УНИВЕРЗИТЕТ "Св. КИРИЛ И МЕТОДИЈ" – СКОПЈЕ
ПРИРОДНО - МАТЕМАТИЧКИ ФАКУЛТЕТ

А. Самарџиски Н. Целакоски

РЕШЕНИ ЗАДАЧИ ПО АЛГЕБРА II

Скопје, 2006

Издавачки совет на ПМФ: Л. Андреева, В. Урумов, Н. Ивановски, М. Караделев, Д. Василески, В. Бакева и Љ. Ристески

Рецензенти:

Проф. д-р Дончо Димовски, ред. проф. на ПМФ, Скопје
Проф. д-р Костадин Тренчевски, ред. проