $S$  и симметрии относительно биссектрисы угла  $A_1SA_2$ , переводящая треугольник  $A_1F_1B_1$  в треугольник  $A_2F_2B_2$ . Значит,  $\frac{A_1S}{A_2S} = \frac{B_1S}{B_2S}$ , откуда  $A_1A_2 \parallel B_1B_2$ .

21<sup>\*</sup> Пусть  $O$  — центр поворотной гомотеии, при которой одна из данных окружностей переходит в другую, а точка  $N$  в  $M$ . Так как все треугольники  $ONM$  подобны друг другу, проекция  $N$  точки  $O$  на прямую  $MN$  будет двигаться по некоторой окружности  $\omega$ . Таким образом задачу можно переформулировать так: даны окружность  $\omega$  и точка  $O$ , найти огибающую прямых, проходящих через произвольную точку  $H \in \omega$  и перпендикулярных  $OH$ .

Если  $O$  лежит на  $\omega$ , то все такие прямые проходят через диаметрально противоположную точку. В противном случае огибающая будет коникой с фокусом  $O$  — эллипсом, если  $O$  лежит внутри  $\omega$ , и гиперболой, если вне. (Это несложно вывести из задачи 18 обратным ходом.)

22<sup>\*</sup> **Ответ:** Парабола, касающаяся данных прямых.

**Доказательство.** Пусть  $A$  и  $B$  — точки,двигающиеся линейно по двум данным прямым, а эти две прямые пересекаются в точке  $X$ . Рассмотрим точку  $F$ , отличную от  $X$ , через которую проходят все окружности  $(ABX)$  (такая существует по лемме о воробьях, если  $A$  и  $B$  в разные моменты времени

проезжают через  $X$ . Если  $AB$  одинаковые, то  $AB$  остаётся параллельна сама себе и огибающей не существует). Точка Микеля четырёх прямых является фокусом параболы, касающейся этих четырёх прямых (см. [1], Теорема 4.10). Поэтому искомая огибающая — парабола с фокусом  $F$ , касающаяся двух данных прямых.

**23)<sup>(</sup>** **Ответ:** Окружность, проходящая через точки пересечения данных, являющаяся окружностью Аполлония для их центров.

### Часть 3

**24°** Оба условия эквивалентны равенству  $AB_1^2 + BC_1^2 + CA_1^2 = BA_1^2 + AC_1^2 + CB_1^2$ .

**25\*** По условию существует точка  $P$ , такая что  $\angle(AP, B_1C_1) = \angle(BP, A_1C_1) = \angle(CP, A_1B_1) = \alpha$ . Пусть  $A_2B_2C_2$  — образ треугольника  $ABC$  при повороте вокруг  $P$  на угол  $\alpha - 90^\circ$ . Тогда  $A_1B_1C_1$  и  $A_2B_2C_2$  ортогональны, значит существует точка  $Q$  такая, что  $A_1Q \perp B_2C_2$ ,  $B_1Q \perp A_2C_2$  и  $C_1Q \perp A_2B_2$ . Так как  $\angle(BC, B_2C_2) = \alpha - 90^\circ$ , получаем  $\angle(A_1Q, BC) = \angle(A_1Q, B_2C_2) - \angle(BC, B_2C_2) = -\alpha$ . Аналогично  $\angle(B_1Q, AC) = \angle(C_1Q, AB) = -\alpha$ , что и требовалось.

Ниже приводим набросок еще одного решения, не использующего задачу 24.

Скажем, что тройка прямых  $a', b', c'$  гармонична тройке прямых  $a, b, c$ , если в треугольнике со сторонами, параллельными  $a, b, c$ , соответствующие чевианы, параллельные  $a', b', c'$ , конкурентны.

*Лемма.* Отношение 'быть гармоничным' симметрично, т.е. если тройка  $a', b', c'$  гармонична тройке  $a, b, c$ , то  $a, b, c$  гармонична  $a', b', c'$ .

*Доказательство.* Пусть  $\ell$  — прямая. Через точку  $O$ , не лежащую на  $\ell$ , проведем прямые, параллельные  $a, b, c, a', b', c'$ . Пусть эти прямые пересекают  $\ell$  в точках  $A, B, C, A', B', C'$  соответственно. Используя синусную теорему Чевы, перепишем условие гармоничности тройки  $a', b', c'$  тройке  $a, b, c$  в виде

$$\frac{\overrightarrow{AB'}}{\overrightarrow{B'C'}} \cdot \frac{\overrightarrow{CA'}}{\overrightarrow{A'B}} \cdot \frac{\overrightarrow{BC'}}{\overrightarrow{C'A}} = -1.$$

Легко видеть, что это условие сохраняется при замене  $a, b, c$  на  $a', b', c'$ . Лемма доказана.

Пусть  $a, b, c$  и  $a', b', c'$  — прямые, содержащие стороны треугольников  $ABC$  и  $A_1B_1C_1$ . Через  $t_\varphi$  обозначаем прямую, получаемую из  $t$  поворотом на угол  $\varphi$ . Условие задачи означает, что тройка  $a, b, c$  гармонична  $a'_\varphi, b'_\varphi, c'_\varphi$ . Выполним поворот на  $-\varphi$ , получаем, что  $a_{-\varphi}, b_{-\varphi}, c_{-\varphi}$  гармонична  $a', b', c'$ , откуда и следует нужное утверждение.

Используем обозначения из задачи 13. Дополнительно предполагаем, что точки  $A_1, A_2, B_1, B_2, C_1, C_2$  лежат на одной окружности  $\mathcal{R}$  с центром  $R$ .

**26.** (*Косопедальные треугольники*) Пусть  $P'$  изогонально сопряжена точке  $P$ . Пусть  $P_a, P_b, P_c$  — проекции  $P$  на  $BC, CA, AB$  соответственно; аналогично обозначим проекции точки  $P'$ . Мы знаем, что середина  $R_0$  отрезка  $PP'$  является центром окружности  $(P_aP_bP_c) = (P'_aP'_bP'_c)$ . Положим  $\angle(PA_1, CA_1) = \angle(PB_1, AB_1) = \angle(PC_1, BC_1) = \varphi$ . Пусть  $R_1$  — центр окружности  $(A_1B_1C_1)$ . Треугольник  $P_aP_bP_c$  переходит в  $A_1B_1C_1$  при поворотной гомотетии с центром  $P$ , отсюда  $PP_aA_1 \sim PR_0R_1$ , значит  $R_1$  — точка на серединном перпендикуляре к  $PP'$  такая, что  $\angle(PR_1, R_1R_0) = \varphi$ . Отсюда  $\angle(R_1R_0, R_1P') = \varphi$ . Рассмотрим поворотную гомотетию с центром  $P'$ , переводящую  $R_0$  в  $R_1$ . Она переводит  $P'_aP'_bP'_c$  в некоторый треугольник  $A'_2B'_2C'_2$  такой, что  $P'R_0R_1 \sim P'P'_aA'_2 \sim P'P'_bB'_2 \sim P'P'_cC'_2$ , таким образом,  $A'_2, B'_2, C'_2$  — точки на прямых  $BC, CA, AB$  такие, что  $\angle(P'A'_2, CA'_2) = \angle(P'B'_2, AB'_2) = \angle(P'C'_2, BC'_2) = -\varphi$ . Так как  $R_0$  — центр окружности  $(P'_aP'_bP'_c)$ , то  $R_1$  — центр окружности  $(A'_2B'_2C'_2)$ . Радиусы окружностей  $(A_1B_1C_1)$  и  $(A'_2B'_2C'_2)$  оба равны  $R(P_aP_bP_c)/\sin \varphi$ , значит, эти окружности совпадают. Отсюда следует, что  $A'_2 = A_2, B'_2 = B_2, C'_2 = C_2, Q = P'$  и  $R_1 = R$ .

В дополнение, заметим, что треугольники  $ABC$  и  $A_1B_1C_1$  удовлетворяют условию задачи 25, с  $P$  и  $Q$  в качестве точек пересечения.

**27.** Из решения предыдущей задачи:  $\angle(PR, QR) = 2\varphi = \angle(PA_1, QA_2)$ . Из задачи 13 получаем  $A' = PA_1 \cap QA_2 \in \mathcal{N}$ , откуда  $R \in \mathcal{N}$ .

Заметим, что  $\angle(PN_c, N_cN) = \angle(PN_c, N_cC) = \angle(PA_1, A_1C) = \varphi$ . Аналогично  $\angle(QN_b, N_bN) = -\varphi$ . Это означает, что дуги  $NP$  и  $NQ$  окружности  $\mathcal{N}$  равны. Равенство  $PR = QR$  следует из решения задачи 26. Таким образом,  $RN$  — серединный перпендикуляр к  $PQ$ , т.е.  $RN$  — диаметр окружности  $\mathcal{N}$ .

**28.** Пусть  $Q_a, Q_b$  и  $Q_c$  симметричны  $Q$  относительно  $BC, CA$  и  $AB$  соответственно. Пусть  $PQ_a, PQ_b, PQ_c$  пересекают  $BC, CA, AB$  в точках  $A^*, B^*, C^*$  соответственно. Тогда  $P$  является центром окружности  $(Q_aQ_bQ_c)$ , отсюда  $PA^* + QA^* = PB^* + QB^* = PC^* + QC^*$ . Таким образом, существует эллипс с фокусами  $P$  и  $Q$ , проходящий через  $A^*, B^*, C^*$ . Он касается сторон треугольника  $\triangle ABC$ , согласно задаче 16.

**29.** Так как  $\angle(PA_1, BC) = \angle(BC, QA_2) = \varphi$ , и  $A_1A_2YX$  вписан в  $\mathcal{R}$ , то  $A_1A_2YX$  симметричен относительно общего серединного перпендикуляра к отрезкам  $XY$  и  $A_1A_2$  (в частности,  $XY \parallel A_1A_2$ ). Чтобы доказать, что  $XY$  касается  $\mathcal{K}$ , достаточно показать, что центр  $\mathcal{K}$  (т.е. середина  $PQ$ ) лежит на средней линии трапеции  $A_1A_2YX$  или, эквивалентно, показать, что  $PA_1 = QY$ . Из доказанного ранее мы знаем, что  $\angle(PR, QR) = 2\varphi$  и  $RP = RQ$ . Так как  $\angle(A_1R, RY) = 2\angle(A_1A_2, A_2Y) = 2\varphi$ , имеем  $\angle(PR, A_1R) = \angle(QR, YR)$ , и по первому признаку равенства, треугольники  $PRA_1$  и  $QRY$  равны. Так, нужное равенство  $PA_1 = QY$  доказано.

**30.** Для окружности  $\mathcal{R}$ , точки  $P$  и угла  $\varphi$  рассмотрим *эллипс Брокара*, т.е. огибающую образов прямых  $PZ$  после поворота на  $\varphi$  вокруг  $Z \in \mathcal{R}$  (см. обратное утверждение к задаче 19с). Для шести положений точки  $Z$  ( $A_1$  и  $X$  из задачи 29 и три аналогичные пары) соответствующие касательные к эллипсу Брокара также касаются  $\mathcal{K}$ . Значит,  $\mathcal{K}$  совпадает с этим эллипсом Брокара. Теперь нужное нам утверждение следует из утверждения, обратного к задаче 19b.

**31. а)** Сведем задачу к общему случаю, рассмотренному в задачах 26-27 (косопедальные треугольники).

Если  $P$  и  $Q$  — точки Брокара, то  $ABC$  — частный случай косопедального треугольника, для которого  $B = A_1$ ,  $C = B_1$ ,  $A = C_1$  и  $B = C_2$ ,  $C = A_2$ ,  $A = B_2$ . Так, в этом случае  $O = R$ , значит  $PO = OQ$  и  $\angle(PO, OQ) = 2\varphi$ , где  $90^\circ - \varphi$  — угол Брокара.

Пусть  $L$  — точка Лемуана. Достаточно доказать, что точка  $N$  из задачи 27 лежит на  $AL$ , или, эквивалентно,  $N_a$  лежит на симедиане  $\triangle ABC$  из вершины  $A$ . Мы знаем, что окружности  $(AN_aC)$  и  $(AN_aB)$  касаются  $AB$  и  $AC$  соответственно. Пусть  $V$  изогонально сопряжена  $N_a$  в  $\triangle ABC$ . Легко видеть, что окружности  $(AVC)$  и  $(AVB)$  касаются  $BC$ , откуда  $V$  лежит на медиане  $\triangle ABC$  из вершины  $A$ , что и требовалось.

В решении выше  $N = L$  и  $R = O$ . Ниже мы приведем другое расположение точек, при котором  $N = O$  и  $R = L$ .

Проведем через  $L$  прямую  $B_2C_1$  ( $B_2 \in AC$ ,  $C_1 \in AB$ ) так, что  $B, C, B_2, C_1$  лежат на одной окружности.

Из подобия  $ABC \sim AB_2C_1$  следует, что  $AL$  — медиана в треугольнике  $AB_2C_1$ , откуда  $B_2L = C_1L$ . Аналогично строим  $C_2A_1$ ,  $A_2B_1$ . Имеем  $\angle(LB_2, AC) = \angle(AB, BC) = \angle(AC, LB_1)$ . Следовательно  $LB_2 = LB_1$ . Таким образом, все 6 отрезков  $LA_1, LA_2, LB_1, LB_2, LC_1, LC_2$  равны, и  $A_1, A_2, B_1, B_2, C_1, C_2$  лежат на одной окружности (известной как окружность Тэйлора) с центром  $R = L$ . Теперь покажем, что точки  $P$  и  $Q$  (определенные как в общей конструкции задачи 26) являются точками Брокара. (Отметим, что  $LP = LQ$ ). Так как  $LA_1 = LA_2 = LC_2$ , имеем  $A_2C_2 \perp BC$ . Аналогично  $B_2A_2 \perp CA$  и  $C_2B_2 \perp AB$ . Далее, из окружностей  $(AB_2C_2Q)$ ,  $(BC_2A_2Q)$ ,  $(CA_2B_2Q)$  имеем:

$$y = \angle(C_2A_2, A_2Q) = \angle(C_2B, BQ) = 90^\circ - \angle(QC_2, C_2B) = \angle(B_2C_2, C_2Q) = \angle(B_2A, AQ)$$

и аналогично,  $y = \angle(A_2C, CQ)$ . Это означает, что  $Q$  — точка Брокара (с углом Брокара  $y$ ), и  $(A_2B_2C_2)$  — ее косопедальная окружность, отвечающая углу  $\varphi = \angle(QC_2, AB) = 90^\circ - y$ . Следовательно  $\angle(PL, LQ) = 2\varphi$ . Таким образом,  $P, Q, L, O$  лежат на окружности, при этом  $P$  и  $Q$  симметричны относительно  $OL$ .

**б)** Пусть  $AS$  — симедиана, так что  $BS : CS = c^2 : b^2$ . Достаточно доказать, что  $\triangle PBS \sim \triangle QCS$ , или  $PB : QC = c^2 : b^2$ ; откуда последует, что  $\angle(PS, SB) = \angle(CS, SQ)$ .

Из теоремы синусов

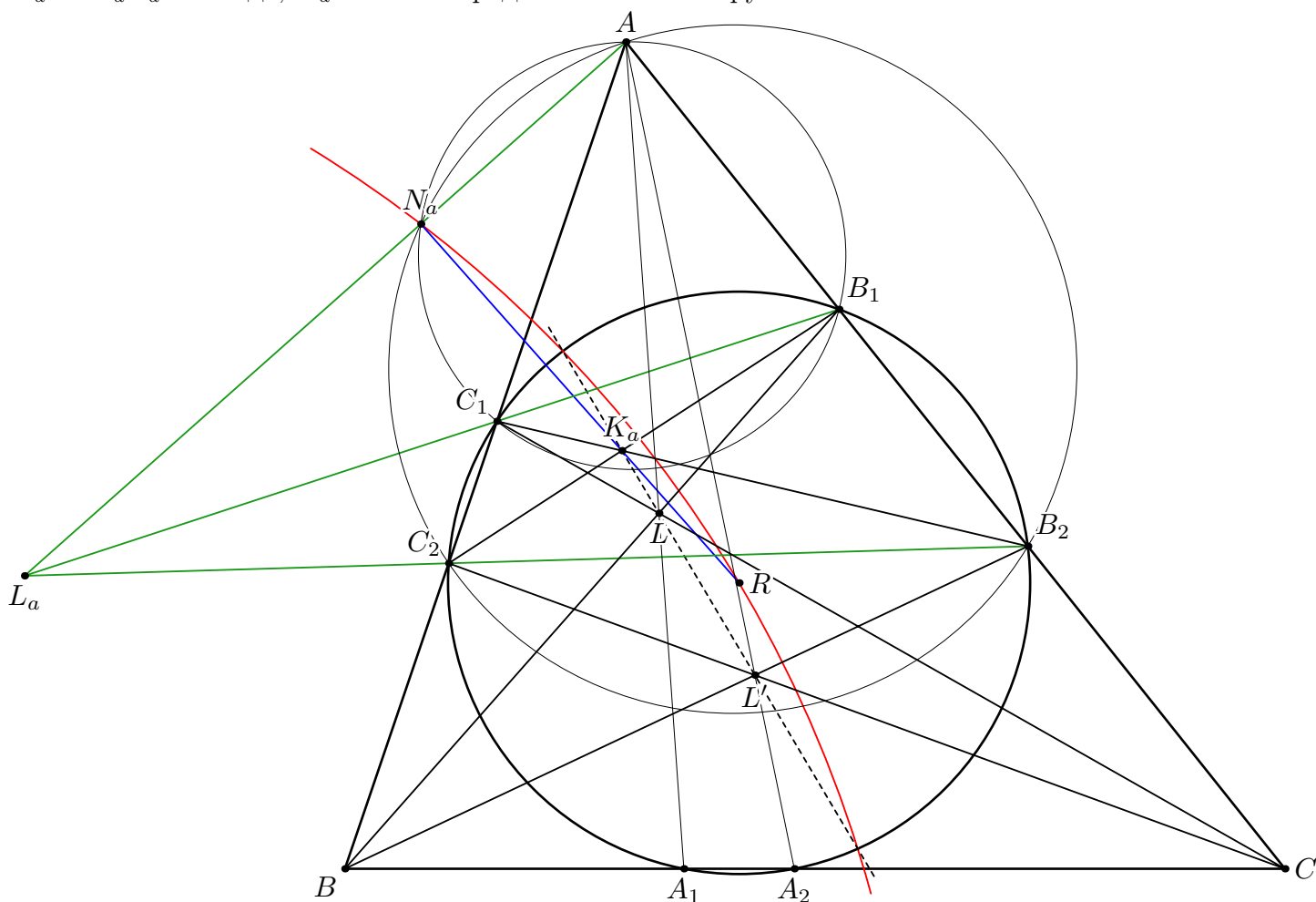
$$\frac{PB}{\sin y} = \frac{c}{\sin APB} = \frac{c}{\sin B} \quad \text{и} \quad \frac{QC}{\sin y} = \frac{b}{\sin C}.$$

Разделив одно равенство на другое, с учетом теоремы синусов для  $\triangle ABC$ , получаем нужное соотношение.

**32\*** Несложно видеть, что  $AA_2$ ,  $BB_2$  и  $CC_2$  пересекаются в какой-то точке  $L'$ . Пусть  $K_a = B_1C_2 \cap B_2C_1$ , точки  $K_b$  и  $K_c$  определим аналогично. По теореме Паппа, точки  $L$ ,  $L'$  и  $K_a$  лежат на одной прямой. Достаточно доказать, что  $K_a$  лежит на радикальной оси окружностей  $\mathcal{R}$  и  $\mathcal{N}$  (аналогичные



рассуждения тогда покажут, что  $K_b$  и  $K_c$  также лежат на этой радикальной оси). Прямые  $B_1C_1$ ,  $B_2C_2$  и  $AN_a$  конкурентны, поскольку они являются радикальными осями окружностей  $(AB_1C_1N_a)$ ,  $(AB_2C_2N_a)$  и  $\mathcal{R}$ . Так,  $AN_aL_aN$  — полярная точка  $K_a$  относительно окружности  $\mathcal{R}$ . Более того,  $N_a \in \mathcal{N}$  и  $NR$  — диаметр  $\mathcal{N}$ , следовательно  $RN_a \perp AN_a$ . Таким образом, инверсия относительно  $\mathcal{R}$  переводит  $K_a$  в  $N_a$ . Эта инверсия переводит прямую  $B_2C_1K_a$  в окружность  $RB_2C_1N_a$ . Следовательно,  $K_aC_1 \cdot K_aB_2 = K_aR \cdot K_aN_a$ . Отсюда,  $K_a$  лежит на радикальной оси окружностей  $\mathcal{R}$  и  $\mathcal{N}$ .



## Список литературы

- [1] А.В.Акопян, А.А.Заславский, *Геометрические свойства кривых второго порядка*. М.: МЦНМО. 2011
- [2] В.В.Прасолов, *Геометрия Лобачевского*. М.: МЦНМО. 2004

По всем вопросам, а также по всем опечаткам, недоработкам и неточностям просьба сообщать Иванову К. С. по адресу [ronyboss3@gmail.com](mailto:ronyboss3@gmail.com).

## Some features of Miquel's structures.

The project is presented by Konstantin Ivanov with the active participation of Ivan Frolov. Idea: Pavel Dolgirev. Special thanks to Alexander Skutin for formulating problems 20-23. With the support of Alexey Zaslavsky, Oleg Zaslavsky and Pavel Kozevnikov.

The symbol  $^\circ$  denotes some well-known facts, without which, however, the solution of further problems will be difficult. An asterisk  $*$  indicates a problem that is suspected to be difficult.

### Part 1

**1 $^\circ$**  (*Miquel's theorem*) In a triangle  $ABC$ , points  $C_1, A_1, B_1$  are chosen on the sides  $AB, BC, CA$ , respectively. Prove that the circumcircles of  $\triangle AB_1C_1, \triangle A_1BC_1, \triangle A_1B_1C$  have a common point.

**2 $^\circ$**  Let an angle  $ABC$  be given. Points  $C_1, A_1$  move along the lines  $AB, BC$  with constant (not necessarily equal) speeds. Prove that all circles  $BC_1A_1$  pass through another fixed point other than  $B$ . When is it wrong?

**3 $^\circ$**  (*Trigonometric form of Ceva's theorem*) In a triangle  $ABC$ , points  $C_1, A_1, B_1$  are chosen on the sides  $AB, BC, CA$ , respectively. Prove that lines  $AA_1, BB_1, CC_1$  meet at one point or are parallel if and only if

$$\frac{\sin \angle ABB_1 \cdot \sin \angle BCC_1 \cdot \sin \angle CAA_1}{\sin \angle B_1BC \cdot \sin \angle C_1CA \cdot \sin \angle A_1AB} = 1$$

**4 $^\circ$**  (*Miquel's point*) Let  $\ell_1, \ell_2, \ell_3$ , and  $\ell_4$  be four lines in general position. Excluding one line, one gets three lines forming a triangle, four triangles in total. Prove that the circumcircles of these four triangles have a common point.

**5 $^\circ$**  (*Miquel's circle*) Let  $\ell_1, \dots, \ell_5$  be 5 lines in general position. Prove that Miquel's points of all five possible quadruples of these lines are concyclic.

**6 $^\circ$**  Given two circles  $\mathcal{A}, \mathcal{B}$ . Prove that the locus of points  $X$  such that

$$\frac{\text{power of } X \text{ with respect to } \mathcal{A}}{\text{power of } X \text{ with respect to } \mathcal{B}} = \text{const}$$

is a circle, in the case

- a) when  $\mathcal{A}, \mathcal{B}$  intersect
- b) for arbitrary position  $\mathcal{A}$  and  $\mathcal{B}$ .

**7 $^\circ$**  In a triangle  $ABC$ , the pedal circles of points  $X$  and  $Y$  coincide. Prove that  $X$  and  $Y$  are isogonal conjugate with respect to  $\triangle ABC$ .

**8.** Inside a triangle  $ABC$ , a point  $M$  is selected, and points  $C_1, A_1, B_1$  are chosen on the sides  $AB, BC, CA$ , respectively. Lines  $AM, BM, CM$  intersect for the second time the circumcircles of triangles  $AB_1C_1, A_1BC_1, A_1B_1C$  at points  $M_a, M_b, M_c$ , respectively. Let  $P$  be the intersection point of the circles  $AB_1C_1, A_1BC_1, A_1B_1C$ . Prove that the points  $M, M_a, M_b, M_c$ , and  $P$  are concyclic. (From now on, we denote the corresponding circle by  $\mathcal{M}$ ).

**9.** Let, in the notation of problem 8, the line  $PA_1$  intersect  $\mathcal{M}$  again at  $A'$ . Prove that  $MA' \parallel BC$ .

**10.** Prove that the lines  $M_aA', M_bB', M_cC'$  are concurrent or parallel.

**11\*** Prove that the circumcircles of the triangles  $AM_aA', BM_bB', CM_cC'$  are coaxial.

**12\*** Let  $a, b, c, d$  be lines in general position and let  $X_{ab}, X_{ac}, X_{ad}, X_{bc}, X_{bd}, X_{cd}$  be their intersection points. Let  $\mathcal{K}$  be a circle with a point  $K$  on it. Let  $Y_{ij}$  be the intersection point of  $X_{ij}K$  with  $\mathcal{K}$ . Prove that the lines  $Y_{ab}Y_{cd}, Y_{ac}Y_{bd}, Y_{ad}Y_{bc}$  are concurrent or parallel.

**13.** In a triangle  $ABC$  arbitrary points  $C_1, C_2$  on the side  $AB$ , points  $A_1, A_2$  on the side  $BC$ , points  $B_1, B_2$  on the side  $CA$  are selected. The lines  $A_1B_1$  and  $A_2B_2$  intersect at  $L_c$ , points  $L_a, L_b$  are defined similarly. Circumcircles of  $\triangle A_1A_2L_c$  and  $\triangle B_1B_2L_c$  intersect at points  $L_c$  and  $N_c$ . Points  $N_b$ , and  $N_a$  are defined similarly.

- a) Prove that the lines  $AN_a, BN_b, CN_c$  meet at one point (let's call it  $N$ )
- b) Prove that  $N, N_a, N_b, N_c$  lie on a circle (let's call it  $N$ ).

Let the circles  $AB_1C_1$ ,  $A_1BC_1$ ,  $A_1B_1C$  intersect at  $P$ , and let the circles  $AB_2C_2$ ,  $A_2BC_2$ ,  $A_2B_2C$  intersect at  $Q$ .

c) Prove that  $P$  and  $Q$  lie on  $\mathcal{N}$ .

d) Prove that the intersection point  $A'$  of lines  $PA_1$  and  $QA_2$  lies on  $\mathcal{N}$ .

## Part 2

In this section, the hyperbola icon  $\text{)}^{\text{h}}$  will denote some problems. In these problems, your goal will be to prove the original statement, and then formulate and prove a similar statement for a hyperbola.

**14.** Let  $A, B$  be two fixed points and let  $X$  be a point moving along a line. Examine the function  $f$  for intervals of monotonicity. Construct an extremum point with a compass and a ruler if

a)  $f(X) = XA + XB$

b)  $f(X) = XA - XB$

**15**<sup>o</sup> (*Fagnano's problem*) In a triangle  $ABC$ , points  $C', A', B'$  are chosen on the sides  $AB, BC, AC$ , respectively, which do not coincide with the vertices of  $\triangle ABC$ . It is known that the triangle  $A'B'C'$  has the smallest possible perimeter among all triangles inscribed in  $\triangle ABC$ . Prove that  $AA_1, BB_1$  and  $CC_1$  are altitudes of  $\triangle ABC$ .

**16**<sup>h</sup> (*Optical Property*) Let  $A$  be a point on an ellipse with foci  $F_1$  and  $F_2$ . Prove that the outer bisector of the angle  $F_1AF_2$  is tangent to the ellipse (has exactly one common point with it).

**17**<sup>h</sup> An ellipse with foci  $F_1$  and  $F_2$  is tangent to the sides of an angle  $ABC$ . Prove that  $\angle ABF_1 = \angle CBF_2$ .

**18**<sup>h</sup> An ellipse with focus  $F$  is fixed, and a line  $\ell$  is tangent to it. Let  $P$  be the projection of  $F$  onto  $\ell$ . Prove that if  $\ell$  is moving, then  $P$  is moving along a circle tangent to the ellipse at two points.

**19.** Let  $\mathcal{K}$  be an ellipse with foci  $F_1$  and  $F_2$ . A circle  $\omega$  with center  $O$  is tangent to  $\mathcal{K}$  at points  $X$  and  $Y$  (the ellipse lies inside the circle). Prove that

a)  $OF_1 = OF_2$ .

b)  $XF_1OF_2Y$  is an inscribed pentagon.

c)<sup>h</sup> Let a point  $P$  move along  $\omega$ . Then the angle between  $PF_1$  and one of the tangents from  $P$  to the ellipse is constant.

d) Redefine  $\omega$  so that  $\omega$  does not have to touch  $\mathcal{K}$  twice.

e) The line through  $O$  and the center of  $\mathcal{K}$  meets  $\mathcal{K}$  at  $Z$ . Prove that the circumcircle of  $\triangle OZF_1$  is tangent to  $\omega$ .

f) Let circles  $\alpha$  and  $\beta$  touch  $\omega$  internally, pass through  $F_1$ , and intersect for the second time at the point  $E$ . Prove that from the two intersection points  $\alpha$  and  $\mathcal{K}$  you can choose a point  $I$ , and from the two intersection points  $\beta$  and  $\mathcal{K}$  you can choose a point  $J$ , so that  $E$  will lie on the line  $IJ$ .

g)<sup>\*</sup> The line through  $O$  and the center of  $\mathcal{K}$  intersects  $\mathcal{K}$  at points  $Z$  and  $T$ , and the circle at points  $A$  and  $B$ . Point  $U$  is chosen on the line  $ZT$  so that  $\angle UF_1O = 90^\circ$ . Prove that the cross-ratio of the points  $A, Z, U, B$  is equal to the cross-ratio of the points  $B, T, U, A$  (in the order indicated).

h) Show that if we take  $\omega$  as an absolute for the Klein model of hyperbolic plane, then  $\mathcal{K}$  is a circle or an equidistant curve.

**20**<sup>h</sup> Let circles  $\alpha$  and  $\beta$  intersect at points  $X$  and  $Y$ . An ellipse  $\mathcal{K}$  is inscribed in the "slice" of their intersection, twice tangent to each of the circles. A line  $\ell_X$  is tangent to  $\mathcal{K}$ , separates the point  $X$  from  $\mathcal{K}$ , and intersects the "slice" at points  $S$  and  $T$ . Also,  $\ell_X$  intersects the circle  $\alpha$  outside the segment  $ST$  at  $A_1$ , and intersects the circle  $\beta$  outside the segment  $ST$  at  $B_1$ . Similarly, chose a line  $\ell_Y$  and define points  $A_2$  and  $B_2$ . Prove that  $A_1A_2 \parallel B_1B_2$ .

**21**<sup>\*</sup> Points  $N$  and  $M$  move along two circles with the same angular velocities. Find the envelope (curve touching all) of lines  $NM$ .

**22**<sup>\*</sup> Two points  $N$  and  $M$  move along two lines with constant speeds. Find the envelope of lines  $NM$ .

**23**<sup>h</sup> Given two intersecting circles, consider all ellipses lying inside both circles and touching each of the circles twice. Find the locus of their foci.

### Part 3

**24°** (*Orthologic triangles*) Let  $A, B, C, A_1, B_1, C_1$  be points in general position. Let the perpendiculars from  $A, B$ , and  $C$  to the lines  $B_1C_1, A_1C_1$ , and  $A_1B_1$ , respectively, intersect at one point. Prove that perpendiculars from  $A_1, B_1$ , and  $C_1$  to the lines  $BC, AC$ , and  $AB$ , respectively, also intersect at one point.

**25\*** Let  $A, B, C, A_1, B_1, C_1$  be points in general position. Suppose that there exists a point  $P$  such that  $\angle(AP, B_1C_1) = \angle(BP, A_1C_1) = \angle(CP, A_1B_1) = \alpha$ . Prove that there exists a point  $Q$  such that  $\angle(A_1Q, BC) = \angle(B_1Q, AC) = \angle(C_1Q, AB) = -\alpha$ .

We use the notation of Problem 13. Suppose additionally that the points  $A_1, A_2, B_1, B_2, C_1, C_2$  lie on a circle  $\mathcal{R}$  with center  $R$ .

**26.** Prove that  $P$  and  $Q$  are isogonal conjugate with respect to  $\triangle ABC$ .

**27.** Prove that:

- a)  $R \in \mathcal{N}$ .
- b)  $RN$  is a diameter of  $\mathcal{N}$ .
- c)  $PR = QR$ .

**28.** Prove that an ellipse  $\mathcal{K}$  with foci  $P$  and  $Q$  can be inscribed into the triangle  $ABC$ .

**29.** Lines  $PA'$  and  $QA'$  meet  $\mathcal{R}$  again at points  $X$  and  $Y$ . Prove that  $XY$  is tangent to  $\mathcal{K}$ .

**30.** Prove that  $\mathcal{K}$  is tangent to  $\mathcal{R}$  if and only if  $\mathcal{N}$  intersects  $\mathcal{R}$ , in which case the tangency points coincide with the intersection points.

**31.** Prove that in a triangle:

a) The Lemoine point, two Brocard points and the circumcenter form a deltoid (i.e. a kite) with two right angles.

b) An ellipse with foci at Brocard's points touches the sides at the bases of the symmedians.

**32\*** Suppose that the lines  $AA_1, BB_1, CC_1$  meet at a point  $L$ . Prove that  $L$  lies on the radical axis of  $\mathcal{N}$  and  $\mathcal{R}$ .

## Some features of Miquel's structures.

### Solutions

#### Part 1

1° Well-known.

2° We consider one position of points  $A_1$  and  $C_1$ , and another position, which we denote  $X$  and  $Y$ , respectively. The circles  $(BC_1A_1)$  and  $(BXY)$  are tangent or intersect at a point  $G \neq B$ .

In the first case there is a homothety with center  $B$  mapping the circle  $(BC_1A_1)$  to the circle  $(BXY)$ . It maps  $A_1$  to  $X$  and  $C_1$  to  $Y$ . Therefore,  $C_1A_1 \parallel XY$ . Consider a third position of points  $A_1$  and  $C_1$ , which we denote  $P$  and  $Q$ . Then  $\frac{A_1X}{A_1P} = \frac{C_1Y}{C_1Q}$ , hence  $PQ \parallel A_1C_1$ . Thus the circle  $(BPQ)$  is tangent to the circle  $(BA_1C_1)$ . So all circles  $(BA_1C_1)$  are tangent at  $B$ .

In the second case the triangles  $GXA_1$  and  $GYC_1$  are similar, since  $\angle(GA_1, A_1B) = \angle(GC_1, C_1B)$  and  $\angle(GX, XB) = \angle(GY, YB)$ . Hence there is a spiral similarity  $\phi$  with center  $G$ , mapping  $A_1$  to  $C_1$  and  $X$  to  $Y$ . Consider a third position of points  $A_1$  and  $C_1$ , which we denote  $P$  and  $Q$ . Then  $\phi(P) = Q$  and it follows that  $\angle(GP, PB) = \angle(GQ, QB)$ , so  $G$  lies on the circle  $(BPQ)$ .

3-4° Well-known.

5° Denote the intersection point of  $\ell_i$  and  $\ell_j$  by  $X_{ij}$ ; and the Miquel point of all lines except  $\ell_i$  by  $A_i$ . It suffices to prove that  $A_1, A_2, A_3$ , and  $A_4$  are concyclic. Using the circles  $(A_1A_2X_{35}X_{45})$ ,  $(A_2A_3X_{15}X_{45})$ ,  $(A_3A_4X_{15}X_{25})$ , and  $(A_4A_1X_{25}X_{35})$  we obtain

$$\begin{aligned} \angle(A_1A_2, A_2A_3) &= \angle(A_1A_2, A_2X_{45}) + \angle(X_{45}A_2, A_2A_3) = \angle(A_1X_{35}, X_{35}X_{45}) + \angle(X_{45}X_{15}, X_{15}A_3) \\ &= \angle(A_1X_{35}, X_{35}X_{25}) + \angle(X_{25}X_{15}, X_{15}A_3) = \angle(A_1A_4, A_4X_{25}) + \angle(X_{25}A_4, A_4A_3) = \angle(A_1A_4, A_4A_3). \end{aligned}$$

6° Below we present an algebraic solution of this problem, which works for parts a) and b) simultaneously. For a synthetic solution, where part a) is easier than part b), see [1], Theorem 2.12.

Let  $f(x, y) = 0$  and  $g(x, y) = 0$  be the equations of  $\mathcal{A}$  and  $\mathcal{B}$ , respectively, in Cartesian coordinates, where  $f(x, y) = x^2 + y^2 + a_1x + a_2y + a_3$  and  $g(x, y) = x^2 + y^2 + b_1x + b_2y + b_3$ . Note that the powers of point  $(x, y)$  with respect to  $\mathcal{A}$  and  $\mathcal{B}$  are equal to  $f(x, y)$  and  $g(x, y)$ , respectively. So the desired locus is given by equation  $f(x, y) = cg(x, y)$  for some constant  $c$ . It is easy to see that this equation defines a line if  $c = 1$  and a circle  $\mathcal{C}$  if  $c \neq 1$ .

Assume now that  $c \neq 1$ . The circle  $\mathcal{C}$  is given by equation  $\frac{f(x, y) - cg(x, y)}{1 - c} = 0$ . Let  $(p, q)$  be a point on the radical axis of  $\mathcal{A}$  and  $\mathcal{B}$ , i.e.  $f(p, q) = g(p, q)$ . The power of the point  $(p, q)$  with respect to  $\mathcal{C}$  is equal to  $\frac{f(p, q) - cg(p, q)}{1 - c} = f(p, q) = g(p, q)$ . Therefore,  $\mathcal{A}$ ,  $\mathcal{B}$ , and  $\mathcal{C}$  are coaxial.

7° Let  $X_b$  and  $Y_b$  be the projections of  $X$  and  $Y$  onto  $AC$ , respectively. Let  $X_c$  and  $Y_c$  be the projections of  $X$  and  $Y$  onto  $AB$ , respectively. Since  $X_b, Y_b, X_c$ , and  $Y_c$  are concyclic, we obtain

$$\begin{aligned} \angle(BA, AX) &= \angle(X_cA, AX) = \angle(X_cX_b, X_bX) = \angle(X_cX_b, X_bY_b) + 90^\circ \\ &= \angle(X_cY_c, Y_cY_b) + 90^\circ = \angle(YY_c, Y_cY_b) = \angle(YA, AY_b) = \angle(YA, AC) \end{aligned}$$

Similarly,  $\angle(AB, BX) = \angle(YB, BC)$ . Hence  $X$  is the isogonal conjugate of  $Y$  with respect to  $\triangle ABC$ .

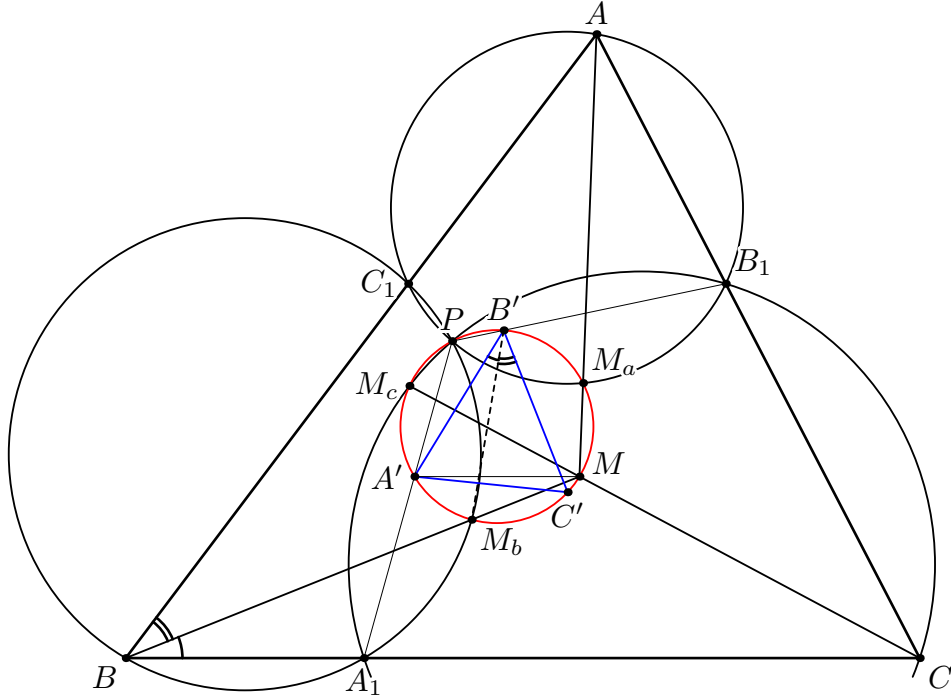
8. Observe that

$$\begin{aligned} \angle(MM_a, M_aP) &= \angle(AM_a, M_aP) = \angle(AB_1, B_1P) = \angle(CB_1, B_1P) \\ &= \angle(CA_1, A_1P) = \angle(CM_c, M_cP) = \angle(MM_c, M_cP). \end{aligned}$$

So  $M_c$  lies on the circle  $(MPM_a)$ . Similar argument shows that  $M_b$  also lies on this circle.

9. The following equalities imply that  $MA' \parallel BC$ .

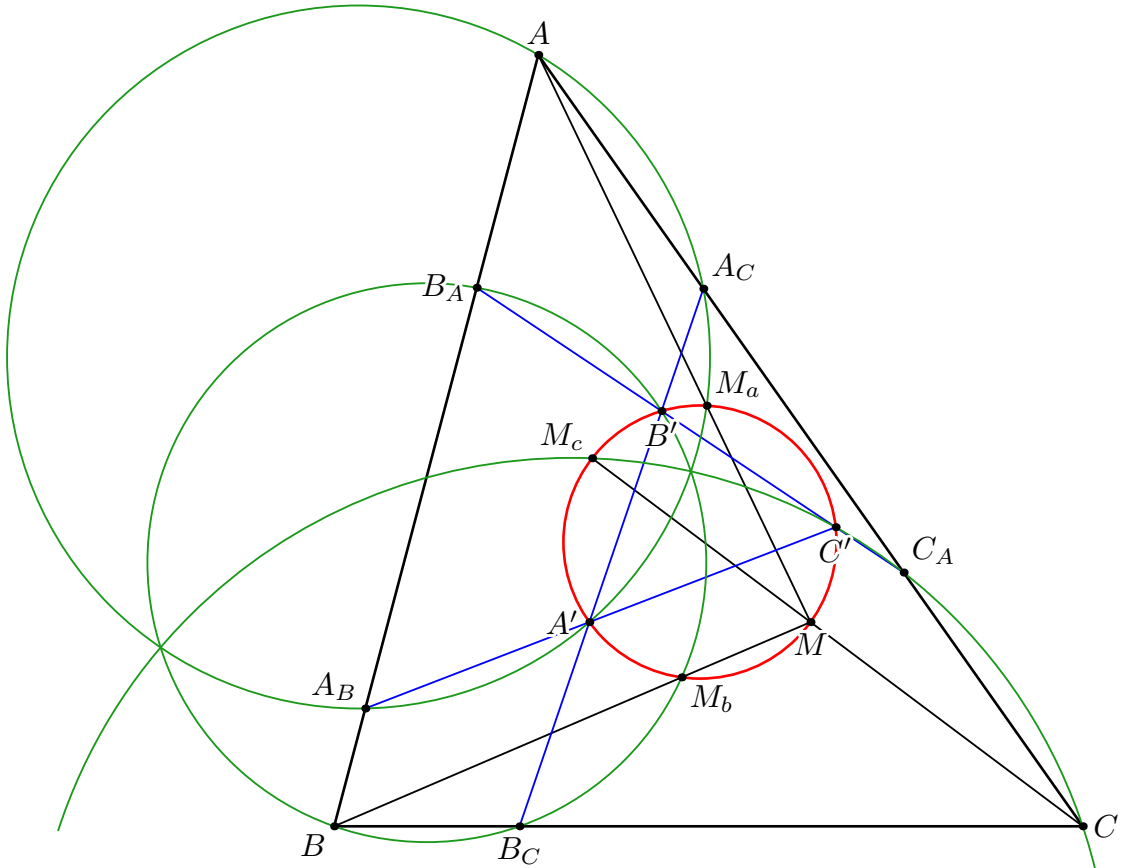
$$\angle(MA', A'P) = \angle(MM_c, M_cP) = \angle(CM_c, M_cP) = \angle(CA_1, A_1P) = \angle(BC, A'P),$$



10. We have

$$\angle(A'B', B'M_b) = \angle(A'M, MM_b) = \angle(CB, BM).$$

Similarly  $\angle(C'B', B'M_b) = \angle(AB, BM)$ , and so on. It follows that the triangles  $ABC$  and  $A'B'C'$  are similar and have different orientations. Moreover,  $A'M_a$ ,  $B'M_b$ , and  $C'M_c$  pass through the point, corresponding to the isogonal conjugate of  $M$  in  $\triangle ABC$ .



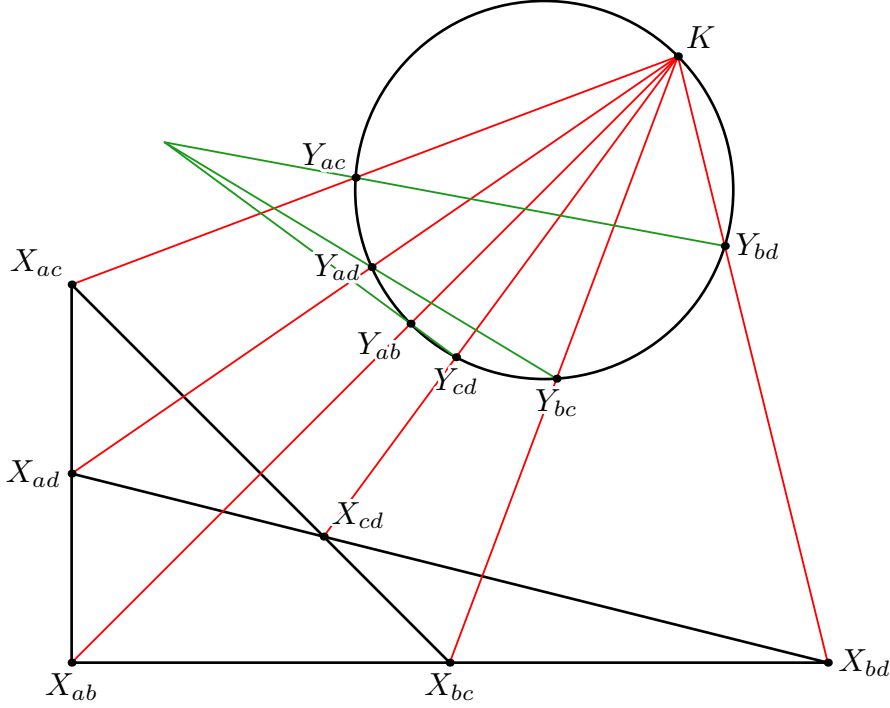
11\* Denote the circles  $(AM_aA')$ ,  $(BM_bB')$ , and  $(CM_cC')$  by  $\omega_a$ ,  $\omega_b$ , and  $\omega_c$ , respectively. Let  $A_B = AB \cap A'C'$ ,  $B_A = BA \cap B'C'$ ,  $A_C = AC \cap A'B'$ ,  $C_A = CA \cap C'B'$ ,  $B_C = BC \cap B'A'$ ,  $C_B = CB \cap C'A'$ .

By angle chase,  $\omega_a$  passes through  $A_B$  and  $A_C$ . Similarly  $B_A, B_C \in \omega_b$  and  $C_A, C_B \in \omega_c$ . Then

$$\frac{AB \cdot AB_A}{AC \cdot AC_A} = \frac{\sin \angle ACB \cdot \sin \angle AC_A B_A}{\sin \angle ABC \cdot \sin \angle AB_A C_A} = \frac{\sin \angle A_C C B_C \cdot \sin \angle A_C C_A B'}{\sin \angle A_C B' C_A \cdot \sin \angle A_C B_C C} = \frac{A_C B_C \cdot A_C B'}{A_C C_A \cdot A_C C}$$

which implies that the ratio of powers of  $A$  with respect to  $\omega_b$  and  $\omega_c$  is equal to the ratio of powers of  $A_C$  with respect to  $\omega_b$  and  $\omega_c$ . Similarly, this ratio is the same for  $A_B$ . The result now follows from problem 6.

**12\*** By the Desargues involution theorem, there exists an involution on the pencil of lines through  $K$ , which swaps  $KY_{ab}$  with  $KY_{cd}$ ,  $KY_{ac}$  with  $KY_{bd}$ , and  $KY_{ad}$  with  $KY_{bc}$ . So there exists an involution on  $\mathcal{K}$ , which swaps  $Y_{ab}$  with  $Y_{cd}$ ,  $Y_{ac}$  with  $Y_{bd}$ , and  $Y_{ad}$  with  $Y_{bc}$ . Such involution must map every point  $P \in \mathcal{K}$  to the second intersection point of  $PU$  with  $\mathcal{K}$ , where  $U = Y_{ab}Y_{cd} \cap Y_{ac}Y_{bd}$ . Therefore,  $Y_{ab}Y_{cd}$ ,  $Y_{ac}Y_{bd}$ ,  $Y_{ad}Y_{bc}$  are concurrent.



**13.** Observe that  $N_c$  is the second intersection point of the circles  $(A_1B_1C)$  and  $(A_2B_2C)$ .

a) Follows from trigonometric Ceva's theorem for the triangle  $ABC$ , since

$$\frac{\sin \angle BCN_c}{\sin \angle ACN_c} = \frac{A_1A_2}{B_1B_2}, \quad \frac{\sin \angle CAN_a}{\sin \angle BAN_a} = \frac{B_1B_2}{C_1C_2}, \quad \frac{\sin \angle ABN_b}{\sin \angle CBN_b} = \frac{C_1C_2}{A_1A_2}.$$

b, c) Follows from problem 8.

d) Follows from problem 9.

## Part 2

**14.** See [1], pp. 6-7.

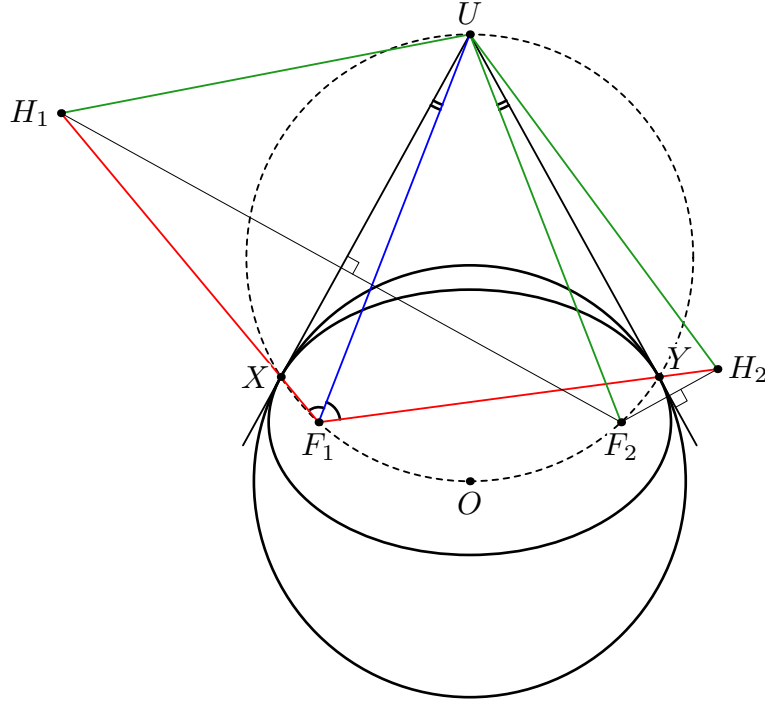
**15°** We fix  $B'$ ,  $C'$ , and move  $A'$ . Since  $B'A' + A'C'$  is minimal,  $BC$  is the external bisector of  $\angle B'A'C'$ . Similarly,  $AC$  and  $AB$  are the external bisectors of  $\angle A'B'C'$  and  $\angle A'C'B'$ , respectively. So  $A$ ,  $B$ , and  $C$  are excenters of  $\triangle A'B'C'$ . Thus  $AA'$ ,  $BB'$ , and  $CC'$  are altitudes of  $\triangle ABC$ .

**16)** See [1], Theorem 1.1 and the discussion after its proof.

**17)** See [1], Theorem 1.3 and the discussion after its proof.

**18)** Let  $\mathcal{K}$  be the ellipse, let  $G$  be its second focus, and let  $M$  be the midpoint of  $FG$ . Let  $A$  be the reflection of  $F$  in  $\ell$  and let  $B = \ell \cap \mathcal{K}$ . Then  $MP = GA/2 = (FB + BG)/2$  is constant, so  $P$  moves along a circle with center  $M$  tangent to  $\mathcal{K}$ .

**19.** a) b) Construct tangents to the ellipse at  $X$  and  $Y$ . Let them meet at  $U$ .



First, let us prove an auxiliary fact — the bisector of the angle  $XF_1Y$  passes through  $U$ . Reflect  $F_2$  in both tangents, denote reflections by  $H_1$  and  $H_2$ . Triangles  $UH_1F_1$  and  $UH_2F_1$  are congruent, by SSS. Therefore,  $\angle XF_1U = \angle YF_1U$ .

It follows that  $U$  lies on the bisector of the angle  $XF_1Y$  (and similarly, the angle  $XF_2Y$ ), and on the perpendicular bisector of  $XY$  (since the segments of tangents are equal). Hence  $X, F_1, F_2, Y, U$  are concyclic. Since  $XOYU$  is inscribed,  $O$  lies on this circle, too.  $XO$  is the bisector of the angle  $F_1XF_2$  (since it is perpendicular to the tangent to the ellipse), therefore,  $F_1O = OF_2$ .

**c)**<sup>(</sup> By Problem 18, the locus of projections of  $F_1$  onto tangents to the ellipse is a circle. Applying spiral similitude with center  $F_1$ , angle  $\pi/2 - \alpha$  and ratio  $1/\sin \alpha$ , we obtain that the locus of points  $P$  such that the oriented angle between  $PF_1$  and the tangent to the ellipse through  $P$  is equal to  $\alpha$ , is also a circle. For  $\alpha = \angle YXU$  this locus is the circle  $\omega$ .

**d)** By the previous item,  $\omega$  could be defined as the locus of  $P$  such that the oriented angle between  $PF_1$  and the tangent to the ellipse through  $P$  is equal to  $\alpha$ .

**Note.** If the circles  $(OF_1F_2)$  and  $\omega$  do not intersect, the tangent points of  $\mathcal{K}$  and  $\omega$  are not real (complex).

**e)** Let the perpendicular to  $OF_1$  through  $F_1$  intersect  $\omega$  at  $U_1$ , let  $Z'$  be the projection of  $U_1$  onto  $OZ$ . Points  $F_1$  and  $Z'$  lie on the circle with diameter  $OU_1$  touching  $\omega$ . Moreover,  $\angle(F_1U_1, U_1Z') = \angle(F_1O, OU) = \angle(F_1X, XU)$ , since  $U_1Z'OF_1$  and  $F_1XOU$  are inscribed. Hence  $U_1Z$  touches  $\mathcal{K}$  (since the circle  $\omega$  is the locus of points such that the angle between the tangent and the segment joining with the focus, is constant), and  $Z'$  coincides with  $Z$ .

**f)** Follows from the following Lemma that generalizes the statement of the previous item (by a spiral similitude with center  $F_1$ ).

**Lemma.** Let  $P$  be an arbitrary point of the ellipse  $\mathcal{K}$ , let the tangent to  $\mathcal{K}$  through  $P$  intersect  $\omega$  at  $A$  and  $B$ . It follows that the circle  $APF_1$  touches  $\omega$ .

**g)**<sup>\*</sup> From e) it follows that  $Z$  and  $T$  are projections onto  $AB$  of the endpoints of the chord of  $\omega$  having the midpoint  $F_1$ . Hence in cross ratios one can replace  $Z$  and  $T$  by the endpoints of this chord, and replace  $A$  and  $B$  by the intersection points of these tangents with  $UF_1$ . If  $U$  lies outside the circle, then perform a projective transformation that maps the circle to itself and takes  $U$  to infinity. If  $U$  lies inside the circle, then perform a projective transformation that maps  $U$  to the center. In both cases the statement is obvious.

**h)** Directly follows from the previous. (About models of Lobachevsky plane one can read in [2].)

**20)**<sup>(</sup> Let  $F_1$  and  $F_2$  be the foci of the ellipse, where  $F_1$  is closer to  $Y$  than  $F_2$ . From 19c it follows that  $F_1A_1B_1$  and  $F_2A_2B_2$  are similar, by equal angles. Let  $S = A_1B_1 \cap A_2B_2$ . From the optic property we have



$\angle A_1SF_1 = \angle A_2SF_2$ . Hence there exists a product of a dilation with center  $S$  and the reflection in the bisector of the angle  $A_1SA_2$ , which maps  $A_1F_1B_1$  to  $A_2F_2B_2$ . Hence  $\frac{A_1S}{A_2S} = \frac{B_1S}{B_2S}$ , therefore  $A_1A_2 \parallel B_1B_2$ .

**21\*** Let  $O$  be the center of the spiral similitude taking one of the circle to the other and taking  $N$  to  $M$ . Since all the triangles  $ONM$  are similar to each other, the projection  $H$  of  $O$  onto  $MN$  lie on a certain circle  $\omega$ . Thus we can reformulate the problem in the following way: let  $\omega$  and  $O$  be a circle and a point; we need to find a curve touching lines passing through a point  $H \in \omega$  and perpendicular to  $OH$ .

If  $O$  lies on  $\omega$ , then all such lines pass through the antipodal point. Otherwise, this curve is a conic with one its focus at  $O$ . This conic is an ellipse, if  $O$  lies inside  $\omega$ , and a hyperbola, if it lies outside  $\omega$  (It could be derived from the Problem 18.)

**22\*** **Answer:** A parabola tangent to given lines.

**Proof.** Let  $A$  and  $B$  be points moving linearly along two given lines intersecting at  $X$ . Consider a point  $F \neq X$ , which is a common point of all circles  $(ABX)$  (it is known that such point exists, if  $A$  and  $B$  do not pass  $X$  simultaneously. If they pass  $X$  simultaneously, then  $AB$  has a constant direction). The Miquel point of four lines is the focus of the parabola touching these four lines (e.g., see [1], Theorem 4.10). this argument completes the proof.

**23)** **Answer:** The circle passing through the intersection points of two given circles, which as the Apollonius circle for their centers.

### Part 3

**24°** It is known that both conditions are equivalent to  $AB_1^2 + BC_1^2 + CA_1^2 = BA_1^2 + AC_1^2 + CB_1^2$ .

**25\*** Let  $A_2B_2C_2$  be the image of the triangle  $ABC$  under the rotation about the point  $P$  through the angle  $\alpha - 90^\circ$ . Then the triangles  $A_1B_1C_1$  and  $A_2B_2C_2$  are orthologic, so there exists a point  $Q$  such that  $A_1Q \perp B_2C_2$ ,  $B_1Q \perp A_2C_2$ , and  $C_1Q \perp A_2B_2$ . Since  $\angle(BC, B_2C_2) = \alpha - 90^\circ$ , we obtain  $\angle(A_1Q, BC) = \angle(A_1Q, B_2C_2) - \angle(BC, B_2C_2) = -\alpha$ . Similarly  $\angle(B_1Q, AC) = \angle(C_1Q, AB) = -\alpha$ , as required.

Below we sketch a different solution, which does not use problem 24.

Let us call a triple of lines  $a', b', c'$  harmonic to a triple of lines  $a, b, c$ , if in a triangle whose sidelines are parallel to  $a, b, c$ , the corresponding cevians parallel to  $a', b', c'$  are concurrent.

*Lemma.* The relation 'harmonic' is symmetric, i.e., if  $a', b', c'$  is harmonic to  $a, b, c$ , then  $a, b, c$  is harmonic to  $a', b', c'$ .

*Proof.* Let  $\ell$  be a line. Through a point  $O$  ( $O$  not in  $\ell$ ) let us construct lines parallel to  $a, b, c, a', b', c'$ . Let these lines intersect  $\ell$  at  $A, B, C, A', B', C'$ , respectively. Using Ceva theorem in the sine form, rewrite the condition that  $a', b', c'$  is harmonic to  $a, b, c$  as  $\frac{AB'}{B'C} \cdot \frac{CA'}{A'B} \cdot \frac{BC'}{C'A} = -1$ . We see that this condition is invariant under replacement of  $a, b, c$  by  $a', b', c'$ . Lemma is proved.

Now let  $a, b, c$  and  $a', b', c'$  be the sidelines of triangles  $ABC$  and  $A_1B_1C_1$ . By  $t_\varphi$  denote  $t$  rotated by angle  $\varphi$ . The condition of the problem means that  $a, b, c$  is harmonic to  $a'_\varphi, b'_\varphi, c'_\varphi$ . Using rotation by  $-\varphi$ , we get that  $a_{-\varphi}, b_{-\varphi}, c_{-\varphi}$  is harmonic to  $a', b', c'$ , and the statement follows.

We use the notation of Problem 13. Suppose additionally that the points  $A_1, A_2, B_1, B_2, C_1, C_2$  lie on a circle  $\mathcal{R}$  with center  $R$ .

**26.** (*Generalized pedal triangles*) Let  $P'$  be the isogonal conjugate to  $P$ . Let  $P_a, P_b, P_c$  be projections of  $P$  onto  $BC, CA, AB$ , respectively; similarly denote projections of  $P'$ . We know that the midpoint  $R_0$  of  $PP'$  is the center of the circle  $(P_aP_bP_c) = (P'_aP'_bP'_c)$ . Let  $\angle(PA_1, CA_1) = \angle(PB_1, AB_1) = \angle(PC_1, BC_1) = \varphi$ . Let  $R_1$  be the circumcenter of  $(A_1B_1C_1)$ . Triangle  $P_aP_bP_c$  maps to  $A_1B_1C_1$  by some spiral similitude with center  $P$ , hence  $PP_aA_1 \sim PR_0R_1$ , thus  $R_1$  is a point on the perpendicular bisector of  $PP'$  such that  $\angle(PR_1, R_1R_0) = \varphi$ . Hence  $\angle(R_1R_0, R_1P') = \varphi$ . Perform the spiral similitude with center  $P'$  taking  $R_0$  to  $R_1$ . It maps  $P'_aP'_bP'_c$  to  $A'_2B'_2C'_2$  so that  $P'R_0R_1 \sim P'P'_aA'_2 \sim P'P'_bB'_2 \sim P'P'_cC'_2$ , so  $A'_2, B'_2, C'_2$  are the points of  $BC, CA, AB$  such that  $\angle(P'A'_2, CA'_2) = \angle(P'B'_2, AB'_2) = \angle(P'C'_2, BC'_2) = -\varphi$ . Since  $R_0$  is the center of the circle  $(P'_aP'_bP'_c)$ ,  $R_1$  is the center of the circle  $(A'_2B'_2C'_2)$ . Radii of circles  $(A_1B_1C_1)$  and  $(A'_2B'_2C'_2)$  are both equal to  $R(P_aP_bP_c)/\sin \varphi$ , hence these circles coincide. It follows that  $A'_2 = A_2, B'_2 = B_2, C'_2 = C_2, Q = P'$ , and  $R_1 = R$ .

In addition, note that triangles  $ABC$  and  $A_1B_1C_1$  satisfy the condition of the Problem 25 with  $P$  and  $Q$  as points of concurrency.

**27.** From the previous proof we have  $\angle(PR, QR) = 2\varphi = \angle(PA_1, QA_2)$ . By problem 13, we obtain  $A' = PA_1 \cap QA_2 \in \mathcal{N}$ , hence  $R \in \mathcal{N}$ .

Note that  $\angle(PN_c, N_cN) = \angle(PN_c, N_cC) = \angle(PA_1, A_1C) = \varphi$ . Similarly,  $\angle(QN_b, N_bN) = -\varphi$ . This means that the arcs  $NP$  and  $NQ$  of  $\mathcal{N}$  are equal.  $PR = QR$  follows from the proof of Problem 26. So  $RN$  is the perpendicular bisector of  $PQ$ , i.e.  $RN$  is a diameter of  $\mathcal{N}$ .

**28.** Let  $Q_a, Q_b$ , and  $Q_c$  be the reflections of  $Q$  in  $BC, CA$ , and  $AB$ , respectively. Let  $PQ_a, PQ_b, PQ_c$  intersect  $BC, CA, AB$  at  $A^*, B^*, C^*$ , respectively. Then  $P$  is the circumcenter of  $Q_a, Q_b, Q_c$ , hence  $PA^* + QA^* = PB^* + QB^* = PC^* + QC^*$ . So there is an ellipse with foci  $P$  and  $Q$  passing through  $A^*, B^*, C^*$ . It is tangent to the sides of  $\triangle ABC$  by problem 16.

**29.** Since  $\angle(PA_1, BC) = \angle(BC, QA_2) = \varphi$ ,  $A_1A_2YX$  is inscribed in  $\mathcal{R}$  and  $A_1A_2YX$  is symmetric in the common perpendicular bisector of  $XY$  and  $A_1A_2$  (in particular,  $XY \parallel A_1A_2$ ). To prove that  $XY$  is tangent to  $\mathcal{K}$  it suffices to show that the center of  $\mathcal{K}$  (that is the midpoint of  $PQ$ ) lies on the midline of  $A_1A_2YX$ , or, equivalently, to show that  $PA_1 = QY$ . From previous we know that  $\angle(PR, QR) = 2\varphi$  and  $RP = RQ$ . Since  $\angle(A_1R, RY) = 2\angle(A_1A_2, A_2Y) = 2\varphi$ , we have  $\angle(PR, A_1R) = \angle(QR, YR)$ , and by SAS, triangles  $PRA_1$  and  $QRY$  are congruent. Thus  $PA_1 = QY$  follows.

**30.** For the circle  $\mathcal{R}$ , point  $P$  and angle  $\varphi$  consider the Brocard ellipse that is a conic touching the lines  $PZ$  rotated by  $\varphi$  around  $Z \in \mathcal{R}$  (see the Problem 19c, inverse statement). For 6 positions of  $Z$  ( $A_1$  and  $X$  from Problem 29 and 3 analogous pairs) the corresponding tangents to the Brocard ellipse also touch  $\mathcal{K}$ . Thus  $\mathcal{K}$  is the Brocard ellipse. Now the statement follows from the Problem 19b and its inverse.

**31.**

a) We put this situation into a general case from the solution of Problem 26 (generalized pedal triangles).

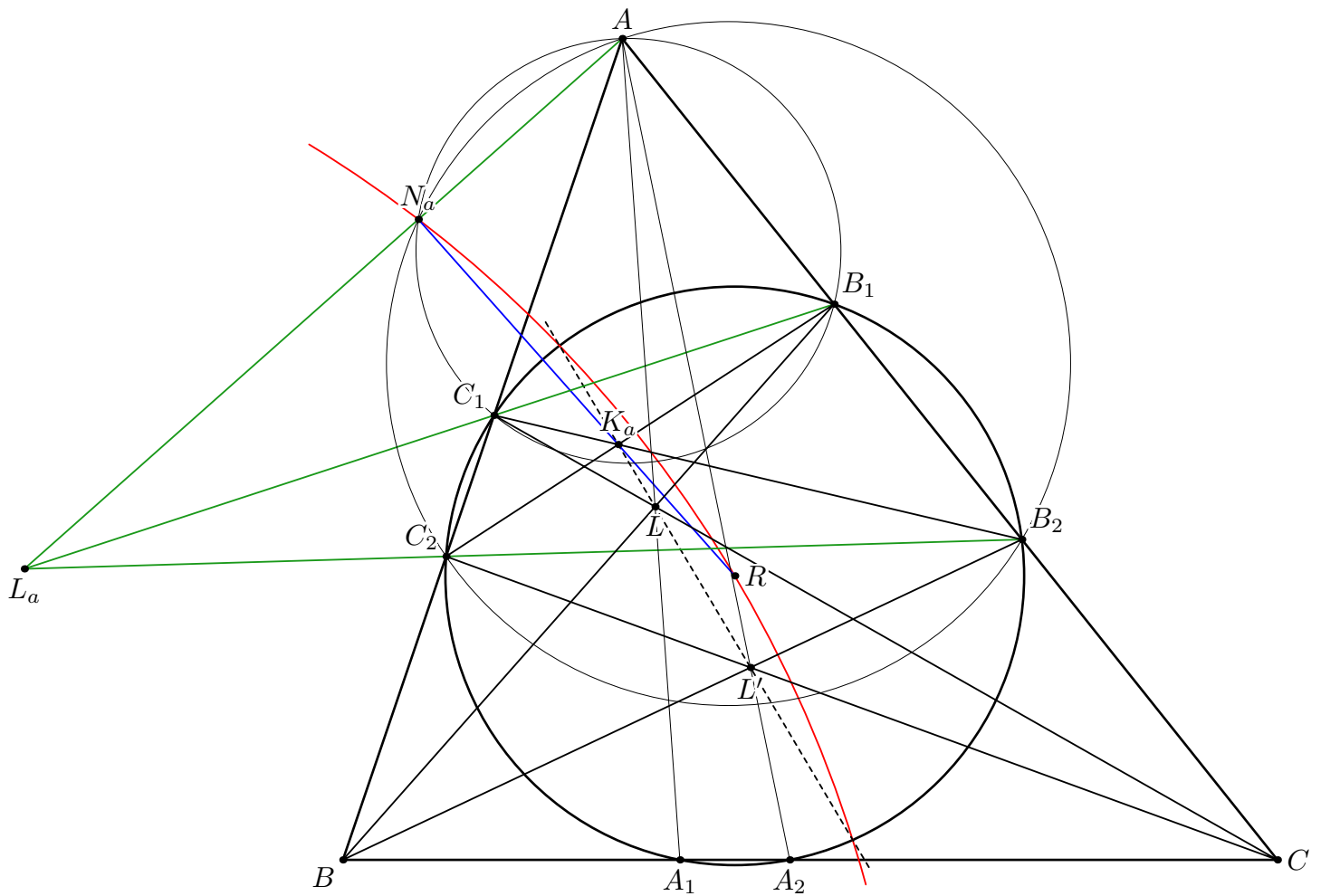
For  $P$  and  $Q$  being the Brocard points,  $ABC$  is a particular case of generalized pedal triangles with  $B = A_1$ ,  $C = B_1$ ,  $A = C_1$  and  $B = C_2$ ,  $C = A_2$ ,  $A = B_2$ . Thus in this case  $O = R$ , and we know that  $PO = OQ$  with  $\angle(PO, OQ) = 2\varphi$ , where  $90^\circ - \varphi$  is the Brocard angle.

Now let  $L$  be Lemoine point. Though  $L$  draw a line  $B_2C_1$  ( $B_2 \in AC$ ,  $C_1 \in AB$ ) so that  $B, C, B_2, C_1$  are concyclic. From  $ABC \sim AB_2C_1$  it follows that  $AL$  is the median in  $AB_2C_1$ , hence  $B_2L = C_1L$ . Similarly construct  $C_2A_1$ ,  $A_2B_1$ . We have  $\angle(LB_2, AC) = \angle(AB, BC) = \angle(AC, LB_1)$ . It follows  $LB_2 = LB_1$ . Thus all 6 segments  $LA_1$ ,  $LA_2$ ,  $LB_1$ ,  $LB_2$ ,  $LC_1$ ,  $LC_2$  are equal, and  $A_1, A_2, B_1, B_2, C_1, C_2$  lie on a circle (known as Taylor circle) centered at  $R = L$ . Now we will show that points  $P$  and  $Q$  (from general construction of Problem 26) are Brocard points. (Note that  $LP = LQ$ ). Since  $LA_1 = LA_2 = LC_2$ , We have  $A_2C_2 \perp BC$ . Similarly,  $B_2A_2 \perp CA$ , and  $C_2B_2 \perp AB$ . Now from the circles  $(AB_2C_2Q)$ ,  $(BC_2A_2Q)$ ,  $(CA_2B_2Q)$  we have:  $y = \angle(C_2A_2, A_2Q) = \angle(C_2B, BQ) = 90^\circ - \angle(QC_2, C_2B) = \angle(B_2C_2, C_2Q) = \angle(B_2A, AQ)$ , and similarly,  $y = \angle(A_2C, CQ)$ . This means that  $Q$  is the Brocard point (with  $y$  as the Brocard angle), and  $(A_2B_2C_2)$  is its generalized pedal circle corresponding to  $\varphi = \angle(QC_2, AB) = 90^\circ - y$ . Hence  $\angle(PL, LQ) = 2\varphi$ . Thus  $P, Q, L, O$  are concyclic with  $P$  and  $Q$  symmetric in  $OL$ .

b) Let  $AS$  be the symmedian, so that  $BS : CS = c^2 : b^2$ . It suffices to show that  $PBS \sim QCS$ , or  $PB : QC = c^2 : b^2$ ; from this it follows that  $\angle(PS, SB) = \angle(CS, SQ)$ .

Now from the sine law,  $\frac{PB}{\sin y} = \frac{c}{\sin APB} = \frac{c}{\sin B}$ . Similarly,  $\frac{QC}{\sin y} = \frac{b}{\sin C}$ . Dividing the first equality by the second one, we get the required similarity.

**32\*** It is not hard to see that the lines  $AA_2$ ,  $BB_2$ , and  $CC_2$  are concurrent at some point  $L'$ . Let  $K_a = B_1C_2 \cap B_2C_1$ , points  $K_b$  and  $K_c$  are defined similarly. By the Pappus theorem the points  $L$ ,  $L'$ , and  $K_a$  are collinear. It suffices to show that  $K_a$  lies on the radical axis of  $\mathcal{R}$  and  $\mathcal{N}$  (a similar argument then implies that  $K_b$  and  $K_c$  also lie on this radical axis). The lines  $B_1C_1$ ,  $B_2C_2$ , and  $AN_a$  are concurrent, since they are the radical axes of circles  $(AB_1C_1N_a)$ ,  $(AB_2C_2N_a)$ , and  $\mathcal{R}$ . So  $AN_aL_aN$  is the polar line of  $K_a$  with respect to  $\mathcal{R}$ . Moreover  $N_a \in \mathcal{N}$  and  $NR$  is the diameter of  $\mathcal{N}$ , hence  $RN_a \perp AN_a$ . Thus the inversion in  $\mathcal{R}$  maps  $K_a$  to  $N_a$ . This inversion maps the line  $B_2C_1K_a$  to the circle  $RB_2C_1N_a$ . Therefore  $K_aC_1 \cdot K_aB_2 = K_aR \cdot K_aN_a$ . It follows that  $K_a$  lies on the radical axis of  $\mathcal{R}$  and  $\mathcal{N}$ .



## References

- [1] A.Akopyan, A.Zaslavsky, *Geometry of Conics*.

*For all questions, typos, shortcomings and inaccuracies, please inform K.S. Ivanov at ponyboss3@gmail.com.*

# Доказательство Кронекера теоремы Галуа о неразрешимости уравнений в радикалах

представляют Д. Герасимов, Е. Коган,  
Е. Морозов, Я. Пан, А. Скопенков \*

## Содержание

1	Введение и основные результаты . . . . .	2
1.1	Обзор и мотивировки . . . . .	2
1.2	Неразрешимость в вещественных радикалах . .	3
1.3	Неразрешимость в комплексных радикалах . .	4
1.4	Рекомендации участникам . . . . .	5
2	Доказательства неразрешимости в задачах . . . . .	6
2.1	Одно извлечение квадратного корня (1-2) . . .	6
2.2	Одно извлечение корня третьей степени . . .	7
2.3	Одно извлечение корня простой степени . . . .	8
2.4	Несколько извлечений квадратных корней . .	9
2.5	К теореме Кронекера . . . . .	10
2.6	Решения задач до промежуточного финиша . .	11
2.7	Решения остальных задач . . . . .	16

---

\*Благодарим В. Волкова за полезные обсуждения и Б. Френкина за перевод части текста на русский язык.

*Д. Герасимов:* Физтех-лицей (Долгопрудный),

*Е. Коган, Е. Морозов:* Высшая школа экономики (Москва).

*Я. Пан:* Институт науки и технологии провинции Хенан (Китай).

*А. Скопенков:* Московский Физико-Технический Институт, Независимый Московский Университет. <https://users.mccme.ru/skopenko/>.

*And the leap is not — is not what I think you sometimes see it as — as breaking, as acting. It's something much more like a quiet transition after a lot of patience and — tension of thought, yes — but with that [enlightenment] as its discipline, its orientation, its truth. Not confusion and chaos and immolation and pulling the house down, not something experienced as a great significant moment.*

I. Murdoch, The Message to the Planet

## 1 Введение и основные результаты

### 1.1 Обзор и мотивировки

Этот раздел не используется в дальнейшем.

Данный текст содержит короткое изложение доказательства Кронекера теоремы Галуа 1.3.2 о неразрешимости алгебраических уравнений в радикалах. Это доказательство интересно, так как предположительно оно является самым коротким.

Мы не используем термин «группа Галуа» и даже термин «группа». Тем не менее наше изложение дает неплохую возможность освоить (или освежить в памяти) некоторые идеи, лежащие в основе теории Галуа. Таким образом, данный проект перекидывает мост (показывая, что нет никакой пропасти) между элементарной математикой и теорией Галуа. Проект доступен школьникам, знакомым с многочленами и комплексными числами (знакомства с перестановками не требуется).

Приводимые доказательства не претендуют на новизну (возможно, за исключением методических находок). Главная идея доказательства известна (см. [Do65, §25], [Pr07, Ti03]), и предположительно принадлежит Кронекеру (ошибка в приведенных выше текстах, указанная в [Sk21m, Замечание 8.4.18b], исправлена в [Sk08, PC19] и [Sk21m, §8]). К сожалению, само доказательство не очень широко известно.

Приводимое доказательство интересно также тем, что оно не использует перестановки. Поэтому в качестве «причины» возникновения неразрешимости в радикалах мы видим не тот факт, что группа  $A_5$  неразрешима, а что существует многочлен степени 5 с

рациональными коэффициентами, неприводимый над  $\mathbb{Q}$ , имеющий более одного вещественного корня и хотя бы один невещественный корень. Таким образом, данное доказательство отлично от доказательств теорем Галуа и Абеля, приводимых в [?, Ay82, Be10, Br, Ed84, FT, Ha78, Le11, PC19, Pe04, Ro95, St94, Sk15] (комментарии и исправления некоторых ошибок см. в [Sk15]).

## 1.2 Неразрешимость в вещественных радикалах

Вещественное число называется **вещественно радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней из положительных чисел. Т.е. если некоторое множество, его содержащее, можно получить из множества  $\{1\}$ , используя операции добавления к уже имеющемуся множеству  $M \subset \mathbb{R}$ , содержащему числа  $x, y$ ,

чисел  $x + y, x - y, xy$ , числа  $x/y$  при  $y \neq 0$

и числа  $\sqrt[n]{x}$  при  $x > 0$  и целом  $n > 0$ .

**1.2.1.** (а) Любой вещественный корень квадратного уравнения с рациональными коэффициентами вещественно радикален.

(б) Уравнение  $x^3 + x + 1 = 0$  имеет ровно один вещественный корень, который вещественно радикален.

(с) Уравнение  $x^4 + 4x - 1 = 0$  имеет два вещественных корня, каждый из которых вещественно радикален.

**Теорема 1.2.2.** (а) Число  $\cos(2\pi/9)$  не является вещественно радикальным.

(б) Существует многочлен 3-й степени с рациональными коэффициентами (например,  $x^3 - 3x + 1$ ), ни один из корней которого не является вещественно радикальным.

Вы сможете доказать п. (б) этой теоремы с помощью задач, выдаваемых до промежуточного финиша. Разрешается использовать п. (б) без доказательства для решения других задач в §1.2.

**1.2.3.** (а) Для любого  $n \geq 3$  существует многочлен  $n$ -й степени с рациональными коэффициентами, один из корней которого не является вещественно радикальным.

(b) Справедлив аналог утверждения п. (a) с заменой слов «один из корней» на «ни один из корней». (При этом корни *некоторых* уравнений высоких степеней (например,  $x^5 = 2$ ) вполне могут быть вещественно радикальны.)

(c) Трисекция угла невозможна при помощи вещественных радикалов, т.е. существует такое  $\alpha$  (например,  $\alpha = 2\pi/3$ ), что число  $\cos \alpha$  вещественно радикально, а число  $\cos(\alpha/3)$  — нет.

### 1.3 Неразрешимость в комплексных радикалах

Комплексное число называется (комплексно) **радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней. Т.е. если некоторое множество, его содержащее, можно получить из множества  $\{1\}$ , используя операции добавления к уже имеющемуся множеству  $M$ , содержащему числа  $x, y$ ,

$$\text{чисел } x + y, x - y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

и любого такого числа  $r \in \mathbb{C}$ , что  $r^n = x$  для некоторого целого  $n > 0$ .

**1.3.1.** (a) Любой (комплексный) корень квадратного уравнения с рациональными коэффициентами радикален.

(b) Число  $\cos(2\pi/9)$  радикально.

(c,d) То же, что и в п. (a) для многочленов 3-й и 4-й степени.

(e) Если действительная и мнимая части комплексного числа  $z$  вещественно радикальны, то число  $z$  радикально.

(f) Обратное утверждение к п. (e) неверно.

Аналоги утверждений пп. (a,c,d) для уравнений более высоких степеней неверны.

**Теорема 1.3.2** (Галуа). Существует уравнение 5-й степени с рациональными коэффициентами (например,  $x^5 - 4x + 2 = 0$ ), ни один из корней которого не является радикальным.

Знаменитую проблему разрешимости уравнений в радикалах решили доказанные немного ранее более слабые теоремы Руффини–Абеля. Строгие формулировки этих теорем сложнее [Sk21m, Теорема Руффини 8.2.2], [Sk15, Замечание 7]. Более простой способ



решить проблему разрешимости уравнений в радикалах предложен в [Sk21m, Теорема 8.1.13 и ее доказательство в §8.4.F]. Здесь мы предлагаем другой короткий способ: вывести теорему Галуа 1.3.2 из следующего результата.

**Теорема 1.3.3** (Кронекер). Если многочлен простой степени с рациональными коэффициентами неприводим над  $\mathbb{Q}$ , имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней не является радикальным.

Эта теорема интересна и нетривиальна даже для многочлена пятой степени. Вы сможете доказать эту теорему с помощью задач, выдаваемых после промежуточного финиша.

## 1.4 Рекомендации участникам

Участник (или группа участников) конференции, решающий задачи проекта, получает «боб» за каждое записанное решение, оцененное в «+» или «+».». Дополнительные бобы могут выдаваться за красивые решения, решения сложных проблем, или оформление некоторых решений в системе  $\text{T}_{\text{E}}\text{X}$ . У жюри бесконечно много бобов. Решения можно сдавать и устно, отдавая один боб за каждые пять попыток (неважно, удачных или нет).

Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. *Загадкой* называется не сформулированный четко вопрос; здесь нужно придумать и четкую формулировку, и доказательство. Если задача выделена словом «теорема» («лемма», «следствие» и т.д.) и жирным шрифтом, 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 последующие задачи. Если Вы застряли на какой-то другой задаче, также перейдите к следующим, они могут помочь. Приглашаем Вас *обсуждать* с жюри возникающие вопросы. Особо успешным решателям мы выдаем *дополнительные задачи* для исследования.

Пожалуйста, сообщите нам, если Вы уже знаете решения нескольких предложенных задач. Если Вы подтвердите свои знания, со-

обобщив нам решения некоторых из них, Вам будет разрешено не получать плюсы по всем этим задачам, но пользоваться ими при решении остальных.

## 2 Доказательства неразрешимости в задачах

В этом тексте «многочлен с рациональными коэффициентами» коротко называется многочленом. Обозначим

$$\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q).$$

### 2.1 Одно извлечение квадратного корня (1-2)

**2.1.1.** Представимо ли следующее число в виде  $a + \sqrt{b}$ , где  $a, b \in \mathbb{Q}$ :

- (a)  $\sqrt{3 + 2\sqrt{2}}$ ; (b)  $\frac{1}{7+5\sqrt{2}}$ ; (c)  $\sqrt[3]{7 + 5\sqrt{2}}$ ; (d)  $\sqrt[3]{2}$ ;  
 (e)  $\sqrt{2} + \sqrt[3]{2}$ ; (f)  $\sqrt{2 + \sqrt{2}}$ ; (g)  $\sqrt{2} + \sqrt{3} + \sqrt{5}$ ; (h)  $\cos(2\pi/9)$ ?

Для п. (g) вам потребуются идеи из §2.4.

**Лемма 2.1.2** (о расширении). Пусть число можно получить из числа 1 при помощи нескольких операций сложений, вычитаний, умножений, делений на ненулевые числа, и одной операции извлечения квадратного корня из положительного числа (т.е. число вещественно построимо с извлечением корня только один раз). Тогда оно имеет вид  $a \pm \sqrt{b}$ , где  $a, b \in \mathbb{Q}$  и  $b > 0$ .

**Лемма 2.1.3.** Пусть  $r \in \mathbb{R} - \mathbb{Q}$  и  $r^2 \in \mathbb{Q}$ .

- (a) **О неприводимости.** Многочлен  $x^2 - r^2$  неприводим над  $\mathbb{Q}$ .  
 (b) **О линейной независимости.** Если  $a, b \in \mathbb{Q}$  и  $a + br = 0$ , то  $a = b = 0$ .  
 (c) Если многочлен  $P$  имеет корень  $r$ , то  $P$  делится на  $x^2 - r^2$ .  
 (d) **О сопряжении.** Если многочлен имеет корень  $r$ , то корнем этого многочлена является также число  $-r$ .  
 (e) **О сопряжении.** Если  $a, b \in \mathbb{Q}$  и многочлен имеет корень  $a + br$ , то корнем этого многочлена является также число  $a - br$ .  
 (f) Если  $a, b \in \mathbb{Q}$  и кубический многочлен имеет корень  $a + br$ , то он имеет рациональный корень.

**Теорема 2.1.4.** Если многочлен степени выше второй неприводим над  $\mathbb{Q}$ , то ни один из его корней не представим в виде  $a \pm \sqrt{b}$ , где  $a, b \in \mathbb{Q}$ .

## 2.2 Одно извлечение корня третьей степени

**2.2.1.** Представимо ли следующее число в виде  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ , где  $a, b, c \in \mathbb{Q}$ :

- (a)  $\sqrt{3}$ ; (b)  $\frac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$ ; (c)  $\cos(2\pi/9)$ ; (d)  $\sqrt[5]{3}$ ; (e)  $\sqrt[3]{3}$ ;  
 (f) наибольший вещественный корень многочлена  $x^3 - 4x + 2$ ;  
 (g)\* единственный вещественный корень многочлена  $x^3 - 6x - 6$ ;  
 (h)\* единственный вещественный корень многочлена  $x^3 - 9x - 12$ ?

**Лемма 2.2.2.** Пусть  $r \in \mathbb{R} - \mathbb{Q}$  и  $r^3 \in \mathbb{Q}$ .

- (a) **О неприводимости.** Многочлен  $x^3 - r^3$  неприводим над  $\mathbb{Q}$ .  
 (b) **О линейной независимости.** Если  $a, b, c \in \mathbb{Q}$  и  $a + br + cr^2 = 0$ , то  $a = b = c = 0$ .

(b') **О линейной независимости над  $\mathbb{Q}[\varepsilon_3]$ .** Если

$$k, l, m \in \mathbb{Q}[\varepsilon_3] := \{u + v\varepsilon_3 : u, v \in \mathbb{Q}\}$$

и  $k + lr + mr^2 = 0$ , то  $k = l = m = 0$ .

(c) Если многочлен имеет корень  $r$ , то этот многочлен делится на  $x^3 - r^3$ .

(d) **О сопряжении.** Если многочлен имеет корень  $r$ , то корнями этого многочлена являются также числа  $\varepsilon_3 r$  и  $\varepsilon_3^2 r$ .

(e) **О сопряжении.** Если  $a, b, c \in \mathbb{Q}$  и многочлен имеет корень  $x_0 := a + br + cr^2$ , то корнями этого многочлена являются также числа

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{и} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2.$$

(f) **О рациональности.** Если  $a, b, c \in \mathbb{Q}$ , то число  $a + br + cr^2$  является корнем некоторого ненулевого многочлена степени 3.

**Теорема 2.2.3.** Пусть многочлен неприводим над  $\mathbb{Q}$  и либо его степень отлична от 3 и 1, либо он имеет более одного вещественного корня. Тогда ни один из его корней не представим в виде  $a + br + cr^2$ , где  $r \in \mathbb{R} - \mathbb{Q}$  и  $a, b, c, r^3 \in \mathbb{Q}$ .

**Лемма 2.2.4** (о расширении). Число, вещественно радикальное с извлечением корня только один раз, причём третьей степени, имеет вид  $a + br + cr^2$ , где  $r \in \mathbb{R}$  и  $a, b, c, r^3 \in \mathbb{Q}$ .

## 2.3 Одно извлечение корня простой степени

**2.3.1.** Представимо ли следующее число в виде

$$a_0 + a_1 \sqrt[7]{2} + a_2 \sqrt[7]{2^2} + \dots + a_6 \sqrt[7]{2^6},$$

где  $a_0, a_1, a_2, \dots, a_6 \in \mathbb{Q}$ ?

- (a)  $\sqrt{3}$ ; (b)  $\cos \frac{2\pi}{21}$ ; (c)  $\sqrt[11]{3}$ ; (d)  $\sqrt[7]{3}$ ;  
 (e) какой-нибудь из корней многочлена  $x^7 - 4x + 2$ .

**Лемма 2.3.2.** Пусть  $q$  простое,  $r \in \mathbb{R} - \mathbb{Q}$  и  $r^q \in \mathbb{Q}$ .

- (a) **О неприводимости.** Многочлен  $x^q - r^q$  неприводим над  $\mathbb{Q}$ .  
 (b) **О линейной независимости.** Если  $A$  — многочлен степени меньше  $q$  и  $A(r) = 0$ , то  $A = 0$ .

(c) **О сопряжении.** Если многочлен имеет корень  $r$ , то он имеет также корни  $r\epsilon_q^k$  для каждого  $k = 1, 2, 3, \dots, q-1$ .

(d) **О рациональности.** Если  $A$  — многочлен, то число  $A(r)$  является корнем некоторого ненулевого многочлена степени не выше  $q$ .

Обозначим

$$\mathbb{Q}[\epsilon_q] := \{a_0 + a_1\epsilon_q + a_2\epsilon_q^2 + \dots + a_{q-2}\epsilon_q^{q-2} : a_0, \dots, a_{q-2} \in \mathbb{Q}\}.$$

**2.3.3.** Пусть  $q$  простое,  $r \in \mathbb{C} - \mathbb{Q}[\epsilon_q]$  и  $r^q \in \mathbb{Q}[\epsilon_q]$ .

- (a) Многочлен  $x^q - r^q$  неприводим над  $\mathbb{Q}[\epsilon_q]$ .  
 (b), (c) Докажите аналоги пунктов (b), (c) предыдущей задачи для многочлена с коэффициентами в  $\mathbb{Q}[\epsilon_q]$ .

**Лемма 2.3.4.** \* Пусть  $q$  простое,  $r \in \mathbb{R} - \mathbb{Q}$  и  $r^q \in \mathbb{Q}$ .

(a) **О неприводимости над  $\mathbb{Q}[\epsilon_q]$ .** Многочлен  $x^q - r^q$  неприводим над  $\mathbb{Q}[\epsilon_q]$ .

(b) **О линейной независимости над  $\mathbb{Q}[\epsilon_q]$ .** Если  $A$  — многочлен степени меньше  $q$  с коэффициентами в  $\mathbb{Q}[\epsilon_q]$  и  $A(r) = 0$ , то  $A = 0$ .

**Теорема 2.3.5.** Пусть многочлен неприводим над  $\mathbb{Q}$  и либо его степень отлична от простого  $q$  и от 1, либо он имеет более одного вещественного корня. Тогда ни один из его корней не представим в виде  $A(r)$  для некоторых  $r \in \mathbb{R} - \mathbb{Q}$  и многочлена  $A \in \mathbb{Q}[x]$ , причём  $r^q \in \mathbb{Q}$ .

**Лемма 2.3.6** (о расширении). Число, вещественно радикальное с извлечением корня только один раз, равно  $A(r)$  для некоторых  $A \in \mathbb{Q}[x]$  и  $r \in \mathbb{R}$ , причём  $r^q \in \mathbb{Q}$  для некоторого  $q \in \mathbb{Z}$ .

Таким образом, если многочлен простой степени, большей 2, неприводим над  $\mathbb{Q}$  и имеет более одного вещественного корня, то ни один из этих корней не является вещественно радикальным с извлечением корня только один раз.

## 2.4 Несколько извлечений квадратных корней

**2.4.1.** Существуют ли рациональные числа  $a, b, c, d$ , для которых  $\sqrt[3]{2}$  равно

$$(a) \ a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}; \quad (b) \ \frac{a + \sqrt{b}}{c + \sqrt{b}}; \quad (c) \ a + \sqrt{b} + \sqrt{c};$$

$$(d) \ a + \sqrt{b + \sqrt{c}}; \quad (e) \ a + \sqrt{b} + \sqrt{c} + \sqrt{d}?$$

**2.4.2.** (a) Число  $\sqrt[3]{2}$  не является вещественно радикальным с извлечением корней только квадратных и только два раза.

(b) Число  $\cos(2\pi/9)$  не является вещественно радикальным с извлечением корней только два раза.

Если  $F \subset \mathbb{C}$ ,  $r \in \mathbb{C}$  и  $r^q \in F$  для некоторого целого положительного  $q$ , то обозначим

$$F[r] := \{a_0 + a_1r + a_2r^2 + \dots + a_{q-1}r^{q-1} \mid a_0, \dots, a_{q-1} \in F\}.$$

В этом тексте **полем** называется подмножество множества  $\mathbb{C}$ , замкнутое относительно операций сложения, умножения, вычитания и деления на ненулевое число. Общепринятое название: числовое поле (а *полем* в математике называется более общий объект). Это понятие полезно для нас тем, что теорема деления с остатком верна для многочленов с коэффициентами в поле.

**Лемма 2.4.3** (о радикальном расширении). Если число  $a \in \mathbb{C}$  радикально, то некоторое содержащее его поле можно получить из

$\mathbb{Q}$  следующими операциями: заменить поле  $F$  на  $F[r]$  для некоторого  $r \in \mathbb{C}$  такого, что  $r^q \in F$  для некоторого простого  $q$ .

**2.4.4.** (a–d) Докажите аналоги утверждений 2.3.2.(a–d) с заменой  $\mathbb{Q}$  на произвольное поле и многочлены над  $\mathbb{Q}$  на многочлены над этим полем.

**Лемма 2.4.5.** Пусть  $q$  простое,  $F \subset \mathbb{R}$  — поле,  $r \in \mathbb{R} - F$  и  $r^q \in F$ . Если многочлен с коэффициентами в  $F$  степени 3 имеет три вещественных корня, ни один из которых не лежит в  $F$ , то ни один из его корней не лежит в  $F[r]$ .

## 2.5 К теореме Кронекера

В этом пункте  $q > 2$  — простое число,  $r \in \mathbb{C}$  — комплексное число,  $F \subset \mathbb{C}$  — поле, содержащее  $\varepsilon = \varepsilon_q$  и  $r^q$ , но не содержащее  $r$ .

**Лемма 2.5.1.** (a) **Неприводимость.** Многочлен  $t^q - r^q \in F[t]$  неприводим над  $F$ .

(b) **Линейная независимость.** Если  $P(r) = 0$  для некоторого многочлена  $P \in F[t]$  степени меньше  $q$ , то  $P = 0$ .

(c) **Сопряжение.** Если  $P(r) = 0$  для некоторого многочлена  $P \in F[t]$ , то  $P(r\varepsilon^k) = 0$  для любого  $k = 1, \dots, q-1$ .

(d) **Параметрическое сопряжение.** Если  $P \in F[x, t]$ , причём  $P(x, r) = 0$  как многочлен от  $x$ , то  $P(x, r\varepsilon^k) = 0$  как многочлен от  $x$  при любом  $k = 0, 1, \dots, q-1$ .

(e) **Рациональность.** Для любого  $H \in F[x, t]$  верно, что

$$H(x, r)H(x, \varepsilon r) \dots H(x, \varepsilon^{q-1}r) \in F[x].$$

(f) **Вещественность.** Пусть  $F = \overline{F}$ , а также  $r \in \mathbb{R}$  или  $|r|^2 \in F$ . Тогда среди значений  $A(r\varepsilon^k)$  многочлена  $A \in F[t]$  при  $k = 0, 1, \dots, q-1$  либо не более одно является вещественным, либо все эти значения вещественны.

**2.5.2.** (a) Пусть  $H \in F[x, t]$  и  $H(x, r)$  неприводим над  $F[r]$ . Тогда для любого  $k = 0, 1, \dots, q-1$  многочлен  $H(x, r\varepsilon^k)$  также неприводим над  $F[r]$ .

(b) Пусть  $H \in F[x, t]$  и  $H(x, r)$  — неприводимый над  $F[r]$  множитель над  $F[r]$  неприводимого над  $F$  многочлена  $G \in F[x]$ , причем

$0 < \deg H(x, r) < \deg G$ . Тогда  $G$  делится над  $F$  на произведение

$$H(x, r)H(x, \varepsilon r) \dots H(x, \varepsilon^{q-1}r).$$

(с) Если в условиях п. (b)  $\deg G$  простое, то существует такой многочлен  $A \in F[t]$ , что корни многочлена  $G$  равны  $A(r\varepsilon^k)$  при  $k = 0, 1, \dots, q-1$ .

**Лемма 2.5.3** (о сохранении неприводимости). Пусть  $F = \overline{F}$ , а также  $r \in \mathbb{R}$  или  $|r|^2 \in F$ , причем многочлен  $G \in F[t]$  простой степени имеет более одного вещественного корня и не менее одного не вещественного. Если при этом  $G$  неприводим над  $F$ , то  $G$  неприводим над  $F[r]$ .

**Лемма 2.5.4** (о хитром радикальном расширении). (а) Если число  $a \in \mathbb{C}$  радикально, то некоторое содержащее его поле можно получить из  $\mathbb{Q}$  следующими операциями: заменить поле  $F$  на  $F[r]$  для некоторого  $r \in \mathbb{C}$ , такого, что  $r \in \mathbb{R}$  или  $|r|^2 \in F$ , причем  $r^q \in F$  для некоторого простого  $q$ .

(b) То же, что в п. (а), с заменой  $r^q \in F$  на  $r^q, \varepsilon \in F$ .

В доказательстве п. (b) можно использовать без доказательства следующий результат (его элементарное доказательство на одной странице см. в [ZSS, §5], [Sk21m, §8.4.D], [Sk21y]).

**Теорема 2.5.5** (теорема Гаусса о понижении степени). Если  $q$  простое, то число  $\varepsilon$  радикально с использованием лишь корней степени  $q-1$ .

## 2.6 Решения задач до промежуточного финиша

**2.1.1. Ответы:** (а), (b), (с) — да, (d), (е), (f), (g), (h) — нет.

(а), (с) Имеем  $\sqrt{3+2\sqrt{2}} = \sqrt[3]{7+5\sqrt{2}} = 1 + \sqrt{2}$ .

(b) Имеем  $\frac{1}{7+5\sqrt{2}} = \frac{7-5\sqrt{2}}{7^2-2\cdot 5^2} = -7 + 5\sqrt{2}$ .

(d) Пусть число  $\sqrt[3]{2}$  представимо. Тогда

$$2 = (\sqrt[3]{2})^3 = (a^3 + 3ab) + (3a^2 + b)\sqrt{b}.$$

Так как  $3a^2 + b \neq 0$ , то  $\sqrt{b} \in \mathbb{Q}$ . Значит,  $\sqrt[3]{2} \in \mathbb{Q}$  — противоречие.

Другой способ — аналогично теореме 2.1.4.

(е) *Набросок первого решения.* Предположим противное и возведем в куб равенство  $\sqrt[3]{2} = a + \sqrt{b} - \sqrt{2}$ .

*Набросок второго решения.* Докажем, что

$$\sqrt[3]{2} \neq a + p\sqrt{b} + q\sqrt{c} + r\sqrt{bc} \quad \text{ни для каких } a, b, c, p, q, r \in \mathbb{Q}.$$

Для этого достаточно доказать, что  $\sqrt[3]{2} \neq u + v\sqrt{c}$  ни для каких чисел  $u, v, c \in \mathbb{Q}[\sqrt{b}] := \{x + y\sqrt{b} : x, y \in \mathbb{Q}\}$ . Идея доказательства состоит в том, что числа из  $\mathbb{Q}[\sqrt{b}]$  (с фиксированным  $b$ ) «ничуть не хуже» рациональных чисел, т. е. сумма, разность, произведение и частное чисел из  $\mathbb{Q}[\sqrt{b}]$  тоже являются числами из  $\mathbb{Q}[\sqrt{b}]$  (или, говоря научно,  $\mathbb{Q}[\sqrt{b}]$  — *числовое поле*). Поэтому можно доказывать утверждение аналогично утверждению (d).

*Набросок третьего решения.* Пусть  $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$  для некоторых  $a, b \in \mathbb{Q}$ . Это число является корнем многочлена  $P(x) := ((x - \sqrt{2})^3 - 2)((x + \sqrt{2})^3 - 2)$  с рациональными коэффициентами. По лемме о сопряжении 2.1.3 (е) для  $r = \sqrt{b}$ , многочлен  $P$  имеет корень  $a - \sqrt{b}$ . Так как  $\sqrt{b} \notin \mathbb{Q}$ , то корни  $a \pm \sqrt{b}$  различны. Но у многочлена  $P$  только два вещественных корня:  $\sqrt{2} + \sqrt[3]{2}$  и  $-\sqrt{2} + \sqrt[3]{2}$ . Поэтому  $a + \sqrt{b} = \sqrt{2} + \sqrt[3]{2}$  и  $a - \sqrt{b} = -\sqrt{2} + \sqrt[3]{2}$ . Отсюда  $\sqrt[3]{2} = a \in \mathbb{Q}$ . Противоречие.

(f) *Набросок первого решения.* Предположим противное и возведем в квадрат равенство  $\sqrt{2} + \sqrt{2} = a + \sqrt{b}$ .

*Набросок второго решения.* Корнями многочлена  $P(x) := (x^2 - 2)^2 - 2$  являются четыре числа  $\pm\sqrt{2} \pm \sqrt{2}$ , где знаки  $+$  и  $-$  обязательно согласованы. Все эти числа иррациональны. Значит, по теореме 2.1.4 достаточно доказать, что многочлен  $P$  не разлагается в произведение двух квадратных трехчленов с рациональными коэффициентами. Эта неразложимость следует из того, что произведение любых двух корней многочлена  $P$  иррационально.

(h) Пусть число  $\cos(2\pi/9)$  представимо. Тогда оно является корнем уравнения  $4x^3 - 3x = -\frac{1}{2}$ . По следствию 2.1.3(f) это уравнение имеет рациональный корень. Противоречие.

**2.1.2.** Обозначим через  $\sqrt{c}$  число, полученное при единственном извлечении корня, где  $c \in \mathbb{Q}$ . Докажем, что все полученные числа имеют вид  $a + b\sqrt{c}$ , где  $a, b \in \mathbb{Q}$ . Достаточно доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания,



умножения и деления. Это неочевидно только в случае деления, для которого оно следует из равенства  $(a+b\sqrt{c})(a-b\sqrt{c}) = a^2 - b^2c$ .

**2.1.3.** (а) Если многочлен  $x^2 - r^2$  приводим над  $\mathbb{Q}$ , то он имеет рациональный корень. Противоречие.

(б) Если  $b \neq 0$ , то  $r = -a/b \in \mathbb{Q}$ , что невозможно. Поэтому  $b = 0$ , а значит,  $a = 0$ .

(с) Поделим многочлен с остатком<sup>1</sup> на  $x^2 - r^2$ :

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

Подставляя  $x = r$ , по лемме о линейной независимости (см. п. (б)) получаем, что остаток нулевой.

(d) Из п. (с) следует, что если  $R^2 = r^2$ , то  $R$  есть корень многочлена.

(е) Обозначим через  $P$  многочлен из условия, и пусть  $G(t) := P(a+bt)$ . Тогда  $G(r) = 0$ . Значит, по пункту (d) имеем  $G(-r) = 0$ .

(f) Если  $b = 0$ , то утверждение доказано. В противном случае по п. (е) многочлен имеет (различные) корни  $a \pm br$ , значит третий корень рационален по теореме Виета.

**2.1.4.** Пусть, напротив, данный многочлен  $P$  имеет корень  $x_0 = a \pm \sqrt{b}$ , где  $\sqrt{b} \notin \mathbb{Q}$ . По лемме 2.1.3 (е) о сопряжении и аналогично ей, корнем многочлена  $P$  является также число  $x_1 = a \mp \sqrt{b}$ . При  $b = 0$  утверждение очевидно. Поэтому считаем, что  $b \neq 0$ . Тогда  $x_0 \neq x_1$ . Значит,  $P(x)$  делится на  $(x - a)^2 - b$ . Так как  $\deg P > 2$ , то многочлен  $P$  приводим. Противоречие.

**2.2.1.** *Ответы:* (а), (с), (d), (е), (f), (h) — нет, (b), (g) — да.

Обозначим  $r := \sqrt[3]{2}$ .

(а) Пусть число  $\sqrt{3}$  представимо.

*Первое решение.* Тогда

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Так как многочлен  $x^3 - 2$  не имеет рациональных корней, то он неприводим над  $\mathbb{Q}$ . Значит,  $2ab + 2c^2 = 2ac + b^2 = 0$  (ср. с задачей

---

<sup>1</sup>Это деление с остатком — то же самое, что «замена»  $x^2$  на  $r^2$ .

2.2.2 (b)). Поэтому  $b^3 = -2abc = 2c^3$ . Тогда либо  $b = c = 0$ , либо  $\sqrt[3]{2} = b/c$ . Оба случая невозможны.

*Второе решение.* Обозначим  $P(x) := x^2 - 3$ . По лемме 2.2.2 (е) о сопряжении  $P$  имеет три корня  $x_0, x_1, x_2$ , введённых в формулировке леммы. Так как ни один из них не рационален, то равенство  $b = c = 0$  невозможно. Значит, по лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_3]$  2.2.2 (b') эти корни различны. Противоречие.

(b) Имеем  $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$ . (Это равенство несложно получить методом неопределённых коэффициентов или при помощи алгоритма Евклида для многочленов  $x^3 - 2$  и  $x^2 + 5x + 1$ , см. решение задачи 2.2.4.) Поэтому

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(c) Пусть число  $\cos(2\pi/9)$  представимо. Оно является корнем уравнения  $4x^3 - 3x = -\frac{1}{2}$ . Два других его вещественных корня есть  $\cos(8\pi/9)$  и  $\cos(4\pi/9)$ .

Применим второе решение пункта (а) для  $P(x) := 8x^3 - 6x - 1$ . Получим, что корни  $x_0, x_1, x_2$  различны. Так как  $\overline{\varepsilon_3} = \varepsilon_3^2$ , то  $\overline{x_2} = x_1$ . Значит,  $x_2$  и  $x_1$  не могут быть вещественными и различными. Противоречие.

(f) Доказательство аналогично п. (c).

**2.2.2.** (а) Если многочлен  $x^3 - r^3$  приводим над  $\mathbb{Q}$ , то он имеет рациональный корень. Противоречие.

(b) Предположим противное. Поделим  $x^3 - r^3$  на  $a + bx + cx^2$  с остатком. По п. (а) остаток ненулевой. Оба многочлена  $x^3 - r^3$  и  $a + bx + cx^2$  имеют корень  $x = r$ . Значит, остаток имеет корень  $x = r$ . Следовательно, остаток имеет иррациональный корень. Противоречие с тем, что степень остатка равна 1.

(b') Рассмотрите вещественную и мнимую части.

*Замечание.* Это утверждение равносильно неприводимости многочлена  $x^3 - r^3$  над  $\mathbb{Q}[\varepsilon_3]$ . Если многочлен  $x^3 - r^3$  неприводим над  $\mathbb{Q}[\varepsilon_3]$ , то многочлен  $k + lx + mx^2 \in \mathbb{Q}[\varepsilon_3][x]$  не может иметь корень  $r$ . Если многочлен  $x^3 - r^3$  приводим над  $\mathbb{Q}[\varepsilon_3]$ , то один из сомножителей даёт линейную зависимость чисел  $1, r, r^2$  над  $\mathbb{Q}[\varepsilon_3]$ .

(с) Поделим многочлен с остатком на  $x^3 - r^3$ . Подставляя  $x = r$ , по лемме о линейной независимости п. (b) получаем, что остаток нулевой.

(d) По п. (с) получаем, что если  $R^3 = r^3$ , то  $R$  есть корень многочлена.

(е) Обозначим через  $P$  многочлен из условия, и пусть  $G(t) := P(a + bt + ct^2)$ . Тогда  $G(r) = 0$ . Значит, по п. (d) имеем  $G(r\epsilon_3) = 0 = G(r\epsilon_3^2)$ .

(f) *Первое доказательство.* Достаточно доказать утверждение для  $a = 0$ . Для числа  $t = br + cr^2$  выполнено равенство  $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$ .

Иными словами, ввиду того, что  $u^3 + v^3 + w^3 - 3uvw$  делится на  $u + v + w$ , число  $a + br + cr^2$  является корнем многочлена

$$(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6.$$

*Второе доказательство.* Обозначим  $x_0 = a + br + cr^2$ . Разложим числа  $x_0^k$  при  $k = 0, 1, 2, 3$  по степеням числа  $r$ :

$$x_0^k = a_k + b_k r + c_k r^2.$$

Достаточно найти числа  $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$ , не все из которых равны нулю, удовлетворяющие условию  $\lambda_0 + \lambda_1 x_0 + \lambda_2 x_0^2 + \lambda_3 x_0^3 = 0$ . Для этого нужно, чтобы эти числа удовлетворяли системе уравнений

$$\begin{cases} \lambda_0 a_0 + \dots + \lambda_3 a_3 = 0, \\ \lambda_0 b_0 + \dots + \lambda_3 b_3 = 0, \\ \lambda_0 c_0 + \dots + \lambda_3 c_3 = 0. \end{cases}$$

Как известно, однородная (т. е. с нулевыми правыми частями) система линейных уравнений с рациональными коэффициентами, в которой уравнений меньше, чем переменных, имеет нетривиальное рациональное решение. Значит, требуемые числа найдутся.

Полученный многочлен имеет степень ровно 3 ввиду лемм 2.2.2 (е, в').

*Третье доказательство.* Обозначим  $A(x) := a + bx + cx^2$ . Произведение  $(x - A(t_0))(x - A(t_1))(x - A(t_2))$  является симметрическим многочленом от  $t_0, t_1, t_2$ . Значит, оно является многочленом от  $x$

и от элементарных симметрических многочленов от  $t_0, t_1, t_2$ . Значения этих элементарных симметрических многочленов при  $t_k = r\varepsilon_3^k$ ,  $k = 0, 1, 2$ , равны коэффициентам многочлена  $x^3 - r^3$ , которые рациональны. Поэтому рассмотренное произведение является искомым многочленом.

**2.2.4.** Пусть при извлечении корня третьей степени получилось число  $r$ . Если  $|r| \in \mathbb{Q}$ , то утверждение очевидно. Если  $|r| \notin \mathbb{Q}$ , то многочлен  $x^3 - r^3$  неприводим над  $\mathbb{Q}$ .

Достаточно доказать, что  $\frac{1}{a+br+cr^2} = h(r)$  для некоторого многочлена  $h$ . По лемме о неприводимости, многочлен  $x^3 - r^3$  неприводим над  $\mathbb{Q}$ . Поэтому он взаимно прост с  $a+bx+cx^2$ . Значит, существуют многочлены  $g$  и  $h$ , для которых  $h(x)(a+bx+cx^2) + g(x)(x^3 - r^3) = 1$ . Тогда  $h$  — искомый многочлен.

**2.3.2.** (а) Все корни многочлена  $x^q - r^q$  есть  $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$ . Пусть он приводим над  $\mathbb{Q}$ . Модуль свободного члена одного из унитарных сомножителей разложения рационален и равен произведению модулей некоторых  $k$  из этих корней,  $0 < k < q$ . Значит,  $r^k \in \mathbb{Q}$ . Так как  $q$  простое, то имеем  $kx + qy = 1$  для некоторых целых  $x, y$ . Тогда  $r = (r^k)^x (r^q)^y \in \mathbb{Q}$ . Противоречие.

(b) Предположим противное. Рассмотрим многочлен  $A(x)$  наименьшей степени, для которого лемма не выполняется. Поделим  $x^q - r^q$  на  $A(x)$  с остатком  $R(x)$ . Тогда  $\deg R < \deg A$ ,  $R(r) = 0$  и по п. (а) многочлен  $R(x)$  ненулевой. Противоречие с выбором многочлена  $A$ .

(с) Доказательство аналогично задачам 2.1.3 (с, d), 2.2.2 (d). Используйте п. (b).

(d) Доказательства повторяют второе и третье доказательства леммы о рациональности 2.2.2 (f). Нужно только везде заменить 3 на  $q$  и 2 на  $q - 1$  (например, во второй строчке второго доказательства  $k = 0, 1, 2, \dots, q$ ).

## 2.7 Решения остальных задач

**1.2.3.** (а,с) Это следует из Теорем 1.2.2.b,a, соответственно.

**1.3.1.** (с,d) Используйте *методы дель Ферро и Феррари* [Sk21m, §3].

**2.2.1.** (d) Если число  $\sqrt[5]{3}$  представимо, то по лемме о рациональности 2.2.2 (f) оно является корнем некоторого кубического многочлена. Противоречие с неприводимостью многочлена  $x^5 - 3$  над  $\mathbb{Q}$ .

(е) Аналогично п. (а), (с) получаем, что комплексные корни многочлена  $x^3 - 3$  есть числа  $x_0, x_1, x_2$ , введённые в формулировке леммы 2.2.2 (е). Поэтому  $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$  для некоторого  $s \in \{1, 2\}$ . Отсюда по лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_3]$  2.2.2 (b') получаем, что  $a = 0$  и  $bs = 0$ . Поэтому либо  $\sqrt[3]{3} = br$ , либо  $\sqrt[3]{3} = cr^2$ . Противоречие.

**2.2.3.** По лемме о рациональности 2.2.2 (f) существует многочлен степени не выше 3 с корнем  $a + br + cr^2$ . Из этого факта и из неприводимости над  $\mathbb{Q}$  данного многочлена  $P$  получаем, что  $\deg P \leq 3$ . По лемме о сопряжении 2.2.2 (е) многочлен  $P$  имеет три корня  $x_0, x_1, x_2$ , введённых в формулировке леммы. Так как многочлен  $P$  неприводим над  $\mathbb{Q}$ , то ни один из корней не рационален. Поэтому равенство  $b = c = 0$  невозможно. Значит, по лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_3]$  2.2.2 (b') корни  $x_0, x_1, x_2$  различны. Следовательно,  $\deg P = 3$ .

Так как  $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$ , то  $\overline{x_2} = x_1$ . Значит,  $x_2$  и  $x_1$  не могут быть вещественными и различными. Следовательно,  $x_2, x_1 \in \mathbb{C} - \mathbb{R}$ . Поэтому  $P$  имеет ровно один вещественный корень.

**2.3.1.** Обозначим  $r := \sqrt[7]{2}$  и  $A(x) := a_0 + a_1x + a_2x^2 + \dots + a_6x^6$ .

(а) Пусть число  $\sqrt{3}$  представимо. Тогда по лемме о сопряжении 2.3.2 (с) многочлен  $x^2 - 3$  имеет корни  $A(r\varepsilon_7^k)$  для  $k = 0, 1, 2, \dots, 6$ . Так как этот многочлен не имеет рациональных корней, то по лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_7]$  2.3.4 (b) эти корни различны. Противоречие.

(b) Обозначим через  $P$  многочлен, для которого  $\cos 7x = P(\cos x)$ . (Докажите, что такой многочлен существует!)

*Первое решение.* Пусть число  $\cos \frac{2\pi}{21}$  представимо. Аналогично п. (а) данный многочлен  $P$  имеет попарно различные корни  $x_k :=$

$A(r\varepsilon_7^k)$  для  $k = 0, 1, 2, \dots, 6$ . Так как  $P(0) > 0$ ,  $P(1) < 0$  и  $P(2) > 0$ , то многочлен  $P$  имеет вещественный корень  $x_k$ , отличный от  $x_0$ . Имеем  $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$ . Поэтому  $x_k = \overline{x_k} = x_{7-k}$ . Противоречие.

*Второе решение.* Корнями многочлена  $2P(x) + 1$  являются вещественные числа  $y_k := \cos \frac{2(3k+1)\pi}{21}$  при  $k = 0, \dots, 6$ . Одно из них, а именно  $y_2 = -1/2$ , рационально.

В следующем абзаце мы докажем, что число  $y_0$  иррационально.

(Иначе из равенства  $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$  следует, что  $\varepsilon_{21} = a + i\sqrt{b}$  для некоторых  $a, b \in \mathbb{Q}$ . Тогда и число  $\varepsilon_7 = \varepsilon_{21}^3$  тоже имеет такой вид. Но  $\varepsilon_7$  является корнем неприводимого<sup>2</sup> многочлена  $1 + x + \dots + x^6$ , что противоречит аналогу теоремы 2.1.4 для чисел вида  $a + i\sqrt{b}$ .)

Итак, число  $y_0$  иррационально и является корнем многочлена  $\frac{2P(x)+1}{2x+1}$  степени 6. Тогда по леммам о сопряжении 2.3.2 (с) и о линейной независимости над  $\mathbb{Q}[\varepsilon_q]$  2.3.4 (b) этот многочлен имеет семь попарно различных корней, что невозможно.

(с) Пусть число  $\sqrt[11]{3}$  представимо. Тогда по лемме о рациональности 2.3.2 (d) существует ненулевой многочлен степени не выше 7 с корнем  $\sqrt[11]{3}$ . Противоречие с неприводимостью многочлена  $x^{11} - 3$  над  $\mathbb{Q}$ .

(d) Пусть число  $\sqrt[7]{3}$  представимо. Аналогично п. (а) все комплексные корни многочлена  $x^7 - 3$  есть  $A(r\varepsilon_7^k)$  для  $k = 0, 1, 2, \dots, 6$ . Поэтому  $A(r)\varepsilon_7^s = A(r\varepsilon_7)$  для некоторого  $s \in \{1, 2, 3, 4, 5, 6\}$ . Отсюда по лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_q]$  2.3.4 (b)  $a_k = 0$  для любого  $k \neq s$ . Поэтому  $\sqrt[7]{3} = a_s r^s$ . Противоречие.

(е) Пусть какой-нибудь из корней представим. Данный многочлен  $P$  не имеет рациональных корней. Тогда по лемме о сопряжении 2.3.2.с и лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_q]$  2.3.4. b  $P$  имеет попарно различные корни  $x_k := A(r\varepsilon_7^k)$  для  $k = 0, 1, 2, \dots, 6$ . Так как  $P(0) > 0$ ,  $P(1) < 0$  и  $P(2) > 0$ , то  $P$  имеет вещественный корень  $x_k$ , отличный от  $x_0$ . Имеем  $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$ . Поэтому  $x_k = \overline{x_k} = x_{7-k}$ . Противоречие.

---

<sup>2</sup>Неприводимость многочлена  $g(x) = 1 + x + \dots + x^6$  можно показать, например, применив признак Эйзенштейна к многочлену  $g(x+1)$ . Впрочем, здесь достаточно доказать, что у него нет рациональных делителей степени 1 и 2.

**2.3.3.** (а) Пусть многочлен приводим. Свободный член одного из унитарных сомножителей разложения лежит в  $\mathbb{Q}[\varepsilon_q]$  и равен  $\pm r^k \varepsilon_q^m$  для некоторого  $m$ . Поэтому  $r^k \in \mathbb{Q}[\varepsilon_q]$ . Далее аналогично лемме 2.3.2 (а) получаем  $r \in \mathbb{Q}[\varepsilon_q]$ . Противоречие.

Пункты (b) и (с) выводятся из п. (а) аналогично соответствующим пунктам задачи 2.3.2.

**2.3.5.** Предположим противное. Обозначим данный многочлен через  $P$ . При  $q < \deg P$  получаем противоречие с леммой о рациональности 2.3.2 (d). При  $q \geq \deg P$  по лемме о сопряжении 2.3.2 (с) и лемме о линейной независимости над  $\mathbb{Q}[\varepsilon_q]$  2.3.4 (b) многочлен  $P$  имеет попарно различные корни  $x_k = A(r\varepsilon_q^k)$  для  $k = 0, 1, 2, \dots, q-1$ . При  $q > \deg P$  получаем противоречие. При  $q = \deg P$  из условий  $q \neq 2$  и  $\overline{x_k} = x_{q-k} \neq x_k$  получаем единственность вещественного корня.

**2.4.1.** *Ответы:* нет. Доказательства аналогичны решениям задач 2.1.1.(e,g). (а) *Первое решение.* Перепишем условие в виде  $(a + c\sqrt{2}) + (b + d\sqrt{2})\sqrt[4]{2} = 0$ . Так как  $b + d\sqrt{2} \neq 0$ , то  $-\sqrt[4]{2} = \frac{a+c\sqrt{2}}{b+d\sqrt{2}} = A + B\sqrt{2}$  для некоторых  $A, B \in \mathbb{Q}$ . Возводя в квадрат, получаем  $A^2 + 2B^2 = 0$ . Противоречие.

*Второе решение.* Рассматривая все комплексные корни многочлена  $x^4 - 2$ , докажем его неприводимость над  $\mathbb{Q}$ . Поэтому он не может иметь общий корень с многочленом  $a + bx + cx^2 + dx^3$  не более чем третьей степени.

(b) Домножьте на сопряжённое.

(с) Проще доказать сразу, что  $\sqrt[3]{2} \neq a + p\sqrt{b} + q\sqrt{c} + r\sqrt{bc}$ , где  $a, b, c, p, q, r \in \mathbb{Q}$ . Для этого достаточно доказать, что  $\sqrt[3]{2} \neq u + v\sqrt{c}$ , где  $u$  и  $v$  - числа вида  $\alpha + \beta\sqrt{b}$ ,  $\alpha, \beta \in \mathbb{Q}$  (с фиксированным  $b$ ) "ничуть не хуже" рациональных чисел, т.е. сумма, разность, произведение и частное чисел такого вида тоже являются числами такого вида (или, говоря научно, такие числа будут образовывать *числовое поле*). Поэтому можно доказывать утверждение аналогично 2.1.1(e).

**2.4.2** (а) Докажем более сильный факт: число  $\sqrt[3]{2}$  не является радикальным с извлечением любого количества квадратных корней.

Тогда существует такая башня квадратичных расширений

$$\mathbb{Q} = F_1 \subset F_1 \subset F_2 \subset F_3 \subset \dots F_{s-1} \subset F_s \subset \mathbb{R},$$

что  $\sqrt[3]{2} \in F_s - F_{s-1}$ . Поскольку  $\sqrt[3]{2} \notin \mathbb{Q}$ , получаем, что  $s \geq 2$ . Значит,

$$\sqrt[3]{2} = \alpha + \beta\sqrt{a}, \quad \text{где } \alpha, \beta, a \in F_{s-1}, \quad \sqrt{a} \notin F_{s-1} \quad \text{и} \quad \beta \neq 0.$$

Отсюда

$$2 = (\sqrt[3]{2})^3 = (\alpha^3 + 3\alpha\beta^2a) + (3\alpha^2\beta + \beta^3a)\sqrt{a} = u + v\sqrt{a}.$$

Поскольку  $2 \in \mathbb{Q} \subset F_{s-1}$ , имеем  $2 - u \in F_{s-1}$ . Из того, что

$$v\sqrt{a} = 2 - u \quad \text{и} \quad v \in F_{s-1},$$

следует равенство

$$0 = v = 3\alpha^2\beta + \beta^3a.$$

Так как  $3\alpha^2 + \beta^2a > 0$ , то  $\beta = 0$ . Противоречие.

Решения остальных задач можно найти в [ZSS, §9.1, §9.4.5, §9.4.7] (это §5.1, §5.4.3, §5.4.4 бумажной версии). В частности, доказательства теорем 1.2.2.а и 1.3.3 приведены в [ZSS, §9.4.5, §9.4.7], соответственно.

## Список литературы

- [Al] *Алексеев В. Б.* Теорема Абеля. М.: Наука, 1976.
- [ABG] Solving equations using one radical, presented by D. Akhtyamov, I. Bogdanov, A. Glebov, A. Skopenkov, E. Streltsova and A. Zysin. <http://www.turgor.ru/1ktg/2015/4/index.htm>.
- [Ay82] *R. G. Ayoub*, On the Nonsolvability of the General Polynomial, Amer. Math. Monthly, 89:6 (1982), 397–401.
- [Be06] *J. Bewersdorff*, Galois Theory for Beginners: A Historical Perspective, AMS, 2006.



- [Be10] *J. Bergen*, A Concrete Approach to Abstract Algebra: From the Integers to the Insolvability of the Quintic, 2010.
- [Br] *J. Brown*, Abel and the insolvability of the quintic, <http://www.math.caltech.edu/~jim1b/abel.pdf>.
- [Do65] *H. Dörrie*, 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.
- [Ed84] *H. M. Edwards*, Galois Theory. Springer Verlag, 1984.
- [FT] *Табачников С. Л., Фукс Д. Б.* Математический дивертисмент, М.: МЦНМО, 2011. <http://www.math.psu.edu/tabachni/Books/taaba.pdf>
- [Ha78] *Ch. R. Hadlock*, Field Theory and its Classical Problems. The Mathematical Association of America, 1978.
- [Le11] *L. Lerner*, Galois Theory without abstract algebra. <http://arxiv.org/abs/1108.4593>.
- [PC19] *Y. Pan and Y. Chen*. On Kronecker's Solvability Theorem, <http://arxiv.org/abs/1912.07489>.
- [Pe04] *P. Pesic*, Abel's Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.
- [Pr07] *Прасолов В. В.* Задачи по алгебре, арифметике и анализу. М.: МЦНМО, 2007.
- [Ro95] *M. I. Rosen*, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.
- [Sk08] *Скопенков А.* Ещё несколько доказательств из Книги: разрешимость и неразрешимость уравнений в радикалах. <http://arxiv.org/abs/0804.4357>.
- [Sk10] *Скопенков А.* Базисные вложения и 13-я проблема Гильберта, Мат. Просвещение, 14 (2010) 143–174; <http://arxiv.org/abs/1001.4011>.

- [Sk11] *Скопенков А.* Простое доказательство теоремы Абеля о неразрешимости уравнений в радикалах, Мат. Просвещение, 15 (2011), 113–126; <http://arxiv.org/abs/1102.2100>.
- [Sk15] *A. Skopenkov*, A short elementary proof of the Ruffini-Abel Theorem. <http://arxiv.org/abs/1508.03317>.
- [Sk21m] *A. Skopenkov*. Mathematics Through Problems: from olympiades and math circles to a profession. Part I. Algebra. 2021, AMS, Providence. Preliminary version: [https://www.mccme.ru/circles/oim/algebra\\_eng.pdf](https://www.mccme.ru/circles/oim/algebra_eng.pdf)
- [Sk21y] *Скопенков А.* Еще одно доказательство из книги: теорема Гаусса-Ванцеля, Мат. Просвещение, 2021.
- [St94] *J. Stillwell*, Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22–27.
- [Ti03] *Тихомиров В. М.* Абель и его великая теорема, Квант. 2003. N1, 11–15.
- [Va] *Вагутен Н.* Сопряжённые числа, Квант. 1980. N2, 26–32.
- [ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии. Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. Изд-во МЦНМО, 2018. Abridged version: <http://www.mccme.ru/circles/oim/materials/sturm.pdf>.

# Kronecker's proof of Galois insolvability theorem

presented by D. Gerasimov, E. Kogan,  
E. Morozov, Y. Pan, A. Skopenkov\*

## Contents

1	Introduction and main results . . . . .	2
1.1	Overview and motivation . . . . .	2
1.2	Insolvability in real radicals . . . . .	3
1.3	Insolvability in complex radicals . . . . .	4
1.4	Recommendations for participants . . . . .	5
2	Proofs as sequences of problems . . . . .	6
2.1	Representations using only one square root . . . . .	6
2.2	Representations using only one cubic root . . . . .	7
2.3	Representations using only one root of prime order . . . . .	8
2.4	Multiple root extractions . . . . .	9
2.5	Towards the proof of Kronecker's theorem . . . . .	10
2.6	Solutions of some problems before the semifinal . . . . .	11
2.7	Solutions of other problems . . . . .	15

---

\*We are grateful to V. Volkov for useful discussions.

D. Gerasimov: Phystex-Lyceum (Dolgoprudnyi).

E. Kogan, E. Morozov: Higher School of Economics (Moscow).

Y. Pan: Henan Institute of Science and Technology (China).

A. Skopenkov: Moscow Institute of Physics and Technology, Independent University of Moscow. <https://users.mccme.ru/skopenko/>.

*And the leap is not — is not what I think you sometimes see it as — as breaking, as acting. It's something much more like a quiet transition after a lot of patience and — tension of thought, yes — but with that [enlightenment] as its discipline, its orientation, its truth. Not confusion and chaos and immolation and pulling the house down, not something experienced as a great significant moment.*

I. Murdoch, The Message to the Planet

## 1 Introduction and main results

### 1.1 Overview and motivation

This subsection is formally not used later.

We present a short exposition of Kronecker's proof of the well-known Galois theorem 1.3.2 on insolubility of algebraic equations in radicals. This proof is interesting because it is presumably the shortest.

We do not use the terms 'Galois group' and even 'group'. However, our presentation is hopefully a nicely paved shortcut to the edge of Galois theory. In the proof of the main result we introduce the idea of conjugation. This is an important particular case of 'field isomorphism' sufficient for the main result. So this project provides a bridge (by showing that there is no gap) between elementary mathematics and Galois theory.

The project is accessible to students familiar with polynomials and complex numbers (permutations are not involved).

We claim no novelty (except possibly expository novelty). The idea of proof presented here is known [Do65, §25], [Pr07, Ti03] and is presumably due to Kronecker. (A mistake in these expositions [Sk21m, Remark 8.4.18b] is corrected in expositions [Sk08, PC19], [Sk21m, §8].) Unfortunately, this proof is not well-known.

The proof presented is also interesting because it does not involve permutations. Thus as the 'reason' for the insolubility we see not that the group  $A_5$  of even permutations is not solvable, but that there is a degree 5 polynomial with rational coefficients irreducible over  $\mathbb{Q}$ , having more than one real root and having at least one non-real root. So this proof is different from other proofs of Galois and Abel theorems

presented in [Al04, Ay82, Be10, Be06, Br, Ed84, FT, Ha78, Le11, PC19, Pe04, Ro95, St94, Sk15] (see comments and corrections of some mistakes in [Sk15]).

## 1.2 Insolubility in real radicals

A real number is called **expressible in real radicals** if it can be obtained using number 1 and operations of addition, subtraction, multiplication, division by a non-zero number, and taking the  $n$ -th root of a positive number, where  $n$  is a positive integer. In other words, a real number  $a$  is expressible in real radicals if some set containing this number can be obtained starting from the set  $\{1\}$  and using the following operations. To a given set  $M \subset \mathbb{R}$  containing numbers  $x, y \in M$  one can add

numbers  $x + y, x - y, xy$ , number  $x/y$  when  $y \neq 0$ ,

and number  $\sqrt[n]{x}$  for  $x > 0$  and integer  $n > 0$ .

**1.2.1.** (a) Any real root of a quadratic equation with rational coefficients is expressible in real radicals.

(b) The equation  $x^3 + x + 1 = 0$  has exactly one real root which is expressible in real radicals.

(c) The equation  $x^4 + 4x - 1 = 0$  has two real roots; both of them are expressible in real radicals.

**Theorem 1.2.2.** (a) The number  $\cos(2\pi/9)$  is not expressible in real radicals.

(b) There exists a cubic polynomial with rational coefficients (for example,  $x^3 - 3x + 1$ ) none of whose roots is expressible in real radicals.

You can prove part (b) of this theorem after solving the problems before the semifinal. You can use without proof part (b) for other problems (only) of §1.2.

**1.2.3.** (a) For any  $n \geq 3$  there exists a polynomial of degree  $n$  with rational coefficients, one of whose roots is not expressible in real radicals.

(b)\* The analogue of (a) with the words ‘one of the roots is not expressible’ replaced by ‘none of the roots is expressible’ is correct. (At

the same time, the roots of *some* equations of high degrees, for example,  $x^5 = 2$ , may well be expressible in real radicals.)

(c) The trisection of an angle is impossible in real radicals. That is, there exists a number  $\alpha$  (for example,  $\alpha = 2\pi/3$ ) such that the number  $\cos \alpha$  is expressible in real radicals and the number  $\cos(\alpha/3)$  is not expressible in real radicals.

### 1.3 Insolvability in complex radicals

A complex number is called **expressible in radicals** if it can be obtained using number 1 and operations of addition, subtraction, multiplication, division by a non-zero number and taking the  $n$ -th root, where  $n$  is a positive integer. In other words, a complex number  $a$  is expressible in radicals if some set containing this number can be obtained starting from the set  $\{1\}$  and using the following operations. To a given set  $M \subset \mathbb{C}$  containing numbers  $x, y \in M$  one can add

numbers  $x + y, x - y, xy$ ,    number  $x/y$  when  $y \neq 0$ ,

and any number  $r \in \mathbb{C}$  such that  $r^n = x$  for some integer  $n > 0$ .

**1.3.1.** (a) Any (complex) root of a quadratic equation with rational coefficients is expressible in radicals.

(b) The number  $\cos(2\pi/9)$  is expressible in radicals.

(c,d) Same as (a) for equations of 3-rd and 4-th degree.

(e) If the real and the imaginary part of a complex number  $z$  are expressible in real radicals, then  $z$  is expressible in radicals.

(f) The converse to (e) is incorrect.

Analogous assertions to (a,c,d) for equations of higher degrees do not hold.

**Theorem 1.3.2** (Galois). There exists an equation of 5-th degree with rational coefficients (for example,  $x^5 - 4x + 2 = 0$ ) none of whose roots is expressible in radicals.

The famous problem of solvability in radicals was solved by weaker Ruffini-Abel theorems proved a little earlier. Their rigorous statements are more complicated [Sk21m, Ruffini Theorem 8.2.2], [Sk15, Remark 7]. An easier way to solve the solvability problem is presented

in [Sk21m, Theorem 8.1.13 and its proof in §8.4.F]. Here we present an alternative short way: deduction of Galois Theorem 1.3.2 from the following result.

**Theorem 1.3.3** (Kronecker). If a polynomial with rational coefficients is irreducible over  $\mathbb{Q}$  and has prime degree, has more than one real root and has at least one non-real root, then the polynomial has no roots expressible in radicals.

This theorem is interesting and nontrivial even for polynomials of degree 5. You can prove this theorem after solving the problems after the semifinal.

## 1.4 Recommendations for participants

For every solution which has been written down and marked with either ‘+’ or ‘+.’ a student (or a group of students) get 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. One may submit a solution in oral form, but one loses a bean with each 5 attempts (successful or not).

If a mathematical fact is formulated as a problem, then the objective is to prove this fact. (Open-ended questions are called challenges or riddles; here one must come up with a clear wording, and a proof.) If a problem is marked by bold and named ‘theorem’ (‘lemma’, ‘corollary’, etc.), then this statement is important. Usually we provide (as a problem) the *formulation* of beautiful or important statement *before* its *proof*. In this case to prove this statement one possibly needs to solve next problems. If you are stuck on a certain problem, try looking at the next ones. They may turn out to be helpful. We advise all the students working on the project to *consult* the jury on any questions on the project. Students who successfully work on the project will get interesting *extra problems*.

Please notify us if you already know solutions of several problems. If you confirm your knowledge by presenting some of them, you will be allowed not to receive plus-marks for their solutions, but to use them in solutions of other problems.

## 2 Proofs as sequences of problems

In this text ‘polynomial with rational coefficients’ is called a ‘polynomial’. Denote

$$\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q).$$

### 2.1 Representations using only one square root

**2.1.1.** Can the following number be represented as  $a + \sqrt{b}$  with  $a, b \in \mathbb{Q}$ :

- (a)  $\sqrt{3 + 2\sqrt{2}}$ ; (b)  $\frac{1}{7+5\sqrt{2}}$ ; (c)  $\sqrt[3]{7 + 5\sqrt{2}}$ ; (d)  $\sqrt[3]{2}$ ;  
 (e)  $\sqrt{2} + \sqrt[3]{2}$ ; (f)  $\sqrt{2 + \sqrt{2}}$ ; (g)  $\sqrt{2} + \sqrt{3} + \sqrt{5}$ ; (h)  $\cos(2\pi/9)$ ?

Observe that for (g) you would need ideas from §2.4.

**Lemma 2.1.2** (Extension). Suppose we can obtain a number using number 1, several operations of addition, subtraction, multiplication, division by a non-zero number and exactly one operation of taking the square root of a positive number. Then the number can be represented as  $a \pm \sqrt{b}$ , where  $a, b \in \mathbb{Q}$  and  $b > 0$ .

**Lemma 2.1.3.** Assume that  $r \in \mathbb{R} - \mathbb{Q}$  and  $r^2 \in \mathbb{Q}$ .

- (a) **Irreducibility.** The polynomial  $x^2 - r^2$  is irreducible over  $\mathbb{Q}$ .  
 (b) **Linear independence.** If  $a, b \in \mathbb{Q}$  and  $a + br = 0$ , then  $a = b = 0$ .  
 (c) If  $r$  is a root of a polynomial, then this polynomial is divisible by  $x^2 - r^2$ .  
 (d) **Conjugation.** If  $r$  is a root of a polynomial, then  $-r$  is also its root.  
 (e) **Conjugation.** If  $a, b \in \mathbb{Q}$  and a polynomial has a root  $a + br$ , then  $a - br$  is also a root of this polynomial.  
 (f) If  $a, b \in \mathbb{Q}$  and a cubic polynomial has a root  $a + br$ , then this polynomial has a rational root.

**Theorem 2.1.4.** If a polynomial of degree at least 3 is irreducible over  $\mathbb{Q}$ , then none of its roots equals to  $a \pm \sqrt{b}$  for some  $a, b \in \mathbb{Q}$ .



## 2.2 Representations using only one cubic root

**2.2.1.** Can the following number be represented as  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$  with  $a, b, c \in \mathbb{Q}$ :

- (a)  $\sqrt{3}$ ; (b)  $\frac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$ ; (c)  $\cos(2\pi/9)$ ; (d)  $\sqrt[5]{3}$ ; (e)  $\sqrt[3]{3}$ ;
- (f) the maximal real root of  $x^3 - 4x + 2 = 0$ ;
- (g)\* the unique real root of  $x^3 - 6x - 6 = 0$ ;
- (h)\* the unique real root of  $x^3 - 9x - 12 = 0$ ?

**Lemma 2.2.2.** Assume that  $r \in \mathbb{R} - \mathbb{Q}$  and  $r^3 \in \mathbb{Q}$ .

- (a) **Irreducibility.** The polynomial  $x^3 - r^3$  is irreducible over  $\mathbb{Q}$ .
- (b) **Linear independence.** If  $a + br + cr^2 = 0$  with  $a, b, c \in \mathbb{Q}$ , then  $a = b = c = 0$ .

(b') **Linear independence over  $\mathbb{Q}[\varepsilon_3]$ .** If

$$k, \ell, m \in \mathbb{Q}[\varepsilon_3] := \{u + v\varepsilon_3 : u, v \in \mathbb{Q}\}$$

and  $k + \ell r + mr^2 = 0$ , then  $k = \ell = m = 0$ .

(c) If  $r$  is a root of a polynomial, then this polynomial is divisible by  $x^3 - r^3$ .

(d) **Conjugation.** If  $r$  is a root of a polynomial, then the numbers  $\varepsilon_3 r$  and  $\varepsilon_3^2 r$  are also its roots.

(e) **Conjugation.** If  $a, b, c \in \mathbb{Q}$  and a polynomial has root  $x_0 := a + br + cr^2$ , then the numbers

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{and} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2$$

are also its roots.

(f) **Rationality.** If  $a, b, c \in \mathbb{Q}$ , then the number  $a + br + cr^2$  is a root of some cubic polynomial.

**Theorem 2.2.3.** Suppose an irreducible polynomial either has more than one real root or its degree is not equal to 1 or 3. Then this polynomial has no root  $a + br + cr^2$  for any  $r \in \mathbb{R} - \mathbb{Q}$ ,  $a, b, c, r^3 \in \mathbb{Q}$ .

**Lemma 2.2.4** (Extension). A number expressible in real radicals with only one extraction of a cubic root can be represented as  $a + br + cr^2$ , where  $r \in \mathbb{R}$  and  $a, b, c, r^3 \in \mathbb{Q}$ .

## 2.3 Representations using only one root of prime order

**2.3.1.** Can the following number be represented in the form

$$a_0 + a_1 \sqrt[7]{2} + a_2 \sqrt[7]{2^2} + \cdots + a_6 \sqrt[7]{2^6}$$

with  $a_0, a_1, a_2, \dots, a_6 \in \mathbb{Q}$ :

- (a)  $\sqrt{3}$ ; (b)  $\cos \frac{2\pi}{21}$ ; (c)  $\sqrt[11]{3}$ ; (d)  $\sqrt[7]{3}$ ;  
 (e) some root of the polynomial  $x^7 - 4x + 2$ ?

**Lemma 2.3.2.** Let  $q$  be a prime number,  $r \in \mathbb{R} - \mathbb{Q}$  and  $r^q \in \mathbb{Q}$ .

- (a) **Irreducibility.** The polynomial  $x^q - r^q$  is irreducible over  $\mathbb{Q}$ .  
 (b) **Linear independence.** If  $r$  is a root of a polynomial  $A$  whose degree is less than  $q$ , then  $A = 0$ .

(c) **Conjugation.** If  $r$  is a root of a polynomial, then all the numbers  $r\varepsilon_q^k$ ,  $k = 1, 2, 3, \dots, q-1$ , are also roots of this polynomial.

(d) **Rationality.** If  $A$  is a polynomial, then the number  $A(r)$  is a root of some nonzero polynomial which degree is at most  $q$ .

Denote

$$\mathbb{Q}[\varepsilon_q] := \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \cdots + a_{q-2}\varepsilon_q^{q-2} : a_0, \dots, a_{q-2} \in \mathbb{Q}\}.$$

**2.3.3.** Let  $q$  be a prime number,  $r \in \mathbb{C} - \mathbb{Q}[\varepsilon_q]$  and  $r^q \in \mathbb{Q}[\varepsilon_q]$ .

- (a) The polynomial  $x^q - r^q$  is irreducible over  $\mathbb{Q}[\varepsilon_q]$ .  
 (b), (c) Prove the analogues of parts (b,c) of the previous problem for a polynomial with coefficients in  $\mathbb{Q}[\varepsilon_q]$ .

**Lemma 2.3.4.** \* Let  $q$  be a prime number,  $r \in \mathbb{R} - \mathbb{Q}$  and  $r^q \in \mathbb{Q}$ .

(a) **Irreducibility over  $\mathbb{Q}[\varepsilon_q]$ .** The polynomial  $x^q - r^q$  is irreducible over  $\mathbb{Q}[\varepsilon_q]$ .

(b) **Linear independence over  $\mathbb{Q}[\varepsilon_q]$ .** If  $A$  is a polynomial of degree less than  $q$  with coefficients in  $\mathbb{Q}[\varepsilon_q]$  and  $A(r) = 0$ , then  $A = 0$ .

**Theorem 2.3.5.** Let  $q$  be a prime. Suppose an irreducible over  $\mathbb{Q}$  polynomial  $P$  either has more than one real root or its degree is not equal to 1 or  $q$ . Then there are no polynomial  $A \in \mathbb{Q}[x]$  and number  $r \in \mathbb{R} - \mathbb{Q}$  such that  $r^q \in \mathbb{Q}$  and  $A(r)$  is a root of  $P$ .

**Lemma 2.3.6** (Extension). Any number expressible in real radicals with only one root extraction is equal to  $A(r)$  for some  $r \in \mathbb{R}$ ,  $q \in \mathbb{Z}$  and  $A \in \mathbb{Q}[x]$ , with  $r^q \in \mathbb{Q}$ .

Thus if a polynomial of prime degree  $q > 2$  is irreducible over  $\mathbb{Q}$  and has more than one real roots, then none of these roots is expressible in radicals with only one root extraction.

## 2.4 Multiple root extractions

**2.4.1.** Are there rational numbers  $a, b, c, d$  for which  $\sqrt[3]{2}$  is equal to

(a)  $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$ ;    (b)  $\frac{a + \sqrt{b}}{c + \sqrt{b}}$ ;    (c)  $a + \sqrt{b} + \sqrt{c}$ ;

(d)  $a + \sqrt{b + \sqrt{c}}$ ;    (e)  $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$ ?

**2.4.2.** (a) The number  $\sqrt[3]{2}$  is not expressible in radicals with only two extractions of square roots.

(b) The number  $\cos(2\pi/9)$  is not expressible in radicals with only two root extractions.

If  $F \subset \mathbb{C}$ ,  $r \in \mathbb{C}$  and  $r^q \in F$  for some positive integer  $q$ , then let

$$F[r] := \{a_0 + a_1r + a_2r^2 + \cdots + a_{q-1}r^{q-1} \mid a_0, \dots, a_{q-1} \in F\}.$$

In this text a **field** is a subset of  $\mathbb{C}$  which is closed under summation, subtraction, multiplication and division by a non-zero number. The conventional name is ‘number field’ (the technical term ‘field’ in mathematics refers to a more general object). This notion is useful for us because the Polynomial Remainder Theorem holds for polynomials with coefficients in a field.

**Lemma 2.4.3** (Simple Radical Extension). If a number  $a \in \mathbb{C}$  is expressible in radicals, then some field containing  $a$  can be obtained from  $\mathbb{Q}$  using only the following operations: replace a field  $F$  by  $F[r]$  for  $r \in \mathbb{C}$  and a prime  $q$  such that  $r^q \in F$ .

**2.4.4.** (a–d) Prove the analogues of Assertions 2.3.2.(a–d) with  $\mathbb{Q}$  replaced by a field, and with polynomials over  $\mathbb{Q}$  replaced by polynomials over the field.

**Lemma 2.4.5.** Let  $q$  be a prime,  $F \subset \mathbb{R}$  a field,  $r \in \mathbb{R} - F$  and  $r^q \in F$ . If a polynomial with coefficients in  $F$  has degree 3, has three real roots none of which lies in  $F$ , then none of the roots lies in  $F[r]$ .

## 2.5 Towards the proof of Kronecker's theorem

In this subsection  $q > 2$  is a prime,  $r \in \mathbb{C}$  a number,  $\varepsilon = \varepsilon_q$  and  $F \subset \mathbb{C}$  a field containing  $r^q, \varepsilon$  but not  $r$ .

**Lemma 2.5.1.** (a) **Irreducibility.** The polynomial  $t^q - r^q \in F[t]$  is irreducible over  $F$ .

(b) **Linear independence.** If  $P(r) = 0$  for some polynomial  $P \in F[t]$  of degree less than  $q$ , then  $P = 0$ .

(c) **Conjugation.** If  $P(r) = 0$  for some polynomial  $P \in F[t]$ , then  $P(r\varepsilon^k) = 0$  for every  $k = 1, \dots, q-1$ .

(d) **Parametric conjugation.** If  $P \in F[x, t]$  and  $P(x, r) = 0$  as a polynomial in  $x$ , then  $P(x, r\varepsilon^k) = 0$  as a polynomial in  $x$  for every  $k = 0, 1, \dots, q-1$ .

(e) **Rationality.** For any  $H \in F[x, t]$  we have

$$H(x, r)H(x, \varepsilon r) \dots H(x, \varepsilon^{q-1}r) \in F[x].$$

(f) **Reality.** If  $F = \overline{F}$  and either  $r \in \mathbb{R}$  or  $|r|^2 \in F$ , then either among the values  $A(r\varepsilon^k)$ ,  $k = 0, 1, \dots, q-1$ , of a polynomial  $A \in F[t]$  at most one is real, or all these values are real.

**2.5.2.** (a) Suppose that  $H \in F[x, t]$  is a polynomial such that  $H(x, r)$  is irreducible over  $F[r]$ . Then for any  $k = 0, 1, \dots, q-1$  the polynomial  $H(x, r\varepsilon^k)$  is irreducible over  $F[r]$  as well.

(b) Let  $G \in F[x]$  be an irreducible over  $F$  polynomial. Suppose that  $H \in F[x, t]$  is a polynomial such that  $0 < \deg H < \deg G$  and  $H(x, r)$  is an irreducible over  $F[r]$  factor of  $G$ . Then  $G$  is divisible in  $F$  by the product

$$H(x, r)H(x, \varepsilon r) \dots H(x, \varepsilon^{q-1}r).$$

(c) If in addition to the assumptions of (b)  $\deg G$  is a prime, then there is a polynomial  $A \in F[t]$  such that the roots of  $G$  are  $A(r\varepsilon^k)$  for  $k = 0, 1, \dots, q-1$ .

**Lemma 2.5.3** (Keeping Irreducibility). Let  $r \in \mathbb{C}$  be a number. Suppose that  $F = \overline{F}$  and either  $r \in \mathbb{R}$  or  $|r|^2 \in F$ . Take a polynomial  $G \in F[t]$  of prime degree which has more than one real root and has at least one non-real root. If  $G$  is irreducible over  $F$ , then  $G$  is irreducible over  $F[r]$ .

**Lemma 2.5.4** (Hard Radical Extension). (a) If a number  $a \in \mathbb{R}$  is expressible in radicals, then some field containing  $a$  can be obtained from  $\mathbb{Q}$  using only the following operations: replace a field  $F$  by  $F[r]$  for  $r \in \mathbb{C}$  such that either  $r \in \mathbb{R}$  or  $|r|^2 \in F$ , and  $r^q \in F$  for a prime  $q$ .

(b) Same as (a) with  $r^q \in F$  replaced by  $r^q, \varepsilon \in F$ .

In 2.5.4(b) you can use the following result without proof. For an elementary one-page proof see [Sk21m, §8.4.D].

**Theorem 2.5.5** (Gauss Lowering Degree Theorem). If  $q$  is a prime, then the number  $\varepsilon$  is expressible in radicals using only roots of degree  $q - 1$ .

## 2.6 Solutions of some problems before the semifinal

**1.2.2.** (a) Apply the triple-angle formula for cosine. We see that the numbers  $\cos(2\pi/9)$ ,  $\cos(8\pi/9)$ ,  $\cos(14\pi/9)$  are the roots of the equation  $8y^3 - 6y + 1 = 0$ . By (b) none of these numbers is expressible in real radicals.

**1.2.3.** (a,c) This follows from Theorems 1.2.2.b,a, respectively.

**1.3.1.** (c,d) Use *del Ferro and Ferrari methods* [Sk21m, §3].

**2.1.2.** It would suffice to prove that the set of all numbers of the form  $a \pm \sqrt{b}$  is closed under operations of addition, subtraction, multiplication and division. This is obviously false:  $(1 + \sqrt{2}) + (1 + \sqrt{3})$  cannot be represented as  $a \pm \sqrt{b}$ , where  $a, b \in \mathbb{Q}$  (prove this!).

**2.1.1. Answers:** (a), (b), (c) — yes, (d), (e), (f), (g) — no.

(a), (c) We have  $\sqrt{3 + 2\sqrt{2}} = \sqrt[3]{7 + 5\sqrt{2}} = 1 + \sqrt{2}$ .

(b) We have  $\frac{1}{7 + 5\sqrt{2}} = \frac{7 - 5\sqrt{2}}{7^2 - 2 \cdot 5^2} = -7 + 5\sqrt{2}$ .

(d) Assume that  $\sqrt[3]{2}$  is representable in this form. Then

$$2 = (\sqrt[3]{2})^3 = (a^3 + 3ab) + (3a^2 + b)\sqrt{b}.$$

Since  $3a^2 + b \neq 0$ , we have  $\sqrt{b} \in \mathbb{Q}$ . Thus  $\sqrt[3]{2} \in \mathbb{Q}$ , which is a contradiction.

(e) *Sketch of the first solution.* It is easier to prove the stronger assertion:

$$\sqrt[3]{2} \neq a + p\sqrt{b} + q\sqrt{c} + r\sqrt{bc} \quad \text{for any } a, b, c, p, q, r \in \mathbb{Q}.$$

It suffices to show that  $\sqrt[3]{2} \neq u + v\sqrt{c}$  for any  $u, v, c \in \mathbb{Q}[\sqrt{b}] := \{x + y\sqrt{b} : x, y \in \mathbb{Q}\}$ . The idea of our proof is that numbers from  $\mathbb{Q}[\sqrt{b}]$  (with  $b$  fixed) are ‘as good as’ rational numbers. That is, the sum, the difference, the product and the quotient of the numbers from  $\mathbb{Q}[\sqrt{b}]$  are also the numbers from  $\mathbb{Q}[\sqrt{b}]$  (the common terminology:  $\mathbb{Q}[\sqrt{b}]$  is a number field). Then we can prove the assertion similarly to (d).

*Sketch of the second solution.* Assume that  $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$  for some  $a, b \in \mathbb{Q}$ . This number is a root of the polynomial  $P(x) = ((x - \sqrt{2})^3 - 2)((x + \sqrt{2})^3 - 2)$  having rational coefficients. We have  $\sqrt{2} + \sqrt[3]{2} \notin \mathbb{Q}$  (prove this!). Hence  $\sqrt{b} \notin \mathbb{Q}$ . By the Conjugation Lemma 2.1.3 (e) for  $r = \sqrt{b}$  we have  $P(a - \sqrt{b}) = 0$ . Since  $\sqrt{b} \notin \mathbb{Q}$ , then roots  $a \pm \sqrt{b}$  are different. The polynomial  $P$  has only two real roots, namely  $\sqrt{2} + \sqrt[3]{2}$  and  $-\sqrt{2} + \sqrt[3]{2}$ . Thus  $a + \sqrt{b} = \sqrt{2} + \sqrt[3]{2}$  and  $a - \sqrt{b} = -\sqrt{2} + \sqrt[3]{2}$ . Therefore  $\sqrt[3]{2} = a \in \mathbb{Q}$ . This is a contradiction.

(f) The roots of the polynomial  $P(x) = (x^2 - 2)^2 - 2$  are four numbers of the form  $\pm\sqrt{2 \pm \sqrt{2}}$ , where the signs need not agree. All these numbers are irrational. From Theorem 2.1.4 it follows that it is sufficient to prove that the polynomial  $P$  cannot be written as a product of two quadratic polynomials with rational coefficients. This irreducibility follows from the fact that the product of any two roots of  $P$  is irrational.

(g) See [Sk21m, Problem 8.3.1(g)].

(h) See [Sk21m, Problem 8.3.3( $n = 9$ )].

**2.1.2.** It would suffice to prove that the set of all numbers of the form  $a \pm \sqrt{b}$  is closed under operations of addition, subtraction, multiplication and division. This is obviously false:  $(1 + \sqrt{2}) + (1 + \sqrt{3})$  cannot be represented as  $a \pm \sqrt{b}$ , where  $a, b \in \mathbb{Q}$  (prove this!).

**2.1.3.** (a) If the polynomial  $x^2 - r^2$  is reducible over  $\mathbb{Q}$ , then it has a rational root. This is a contradiction.

(b) If  $b \neq 0$ , then  $r = -a/b \in \mathbb{Q}$ , which is impossible. Hence  $b = 0$ , thus  $a = 0$ .

(c) Divide our polynomial with a remainder<sup>1</sup> by  $x^2 - r^2$ :

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

---

<sup>1</sup>The division with a remainder is equivalent to ‘replacing’  $x^2$  by  $r^2$ .

Substitute  $x = r$ . By the Linear Independence Lemma (see (b)) the remainder is zero.

(d) By (c) if  $R^2 = r^2$ , then  $R$  is a root of the polynomial.

(e) Let  $P$  be given polynomial, and set  $G(t) := P(a + bt)$ . Then  $G(r) = 0$ . Hence by (d) we obtain  $G(-r) = 0$ .

(f) If  $b = 0$  the assertion is proved. Otherwise by (e) the polynomial has the roots  $a \pm br$ . These roots are distinct. Hence the third root is rational by the Vieta Theorem.

**2.1.4.** Suppose to the contrary that the given polynomial  $P$  has a root  $x_0 = a \pm \sqrt{b}$ , where  $b \notin \mathbb{Q}$ . By the Conjugation Lemma 2.1.3.e and analogously to it, the number  $x_1 = a \mp \sqrt{b}$  is also a root of  $P$ . Since  $\sqrt{b} \notin \mathbb{Q}$ , we have  $b \neq 0$ . Then  $x_0 \neq x_1$ . Therefore  $P$  is divisible by  $(x - a)^2 - b$ . Since  $\deg P > 2$ , the polynomial  $P$  is reducible. This is a contradiction.

**2.2.1. Answers:** (a), (c), (d), (e), (f), (h) — no, (b), (g) — yes.

Denote  $r := \sqrt[3]{2}$ .

(a) Assume that  $\sqrt{3}$  is representable in this form.

*First solution.* Then

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Since the polynomial  $x^3 - 2$  has no rational roots, it is irreducible over  $\mathbb{Q}$ . Thus,  $2ab + 2c^2 = 2ac + b^2 = 0$  (cf. 2.2.2.b). So we have  $b^3 = -2abc = 2c^3$ . Hence either  $b = c = 0$  or  $\sqrt[3]{2} = b/c$ . Both cases are impossible.

*Second solution.* Denote  $P(x) := x^2 - 3$ . By the Conjugation Lemma 2.2.2 (e),  $P$  has three roots  $x_0, x_1, x_2$  defined in the statement of the lemma. Since none of them is rational, the equality  $b = c = 0$  does not hold. So by the Linear Independence Lemma over  $\mathbb{Q}[\varepsilon_3]$  2.2.2 (b') the three roots are distinct. This is a contradiction.

(b) We have  $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$ . (This equality can be easily obtained by the undetermined coefficients method or applying Euclid algorithm to  $x^3 - 2$  and  $x^2 + 5x + 1$ , see solution of 2.2.4.) Therefore,

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(c) Assume that  $\cos(2\pi/9)$  is representable in this form. This number is a root of the equation  $4x^3 - 3x = -\frac{1}{2}$ . Its other two real roots are  $\cos(8\pi/9)$  and  $\cos(4\pi/9)$ .

**2.2.2.** (a) Suppose that  $x^3 - r^3$  is reducible over  $\mathbb{Q}$ . Then it has a rational root. This is a contradiction.

(b) Assume the contrary. Divide  $x^3 - r^3$  by  $a + bx + cx^2$  with a remainder. By (a), the remainder is nonzero. Both polynomials  $x^3 - r^3$  and  $a + bx + cx^2$  have a root  $x = r$ . Hence the remainder has the root  $x = r$ . Thus, the remainder has an irrational root. This is impossible because the remainder has degree 1.

(b') Consider the real and the imaginary parts separately.

(c) Divide our polynomial by  $x^3 - r^3$  with a remainder. Taking  $x = r$  and applying Linear Independence Lemma (b), we get that the remainder is zero.

(d) By (c), if  $R^3 = r^3$ , then  $R$  is a root of our polynomial.

(e) Let  $P$  be the given polynomial, and set  $G(t) := P(a + bt + ct^2)$ . Then  $G(r) = 0$ . Hence by (d) we have  $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$ .

(f) *First solution.* Taking  $x = y + a$  we see that it suffices to prove the assertion for  $a = 0$ . The number  $t = br + cr^2$  satisfies  $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$ .

In other words, since  $u^3 + v^3 + w^3 - 3uvw$  is divisible by  $u + v + w$ , the number  $a + br + cr^2$  is a root of the polynomial

$$(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6.$$

*Second solution.* Denote  $x_0 := a + br + cr^2$ . Expand the numbers  $x_0^k$ ,  $k = 0, 1, 2, 3$ , as polynomials in  $r$ :

$$x_0^k = a_k + b_k r + c_k r^2.$$

It suffices to find numbers  $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$ , not all zeros, such that  $\lambda_0 + \lambda_1 x_0 + \lambda_2 x_0^2 + \lambda_3 x_0^3 = 0$ . So, these numbers must satisfy the system of equations

$$\begin{cases} \lambda_0 a_0 + \dots + \lambda_3 a_3 = 0, \\ \lambda_0 b_0 + \dots + \lambda_3 b_3 = 0, \\ \lambda_0 c_0 + \dots + \lambda_3 c_3 = 0. \end{cases}$$



It is known that a homogeneous (i.e. with zero right-hand parts) system of linear equations with rational coefficients, where the number of equations is smaller than the number of variables, has a nontrivial rational solution. Hence, the required numbers exist.

The obtained polynomial has degree exactly 3 by lemmas 2.2.2 (e, b').

*Third solution.* Denote  $A(x) := a + bx + cx^2$ . The product  $(x - A(t_0))(x - A(t_1))(x - A(t_2))$  is a symmetric polynomial in  $t_0, t_1, t_2$ . Hence this product is a polynomial in  $x$  and the elementary symmetric polynomials in  $t_0, t_1, t_2$ . The values of these elementary symmetric polynomials at  $t_k = r\varepsilon_3^k$  ( $k = 0, 1, 2$ ) are the coefficients of the polynomial  $x^3 - r^3$ , and hence are rational. So the considered product is the required polynomial.

**2.2.4.** Assume that after extracting the third root we get number  $r$ . If  $|r| \in \mathbb{Q}$ , the statement is trivial. If  $|r| \notin \mathbb{Q}$ , then the polynomial  $x^3 - r^3$  is irreducible over  $\mathbb{Q}$ .

It suffices to prove that  $\frac{1}{a+br+cr^2} = h(r)$  for some polynomial  $h$ . By the Irreducibility Lemma, the polynomial  $x^3 - r^3$  is irreducible over  $\mathbb{Q}$ . Hence it is coprime with  $a + bx + cx^2$ . Therefore, there exist polynomials  $g$  and  $h$  such that  $h(x)(a + bx + cx^2) + g(x)(x^3 - r^3) = 1$ . Then  $h$  is the required polynomial.

**2.3.1.** *Answers: no.* The arguments are similar to those in the solutions of problems 2.2.1. Use lemmas stated below the problem.

**2.3.5.** The proof is analogous to the proofs of Theorems 2.1.4, 2.2.3 and to the solutions of 2.3.1 (abc).

**2.3.6.** The proof is similar to the proof of the Extension Lemma 2.2.4.

## 2.7 Solutions of other problems

**2.1.2.** Let  $\sqrt{c}$  be the number we obtain with only one extraction of the root, where  $c \in \mathbb{Q}$ . Prove that all the obtained numbers have the form  $a + b\sqrt{c}$  with  $a, b \in \mathbb{Q}$ .

**2.2.1.** (d) Assume that  $\sqrt[5]{3}$  is representable in this form. By the Rationality Lemma 2.2.2 (f),  $\sqrt[5]{3}$  is a root of a cubic polynomial. This

contradicts to the irreducibility of the polynomial  $x^5 - 3$  over  $\mathbb{Q}$ .

Repeat the second solution of (a) for  $P(x) := x^5 - 3$  has three roots  $x_1, x_2, x_3$ . all three roots are distinct. Therefore,  $x^5 - 3$  is divisible by  $(x - x_1)(x - x_2)(x - x_3)$ .

*First solution.* Expand the numbers  $1, 3^{1/5}, 3^{2/5}$ , and  $3^{3/5}$  as polynomials in  $r$ . We get that these four numbers are linearly dependent. This shows that there exists a nonzero polynomial of degree at most 3 having a root  $3^{1/5}$ . This contradicts the irreducibility of  $x^5 - 3$  over  $\mathbb{Q}$ .

(e) Analogously to (a) and (c), by the Conjugation Lemma 2.2.2 (e) it follows that the polynomial  $x^3 - 3$  has three roots  $x_0, x_1, x_2$  defined in the statement of the lemma. Thus,  $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$  for some  $s \in \{1, 2\}$ . By the Linear Independence Lemma over  $\mathbb{Q}[\varepsilon_3]$  2.2.2 (b') we have  $a = 0$  and  $bc = 0$ . Hence either  $\sqrt[3]{3} = br$  or  $\sqrt[3]{3} = cr^2$ . This is a contradiction.

(f) The proof is analogous to (c).

(g) This equation has a root  $\sqrt[3]{2} + \sqrt[3]{4}$ .

(h) The only real root of this equation is  $\sqrt[3]{3} + \sqrt[3]{9}$ . Assume that this number is representable in the required form. Repeat the second solution of (a) for  $P(x) := x^3 - 9x - 12$ . We obtain that  $x_0, x_1, x_2$  are all roots of  $P$ . On the other hand, by the del Ferro theorem all roots of  $P$  are

$$y_0 := \sqrt[3]{3} + \sqrt[3]{9}, \quad y_1 := \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_2 := \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

Since  $P$  has exactly one real root,  $x_0 = y_0$ . Then either  $x_1 = y_1$ ,  $x_2 = y_2$ , or  $x_2 = y_1$ ,  $x_1 = y_2$ .

Denote  $R(x) := \sqrt[3]{3}x + \sqrt[3]{9}x^2$  and let  $S(x) := a + brx + cr^2x^2$  or  $S(x) := a + brx^2 + cr^2x$  in the first and second case, respectively. Then the polynomial  $R(x) - S(x)$  has three distinct roots  $1, \varepsilon_3$ , and  $\varepsilon_3^2$ . But the degree of this polynomial is at most 2. Thus  $R = S$ . Hence either  $\sqrt[3]{3} = br$  or  $\sqrt[3]{3} = cr^2$ . A contradiction.

**2.2.3.** By the Rationality Lemma 2.2.2 (f) there exists a cubic polynomial having  $a + br + cr^2$  as a root. Since the given polynomial  $P$  is irreducible over  $\mathbb{Q}$  and has the same root, we conclude that  $\deg P \leq 3$ . By the Conjugation Lemma 2.2.2 (e),  $P$  has three roots  $x_0, x_1, x_2$  defined in the statement of the lemma. Since  $P$  is irreducible over  $\mathbb{Q}$ , none of its roots is rational. So the equality  $b = c = 0$  is impossible.

By the Linear Independence Lemma over  $\mathbb{Q}[\varepsilon_3]$  2.2.2 (b'),  $x_0, x_1, x_2$  are distinct. Hence  $\deg P = 3$ .

Since  $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$ , we have  $\overline{x_2} = x_1$ . Hence  $x_2$  and  $x_1$  cannot be real and distinct. So  $x_2, x_1 \in \mathbb{C} - \mathbb{R}$ . Then  $P$  has a unique real root.

**2.3.3.** See [Sk21m, Problem 8.3.23].

**2.3.4.** See [Sk21m, Problem 8.3.24].

**2.4.1.** See [Sk21m, Problem 8.3.9].

**2.4.2.** (a) See [Sk21m, Theorem 8.1.2].

(b) See [Sk21m, Theorem 8.1.5].

**2.4.3.** See [Sk21m, Lemma 8.4.1b].

**2.4.4.** (a,b,c) See [Sk21m, Lemma 8.4.14].

(d) See [Sk21m, Lemma 8.4.17].

**2.4.5.** See [Sk21m, Lemma 8.4.11a].

For solutions of the remaining problems see [Sk21m, Lemma 8.4.14, §8.4.E,G]. In particular, proofs of Theorems 1.2.2.a and 1.3.3 are presented in [Sk21m, §8.4.E,G], respectively.

## References

- [Al04] *V. B. Alekseev*, *Abel's Theorem in Problems and Solutions*. Springer Netherlands, 2004.
- [Ay82] *R. G. Ayoub*, On the Nonsolvability of the General Polynomial, *Amer. Math. Monthly*, 89:6 (1982), 397–401.
- [Be06] *J. Bewersdorff*, *Galois Theory for Beginners: A Historical Perspective*, AMS, 2006.
- [Be10] *J. Bergen*, *A Concrete Approach to Abstract Algebra: From the Integers to the Insolvability of the Quintic*, 2010.
- [Br] *J. Brown*, *Abel and the insolvability of the quintic*, <http://www.math.caltech.edu/~jim1b/abel.pdf>.
- [Do65] *H. Dörrie*, *100 Great Problems of Elementary Mathematics: Their History and Solution*. New York: Dover Publ, 1965.

- [Ed84] *H. M. Edwards*, Galois Theory. Springer Verlag, 1984.
- [FT] *D. Fuchs and S. Tabachnikov*, Mathematical Omnibus. AMS, 2007.
- [Ha78] *Ch. R. Hadlock*, Field Theory and its Classical Problems. The Mathematical Association of America, 1978.
- [Le11] *L. Lerner*, Galois Theory without abstract algebra. <http://arxiv.org/abs/1108.4593>.
- [PC19] *Y. Pan and Y. Chen*. On Kronecker’s Solvability Theorem, <http://arxiv.org/abs/1912.07489>.
- [Pe04] *P. Pesic*, Abel’s Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.
- [Pr07] *V. V. Prasolov*, Problems in algebra, arithmetics and analysis, Moscow, MCCME, 2007.
- [Ro95] *M. I. Rosen*, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.
- [Sk08] *A. Skopenkov*. Some more proofs from the Book: solvability and insolvability of equations in radicals, <http://arxiv.org/abs/0804.4357>.
- [Sk15] *A. Skopenkov*, A short elementary proof of the Ruffini-Abel Theorem. <http://arxiv.org/abs/1508.03317>.
- [Sk21m] *A. Skopenkov*. Mathematics Through Problems: from olympiades and math circles to a profession. Part I. Algebra. 2021, AMS, Providence. Preliminary version: [https://www.mccme.ru/circles/oim/algebra\\_eng.pdf](https://www.mccme.ru/circles/oim/algebra_eng.pdf)
- [St94] *J. Stillwell*, Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.
- [Ti03] *V. M. Tikhomirov*, Abel and his great theorem (in Russian), Kvant. 2003. N 1. P. 11–15.

# Теория определимости: Логика. Алгебра. Геометрия

А. Л. Семенов, С. Ф. Сопрунов

Жюри проекта: А. Канель-Белов, И. Иванов-Погодаев, Р. Исаев,  
В. Кондратьев, А. Семёнов, С. Сопрунов, Б. Френкин.

## Введение

К центральным понятиям всей математики относятся истинность и доказуемость. Но наряду с теоремами и гипотезами в математике встречаются также определения одних понятий через другие. Например, через произведение чисел  $xy = z$ , можно определить делимость  $x|y$  и свойство «быть простым числом». Мы будем заниматься *теорией определимости*, в которой сегодня имеется большое количество нерешенных задач с ясными и простыми формулировками, пожалуй, больше, чем в теории доказательств и теории моделей. Такие нерешенные задачи мы будем обсуждать и пытаться решить во второй части проекта. В первой части будут как совсем простые задачи (упражнения), так и задачи посложнее, и совсем сложные, которые могут не получиться, но продвижение в них и обсуждение — полезны. Такие задачи отмечены звездочкой. Некоторые из задач — особенно во второй части — будут больше похожи не на олимпиадные, а на исследовательские, в них потребуется уточнить условие и самостоятельно спланировать свое исследование.

Мы будем изучать *определения свойств* и начнем с нематематического примера. Определение: «Деверь — это брат мужа». Более развернуто, без сокращений русского языка:

«человек  $A$  — деверь человека  $C$ » по определению означает, что существует такой человек  $B$ , что  $B$  — муж человека  $C$  и  $A$  — брат человека  $B$ .

Мы определили *двухместное свойство*  $D(A, C)$  «быть деверем» через свойство  $H(C, B)$  «быть мужем» и свойство  $F(A, B)$  «быть братом». Используя язык математики, можно записать:

$$D(A, C) \Leftrightarrow (\exists B)(H(C, B) \wedge F(A, B)).$$

Здесь  $\Leftrightarrow$  читается «есть по определению», слева от этого знака мы указываем имя свойства, которое определяем, справа — его определение через заданные свойства;  $(\exists B)$  читается «существует  $B$ , такое что»;  $\wedge$  читается «и».

Вот еще пример: «Точный квадрат — это произведение какого-то целого числа на себя»

Более развернуто: Целое число  $x$  — точный квадрат, если существует целое число  $y$  такое, что  $x = y \cdot y$ . Мы определили *одноместное свойство* «быть квадратом» через *трехместное*: « $x$  есть произведение  $y$  на  $z$ ».

На математическом языке: « $x$  — точный квадрат»  $\Leftrightarrow (\exists y)(x = y \cdot y)$

В данном проекте мы ограничиваем возможный вид определений. Все вышеприведенные определения подходят, а вот определение: «человек  $A$  — предок человека  $B$ , если есть последовательность людей, начинающаяся с  $A$  и заканчивающаяся  $B$ , где каждый следующий — родитель предыдущего» не подходит. В определениях не разрешается говорить о множествах или последовательностях, а только об элементах, как правило — о числах. Другими словами, нельзя говорить «для любого множества чисел», или «существует множество чисел», но можно говорить «для любого числа», «существует число», «число  $x$  равно числу  $y$ ». Дальше мы всегда будем считать, что *двухместное свойство равенства*  $x = y$  можно использовать в определениях всегда.

## А. Вводный цикл

**A1** Определить через *трехместное свойство* натуральных чисел «произведение»  $xy = z$ :

- двухместное свойство «делиться на»;
- одноместное свойство «быть единицей»;
- одноместное свойство «быть простым числом».

- A2** Определить через трехместные свойства «произведение» и «сумма» натуральных чисел:
- а) Одноместные свойства «быть 2», «быть 3»;
  - б) Одноместные свойства «быть степенью 2», «быть степенью 4»;
- A3** (\*) Определить через трехместные свойства «произведение» и «сумма» натуральных чисел одноместное свойство «быть степенью 6»;
- A4** Определить через трехместное свойство «сумма» натуральных чисел и одноместное свойство «быть квадратом натурального числа» трехместное свойство «произведение» натуральных чисел.
- A5** Определить через свойство «меньше» («порядок»,  $<$ ) для рациональных чисел:
- а) Свойство «больше или равно», свойство «больше»;
  - б) Трехместное свойство «лежать между».

## В. ЭКВИВАЛЕНТНОСТЬ СВОЙСТВ

Два свойства *эквивалентны*, если первое можно определить через второе, и наоборот – второе через первое.

- B1** Найдите наибольшее количество неэквивалентных среди свойств, определяемых через порядок для рациональных чисел. Попробуйте их искать среди одноместных, двухместных, трехместных и т.д. свойств.
- B2** (\*) Докажите, что для всякого  $n$  существует только конечное количество неэквивалентных  $n$ -местных свойств для порядка рациональных чисел.
- B3** Найдите наибольшее количество неэквивалентных среди свойств, определяемых через двухместное свойство «следование»  $y = x + 1$  для целых чисел.

## С. ПРЕОБРАЗОВАНИЯ И ИНВАРИАНТЫ

*Преобразование* – это взаимно однозначное отображение какого-то множества  $S$  на себя. Будем говорить, что преобразование *сохраняет* свойство, если выполненность свойства для произвольных элементов  $S$  равносильна его выполненности для их образов. Также говорят, что свойство — *инвариант* преобразования.

Совокупность всех преобразований, сохраняющих данное свойство, называется *группой преобразований* этого свойства. Аналогично для семейства свойств.

В следующих задачах мы рассматриваем только свойства, определяемые через порядок для рациональных чисел.

- C1** Постройте группу преобразований для каждого из найденных свойств, которые могут оказаться неэквивалентными.
- C2** Найдите для любых двух неэквивалентных свойств преобразование, которое одно из них сохраняет, а другое – нет.
- C3** (\*) Докажите, что существует только конечное количество не эквивалентных свойств. Постарайтесь найти их все.

В следующей задаче речь идет о следовании целых чисел

- C4** (\*) Попытайтесь создать план поиска не эквивалентных свойств и построения для них групп преобразований.

## D. НЕСТАНДАРТНЫЕ МОДЕЛИ

- D1** (\*) Пусть  $S$  — множество свойств, определяемых через «следование»  $y = x + 1$  для целых чисел. Может оказаться, что в  $S$  имеются два свойства, про которые мы хотим доказать, что они не эквивалентны, но построить преобразование "их различающее" не удастся. Попробуйте так расширить множество целых чисел (например, добавить еще одну "копию" целых и определить на объединении двух "копий" свойство следования), чтобы в этом расширении нашлось преобразование, различающее эти свойства.

## ТЕОРИЯ ОПРЕДЕЛИМОСТИ

### Дополнительные задачи

**В4.** Все свойства, определяемые через сумму и произведение, называются арифметическими. Как вы думаете, бывают ли не арифметические свойства натуральных чисел? Как можно было бы такое свойство построить?

**С5.** Правда ли, что если свойство  $R$  определимо через свойство  $Q$ , то множество преобразований  $\Gamma_Q$ , сохраняющих свойство  $Q$  является подмножеством множества преобразований (сохраняющих)  $\Gamma_R$ ?

**В5.** Рассмотрим множество точек на плоскости. Определимо ли свойство  $C(x, y, z)$  -- точки  $x, y, z$  лежат на одной прямой, через свойство  $D(x, y, z, v) \Leftrightarrow d(x, y) = d(z, v)$ ?

**С6.** На целых числах:  $\mathbb{Z}$ , задано свойство  $R(x, y, z) \Leftrightarrow z = x + y$ ; Опишите группу преобразований этого свойства. Определимы ли через  $R$  одноместные свойства  $x = 0$ ;  $x = 1$ , двухместное свойство  $x < y$ ?

**D2.** Напишите формулу, означающую, что отношение  $<$  не имеет наименьшего и наибольшего элемента и формулу, означающую, что между любыми двумя различными элементами найдется отличный от них третий. Выполнены ли эти утверждения для рациональных, целых, действительных чисел?

Попробуйте доказать, что существует взаимно однозначное, сохраняющее порядок соответствие между любым таким счетным множеством и рациональными числами.

### Новая структура: Сложение рациональных

**В6.** Даны рациональные числа  $\mathbb{Q}$  со свойством суммы

$$S(x, y, z) \Leftrightarrow (z = x + y).$$

Следующие задачи относятся к указанному множеству и свойству.

(а) Опишите группу преобразований данного свойства.

(б) Определимо ли через  $S$  двухместное свойство

$$M(x, y) \Leftrightarrow (y = 3 * x)?$$

Верно ли обратное? Опишите группу преобразований свойства  $M$ .

(в) Попытайтесь найти максимальную систему попарно не эквивалентных семейств свойств.

### Цикл Е: Проблемы для исследования

Цикл Е содержит основные исследовательские задачи проекта, они представлены в таблице ниже. Большинство из них представляет собой открытые (пока никем не решенные) проблемы. Те из них, которые не удастся до конца решить в ближайшие дни, мы продолжим вместе решить в последующие месяцы и результаты опубликуем.

Отношения/множества	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$(x < y)$	E1	E2	E3
$(y = x + 1)$	E4	E5	E6
$(z = x + y)$	E7	E8	E9

Помимо числовых структур из таблицы мы предлагаем исследовать еще одну.

**E10.** Бесконечный неориентированный граф без циклов (дерево), где каждая вершина имеет степень три; свойство "быть соседними вершинами". "Ветвящиеся целые".

Кого-то может заинтересовать и такая структура:

**E11.** Порядок неотрицательных рациональных чисел.

Мы выделяем в исследовании проблемы определимости для каждой структуры (множества с исходным семейством свойств на нем) следующие основные ступени (которые могут перемешиваться в наших исследованиях):

I. Поиск свойств (семейств свойств, часто семейств из одного элемента), определимых через заданное исходное семейство. Выдвижение гипотезы, что мы нашли максимальную систему свойств, и что найденные свойства (семейства) не эквивалентны.

II. Построение для каждого свойства его группы преобразований. Возможно, для этого нам придется построить расширение исходного множества и определить свойства на расширении. Доказательство с помощью групп того, что найденные свойства не эквиваленты.

III. Доказательство того, что мы нашли максимальное семейство не эквивалентных свойств.

IV. Для всех найденных свойств (семейств свойств) найти их твг и тнг. Определение

**Точной верхней гранью (твг,  $\sup$ )** семейств свойств  $A$  и  $B$  называется семейство свойств, определимых через свойства из объединения семейств  $A$  и  $B$ .

**Точной нижней гранью (тнг,  $\inf$ )** семейств свойств  $A$  и  $B$  называется семейство свойств, определимых и через свойства из семейства  $A$  и через свойства из семейства  $B$ .



# Теория определимости: Логика. Геометрия. Алгебра

Алексей Львович Семенов, Сергей Федорович Сопрунов  
Илья Иванов-Погодаев, Роман Исаев, Владимир Кондратьев,  
Борис Рафаилович Френкин

Летняя конференция Турнира Городов  
2 августа 2021

# Пример задачи по теории определимости

Задача: определить одноместное свойство «быть степенью 6» через отношения сложения и умножения на множестве натуральных чисел. Эта проблема может быть решена (и была решена участниками проекта) с помощью «техники арифметизации», аналогичной доказательству Гёделя его теоремы о неполноте. Участник проекта Валерий Кожуркин предложил другое короткое решение:

Пусть  $6^k = 2^a 3^b$ . Найдём  $2^a$  and  $3^b$  как максимальные степени 2 и 3 которые делят  $6^k$ .

Пусть  $p$  – простое число, такое что  $p > 6^k$ .

Минимальные решения сравнений

$$p^m + 2^a \equiv 0 \pmod{p+2}$$

$$\text{and } p^n + 3^b \equiv 0 \pmod{p+3}$$

для нечётных  $k$  это  $m = a$  и  $n = b$ .

Если  $a$  и  $b$  чётные, мы можем умножить на 6 чтобы работать с нечётными показателями.

В нашем проекте под проблемой определимости мы понимаем описание решетки определимости данной структуры. Решение проблемы можно разделить на 4 этапа.

- 1 Найти как можно больше неэквивалентных отношений. В какой-то момент возникает предположение, что ничего нового получить нельзя.
- 2 Для каждого отношения описать группу преобразований, которые его сохраняют. Рассмотрение этих групп позволяет нам объяснить, почему одни отношения не могут быть определены через другие.
- 3 Доказать, что других неэквивалентных отношений нет. Это самая сложная часть проекта. До сих пор у нас нет общего способа сделать это, поэтому мы должны изобретать что-то конкретное для каждого случая. В большинстве случаев полезно групповое обсуждение.
- 4 Для каждой пары отношений указать их супремум (сокр.  $\sup$ ) наименьшая верхняя граница и  $\inf$ imum (сокр.  $\inf$ ) их наибольшая нижняя граница. Это решеточные операции над замыканиями отношений.

# Рациональные числа с порядком (1 этап)

- ①  $(x < y)$
- ②  $B(x, y, z) \Leftrightarrow (x < y < z) \vee (z < y < x)$
- ③  $C(x, y, z) \Leftrightarrow (x < y < z) \vee (y < z < x) \vee (z < x < y)$
- ④  $S(x, y, z, u)$ : интервалы  $(x, y)$  и  $(z, u)$  пересекаются, но не содержатся друг в друге (зацепляются).
- ⑤  $(x = y)$

## Рациональные числа с порядком (2 этап)

Определим группы преобразований в каждом случае

- 1  $\Gamma$  состоит из монотонно возрастающих непрерывных преобразований. Все группы ниже содержат подобные преобразования, так что мы не будем упоминать их далее.
- 2  $\Gamma_B$  содержит монотонно убывающих непрерывных преобразований.
- 3  $\Gamma_C$  содержит **транспозиции**. Это такие преобразования с двумя иррациональными параметрами  $s, t$ , которые отображают интервалы  $(-\infty, s)$  и  $(s, +\infty)$  в  $(t, +\infty)$  и  $(-\infty, t)$  соответственно, при этом сохраняя отношение порядка на каждом из них.
- 4  $\Gamma_S$  содержит все преобразования из  $\Gamma_B$  и  $\Gamma_C$  и их композиции.
- 5  $Sym(\mathbb{Q})$  – группа всех преобразований рациональных чисел. Они сохраняют отношение равенства.

## Рациональные числа с порядком (3 этап)

Опишем идею доказательства отсутствия других неэквивалентных соотношений. Для этого нам потребуется теоретико-групповое понятие  $k$ -транзитивности.

Группа  $G$  называется  $k$ -транзитивной, если для любых двух  $k$ -наборов  $(a_1, \dots, a_k); (b_1, \dots, b_k); a_i \neq a_j; b_i \neq b_j$  существует преобразование  $g \in G$  такое, что  $\forall (i \leq k) (g(a_i) = b_i)$ .

Например, группа  $\Gamma$  1-транзитивна, но не 2-транзитивна. А  $\Gamma_B$  2-транзитивна, но не 3-транзитивна.

Опишем все группы, включающие  $\Gamma$ . Для этого мы будем рассматривать все  $k$ -транзитивные, но не  $(k+1)$ -транзитивные группы для каждого натурального  $k$ . Оказывается, мы не получим никаких групп, кроме пяти групп, описанных выше. Это решающий шаг в доказательстве отсутствия других отношений. Доказательство сложное, но прямолинейное. Некоторым участникам проекта удалось его придумать.

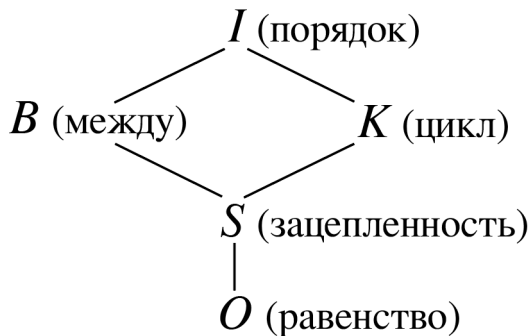
## Рациональные числа с порядком (4 этап)

Представим полученные ранее результаты в виде ориентированного графа. Его вершинами будут символы отношений, а направление рёбер будет указывать на определимость одних отношений через другие. Также вспомним два определения, о которых говорили ранее.

**Точной верхней гранью (твг,  $\sup$ )** семейств свойств  $A$  и  $B$  называется семейство свойств, определимых через свойства из объединения семейств  $A$  и  $B$ .

**Точной нижней гранью (тнг,  $\inf$ )** семейств свойств  $A$  и  $B$  называется семейство свойств, определимых и через свойства из семейства  $A$ , и через свойства из семейства  $B$ .

Точные верхнюю и нижнюю грани двух семейств можно определить благодаря построенному графу.



Помимо графа отношений мы можем представить наши результаты в виде графа групп, где вместо отношений мы пишем их группы преобразований. Направление рёбер означать отношение включения между группами.



# Целые со следованием (1 этап)

①  $A_n(x, y) \Leftrightarrow y = x + n$

②  $B_n(x, y, z, u) \Leftrightarrow (|x - y| = n) \wedge (x - y = z - u)$

③  $C_n(x, y) \Leftrightarrow |x - y| = n$

## Целые со следованием (2 этап)

Определим основные типы преобразований. Для начала, разобьём целые числа на  $n$  классов в зависимости от их остатков при делении на  $n$ :  $r + n\mathbb{Z}$ ,  $0 \leq r < n$ . Множество, состоящее из таких классов будет обозначать за  $\mathbb{Z}/n\mathbb{Z}$ .

- **Сдвиг** класса  $r + n\mathbb{Z}$  на величину  $k$  – это преобразование  $\sigma$  вида  $\sigma(r + n \cdot S) = r + n \cdot (S + k)$ .
- **Перестановка**  $\sigma \in S_n$  классов – это преобразование  $\sigma$ , действующее следующим образом  $\sigma(r + n \cdot S) = \sigma(r) + n \cdot S$ .
- **Разворот** класса  $r + n\mathbb{Z}$  – преобразование вида  $\sigma(r + n \cdot S) = r + n \cdot (-S)$ .

Тогда

- 1  $\Gamma_{A_n}$  состоит из сдвигов и перестановок классов из  $\mathbb{Z}/n\mathbb{Z}$ .
- 2  $\Gamma_{B_n}$  состоит из сдвигов, перестановок и разворотов классов из  $\mathbb{Z}/n\mathbb{Z}$ .
- 3  $\Gamma_{C_n}$  состоит из сдвигов, перестановок классов и одновременного разворотов всех классов из  $\mathbb{Z}/n\mathbb{Z}$ .

# Открытые проблемы

Отношения/множества	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$(x < y)$	решена	не решена	не решена
$(y = x + 1)$	были попытки	решена	были попытки
$(z = x + y)$	В процессе	тяжёлая	тяжёлая

И ещё две проблемы, которые также в процессе решения:

1. Бесконечный неориентированный граф без циклов (бесконечное дерево), где каждая вершина имеет степень три; свойство "быть соседними вершинами". ("Ветвящиеся целые".)
2. Порядок на неотрицательных рациональных числах.

# Theory of definability: Logic. Algebra. Geometry

A. L. Semyonov, S. F. Soprunov

The jury of the project: A.Kanel-Belov, I.Ivanov-Pogodayev, R.Isayev,  
V.Kondratyev, A.Semyonov, S.Soprunov, B.Frenkin.

## Introduction

Truth and provability belong to central concepts of mathematics. But mathematics includes not only theorems and conjectures but also definitions. For instance, using the ternary relation of product  $xy = z$  we can define the binary relation of divisibility  $x|y$  and the unary relation «to be a prime»  $Prime(x)$ . We will deal with the *definability theory* which now has perhaps more unsolved problems with simple and clear formulation than the proof theory and the model theory. We will consider and try to solve these open problems in the second part of the project. The first part contains some quite simple problems (exercises) as well as more difficult problem such that you may fail in solving them but any advancement and discussion would be useful. These problems are starred. Some problems, especially in the second part, are more similar not to olympiad but to research problems: you have to specify the condition and construct your own plan of research.

We will study *definitions of relations* starting with some non-mathematical example.

Here is the first example: «A brother in law is a brother of the husband.» [In English a brother in law may also mean a brother of the wife but we don't consider this case here.] In more detail, without any abbreviations:

By definition, «a person  $A$  is a brother in law of a person  $C$ » means that there exists a person  $B$  such that  $B$  is the husband of the person  $C$  and  $A$  is a brother of the person  $B$ .

We have defined the binary relation  $D(A, C)$  «to be a brother in law» via the relation  $H(C, B)$  «to be the husband» and the relation  $F(A, B)$  «to be a brother». Using the language of mathematics we write:

$$D(A, C) \Leftarrow (\exists B)(H(C, B) \wedge F(A, B)).$$

Here  $\Leftarrow$  is read "is by definition"; to the left from this sign we indicate the name of the relation that is defined, and to the right we indicate its definition via given relations;  $(\exists B)$  is read «there exists  $B$  such that»;  $\wedge$  is read «and».

A further example: «A perfect square is the product of some integer by itself.»

In more detail: «An integer  $x$  is a perfect square if there exists an integer  $y$  such that  $x = y \cdot y$ .» We have defined the unary relation «to be a perfect square» via the ternary relation « $x$  is the product of  $y$  by  $z$ ».

In the mathematical language: « $x$  is a perfect square»  $\Leftarrow (\exists y)(x = y \cdot y)$ .

In this project we restrict the possible form of definitions. All the above definitions do fit but this is not the case with the definitions of the form «a person  $A$  is an ancestor of a person  $B$  if there exists a sequence of persons which starts by  $A$  and finishes by  $B$  and such that each subsequent person is a parent of the preceding one». In the definitions, it is allowed to mention not sets or sequences but only elements, usually numbers. In other words, in a definition it is forbidden to say «for any set of numbers» or «there exists a set of numbers» but it is allowed to say «for any number», «there exists a number», «the number  $x$  equals the number  $y$ ». In the sequel, we assume that the binary relation of equality « $x=y$ » is always admissible.

## A. INTRODUCTORY CYCLE

**A1** Define the following relations via the ternary relation of positive integers «product»  $xy = z$ :

- a) the binary relation «to be divisible by»;
- b) the unary relation «to be the unit»;
- c) the unary relation «to be a prime».

**A2** Define the following relations via the ternary relations «product» and «sum» of positive integers:

- a) the unary relations «to be 2», «to be 3»;
- b) the unary relations «to be a power of 2», «to be a power of 4».

**A3** (\*) Define the unary relation «to be a power of 6» via the ternary relations «product» and «sum» of positive integers.

- A4** Define the ternary relation «product» of positive integers via the ternary relation «sum» of positive integers and the unary relation «to be the square of a positive integer».
- A5** Define the following relations via the relation «less» («order»,  $<$ ) of rationals:
- a) the binary relations «greater or equal», «greater»;
  - b) the ternary relation «to lie between».

## B. EQUIVALENCE OF RELATIONS

Two relations are *equivalent* if the first of them is definable through the second one, and conversely, the second of them is definable through the first one.

- B1** For the relations definable via the order of rationals, try to find the maximum possible set of non-equivalent relations; for this, consider unary, binary, ternary etc. relations.
- B2** (\*) Prove that for each  $n$  there exists only a finite number of non-equivalent  $n$ -ary relations for the order of rationals.
- B3** Among the relations definable via the binary relation «consecution»  $y = x + 1$  for integers, find the maximum possible set of non-equivalent ones.

## C. TRANSFORMATIONS AND INVARIANTS

A *transformation* is a one-to-one mapping of a set. We say that a transformation *preserves a relation* if fulfilment of the relation for arbitrary elements of the domain is equivalent to its fulfilment for their images. In other words, the relation is *an invariant of the transformation*.

The collection of all transformations preserving a given relation is called *the transformation group of this relation*. Similarly for a family of relations.

In the problems below we consider only relations definable via the order of rationals.

- C1** Construct the transformation group for each of the relations found above which may occur non-equivalent.
- C2** For any two non-equivalent relations find a transformation which preserves one of these and doesn't preserve the other one.
- C3** (\*) Prove that there exists only a finite number of non-equivalent relations. Try to find all of these.
- C4** (\*) Try to construct a plan for search for non-equivalent relations and for constructing their transformation groups.

## D. NON-STANDARD MODELS

- D1** Let  $S$  is the set of relations definable via «consecution»  $y = x + 1$  for integers. Suppose  $S$  contains two relations for which we want to prove non-equivalence but we fail to construct a transformation which «distinguishes» them. Try to extend the set of integers (for instance, add one more «copy» of integers and define the relation of consecution on the joint of two «copies») in such a way that the extension possesses a transformation which distinguishes these relations.

## DEFINABILITY THEORY

### FURTHER PROBLEMS

**B4.** All relations definable via sum and product are called arithmetical. In your opinion, do there exist non-arithmetical relations of positive integers? What is a possible way to construct such relations?

**C5.** Is it true that if a relation  $R$  is definable via a relation  $Q$  then the set  $\Gamma_Q$  of transformations preserving  $Q$  is a subset of the set  $\Gamma_R$  of transformations preserving  $R$ ?

**B5.** Consider the set of points of the plane. Is it possible to define the relation  $C(x, y, z)$ : "points  $x, y, z$  are collinear" via the relation  $D(x, y, z, v) \Leftrightarrow d(x, y) = d(z, v)$ ?

**C6.** The relation  $R(x, y, z) \Leftrightarrow z = x + y$  is defined on the set of integers  $\mathbb{Z}$ . Describe the transformation group of this relation. Are the following relations definable via  $R$ : the unary relations  $x = 0$ ;  $x = 1$ ; the binary relation  $x < y$ ?

**D2.** Present the formula which means that the relation  $<$  has no least and greatest elements, and the formula which means that among any two distinct elements there exists an element distinct from these. Are these statements fulfilled for rationals, integers, reals?

Try to prove that there exists an order-preserving bijection between rationals and any countable set with the above properties.

### A NEW STRUCTURE: ADDITION OF RATIONALS

**B6.** Given the set of rationals  $\mathbb{Q}$  with the relation of sum

$$S(x, y, z) \Leftrightarrow (z = x + y).$$

In the following problems, we consider this set and this relation.

- (a) Describe the transformation group of the above relation.
- (b) Is it possible to define via  $S$  the binary relation

$$M(x, y) \Leftrightarrow (y = 3 * x)?$$

Is the converse true? Describe the transformation group for  $M$ .

- (c) Try to determine the maximal system of pairwise non-equivalent families of relations.

### CYCLE E: PROBLEMS FOR RESEARCH

The cycle E contains the main research problems of the project, they are presented in the table below. Most of them are open (up to now, unsolved) problems. If some of these won't be solved in a few days then we will proceed to collaborate on these problems and will publicate the results.

Relations/sets	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$(x < y)$	E1	E2	E3
$(y = x + 1)$	E4	E5	E6
$(z = x + y)$	E7	E8	E9

Besides the number structures from the table, we suggest to investigate one more.

**E10.** "Branching integers:" an infinite non-oriented graph without cycles (an infinite tree) such that every vertex is of degree 3; the relation "to be neighboring vertices".

Perhaps some of you would be interested in the following structure:

**E11.** The order on non-negative rationals.

Investigating the issue of definability for every structure (a set with a family of basic relations on it) we distinguish the following stages of research (which in fact may overlap):

I. The search for relations (families of relations but often consisting of a single element) which are definable via a given basic relation. Proposal of the conjecture that the family of relations is the maximal one, and that these (families of) relations are non-equivalent.

II. For each relation, construction of its transformation group. Perhaps we would have to extend the basic set and to define the relations on the extension. Proof of non-equivalence of the relations found.

III. Proof that the the found family of non-equivalent relations is maximal.

IV. For all (families of) relations found, determine their least upper bound and greatest lower bound.  
Definitions:

**The least upper bound (the supremum, sup)** of families of relations  $A$  and  $B$  is the family of relations definable via the relations from the union of families  $A$  and  $B$ .

**The greatest lower bound (the infimum, inf)** of families of relations  $A$  and  $B$  is the family of relations that are definable both via the relations from  $A$  and via the relations from  $B$ .

# Definability theory: Logic. Geometry. Algebra

Alexey Semyonov, Sergey Soprunov, Alexey Kanel-Belov,  
Ilya Ivanov-Pogodayev, Roman Isayev, Vladimir Kondratyev,  
Boris Rafailovich Frenkin

Summer Conference of the Tournament of Towns  
August 10, 2021



# An example of definability problem

Problem: to define the unary relation "to be a power of 6" via addition and multiplication relations on the set of natural numbers.

This problem can be solved (and was solved by members of the Project) by 'Arithmetization technique' similar to the Goedel proof of his Incompleteness Theorem. A participant of the project Valery Kozhurkin proposed a different and short solution:

Let  $6^k = 2^a 3^b$ . It is easy to find  $2^a$  and  $3^b$  as the maximal exponents of 2 and 3 that divide  $6^k$ .

Let  $p$  be a prime number such that  $p > 6^k$ .

The minimal solutions for the congruences

$$p^m + 2^a \equiv 0 \pmod{p+2}$$

$$\text{and } p^n + 3^b \equiv 0 \pmod{p+3}$$

for odd  $k$  are  $m = a$  and  $n = b$ .

If  $a$  and  $b$  are even, we can multiply by 6 in order to work with odd exponents.

In our project by definability problem we mean describing the definability lattice of a given structure. A solution for the problem can be divided in 4 stages.

- 1 Find as many non-equivalent relations as possible. At some moment you see that nothing new can be obtained. Then you pass to the next stage.
- 2 For each relation, describe the group of transformations which preserve it. Consideration of these groups enables us to explain why some relations are not definable via others.
- 3 Prove that there are no other non-equivalent relations. This is the most difficult part of the project for the given structure. Up to now, we have no general way to do it, so we have to invent something specific for each case. In most cases group considerations are helpful.
- 4 For each pair of relations, indicate their supremum (abbr. sup) least upper bound and infimum (abbr. inf) their greatest lower bound. These are the lattice operations on the closures of relations. .

# Rationals with the order (I stage)

- ①  $(x < y)$
- ②  $B(x, y, z) \Leftrightarrow (x < y < z) \vee (z < y < x)$
- ③  $C(x, y, z) \Leftrightarrow (x < y < z) \vee (y < z < x) \vee (z < x < y)$
- ④  $S(x, y, z, u)$ : open intervals  $(x, y)$  and  $(z, u)$  intersect and do not contain in each other (they are 'linked').
- ⑤  $(x = y)$

# Rationals with the order (II stage)

Let us indicate the transformation groups for each case.

- 1  $\Gamma$  consists of all increasing continuous transformations. All the groups below contain these transformations, so these will not be mentioned explicitly.
- 2  $\Gamma_B$  consists of all continuous decreasing transformations.
- 3  $\Gamma_C$  contains **transpositions**. Here we use the term «transposition» for a transformation with irrational parameters  $s, t$  which maps the intervals  $(-\infty, s)$  and  $(s, +\infty)$  onto  $(t, +\infty)$  and  $(-\infty, t)$  respectively and preserves the order of rationals in both cases.
- 4  $\Gamma_S$  contains all transformations from the groups  $\Gamma_B$  and  $\Gamma_C$ .
- 5  $Sym(\mathbb{Q})$  is the group of all transformations of rationals. They preserve the identity relation.

## Rationals with the order (III stage)

Let us describe the idea of the proof that there are no other non-equivalent relations. For this we require the group-theoretic notion of  **$k$ -transitivity**.

A group  $G$  is called  $k$ -transitive if for every two  $k$ -tuples  $(a_1, \dots, a_k); (b_1, \dots, b_k); a_i \neq a_j; b_i \neq b_j$  there exists a transformation  $g \in G$  such that  $\forall (i \leq k) (g(a_i) = b_i)$ .

For instance, the group  $\Gamma$  is 1-transitive but not 2-transitive. And  $\Gamma_B$  is 2-transitive but not 3-transitive.

We will describe all groups including  $\Gamma$  (its supergroups). For this, we will consider all  $k$ -transitive but not  $(k+1)$ -transitive groups for every natural  $k$ . It occurs that we will obtain no groups besides the five groups described above. This is the crucial step in the proof for absence of other relations. The proof is difficult but straightforward. Some members of the project succeeded in it

## Rationals with the order (IV stage)

Let us represent the above results in the form of an oriented graph. Its vertices are the symbols of relations, and the directed edges indicate definability of some relations via others. Let us recall two notions.

**Supremum** of the families of relations  $A$  and  $B$  is the family of relations definable via the relations from the union of  $A$  and  $B$ .

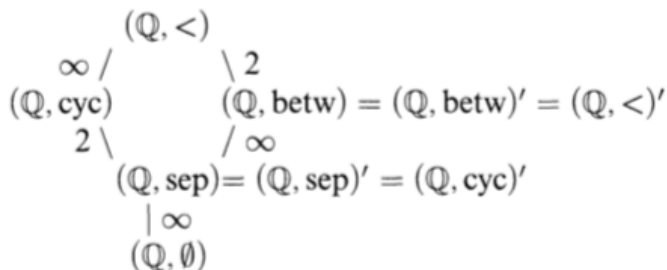
**Infimum** of the families of relations  $A$  and  $B$  is the family of relations definable both via the relations from  $A$  and via the relations from  $B$ .

On this graph the infimum for families  $A$  and  $B$ , for instance, is the family of all relations such that from each of them there exists directed paths to  $A$  and  $B$ .

We can represent the results not only as the graph of relations but also as the graph of transformation groups. Its vertices are the transformation groups of relations, and the direction of edges corresponds to the inclusion relation between the groups.

# Graph of relations

The lattice for  $(\mathbb{Q}, <)$  looks as follows:



# Integers with successor (I stage)

- ①  $A_n(x, y) \Leftrightarrow y = x + n$
- ②  $B_n(x, y, z, u) \Leftrightarrow (|x - y| = n) \wedge (x - y = z - u)$
- ③  $C_n(x, y) \Leftrightarrow |x - y| = n$



# Integers with successor (II stage)

Let us define the basic sorts of transformations. To begin with, divide the integers into  $n$  classes respective to their remainders modulo  $n$ :

$r + n\mathbb{Z}$ ,  $0 \leq r < n$ . The set consisting of  $n$  these classes will be denoted  $\mathbb{Z}/n\mathbb{Z}$ .

- **A shift** of a class  $r + n\mathbb{Z}$  by a value  $k$  is a transformation  $\sigma$  of the form  $\sigma(r + n \cdot S) = r + n \cdot (S + k)$ .
- **A permutation**  $\sigma \in S_n$  of classes is a transformation  $\sigma$  of the form  $\sigma(r + n \cdot S) = \sigma(r) + n \cdot S$ .
- **U-turn** of a class  $r + n\mathbb{Z}$  is a transformation  $\sigma$  of the form  $\sigma(r + n \cdot S) = r + n \cdot (-S)$ .

Then

- 1  $\Gamma_{A_n}$  consists of the shifts and the permutations of the classes  $\mathbb{Z}/n\mathbb{Z}$ .
- 2  $\Gamma_{B_n}$  consists of the shifts, the permutations and the U-turns of the classes  $\mathbb{Z}/n\mathbb{Z}$ .
- 3  $\Gamma_{C_n}$  consists of the shifts, the permutations and the simultaneous U-turn of all the classes  $\mathbb{Z}/n\mathbb{Z}$ .

# Unsolved at ToT and Open Problems

Here are some natural problems for usual number sets.

Relations/sets	$\mathbb{Q}$	$\mathbb{Z}$	$\mathbb{N}$
$(x < y)$	solved	unsolved	unsolved
$(y = x + 1)$	try	solved	try
$(z = x + y)$	in process	hard	hard

Two more (from many):

1. "Branching integers:" an infinite non-oriented graph without cycles (an infinite tree) such that every vertex is of degree 3; the relation "to be neighboring vertices".
2. The order on non-negative rationals.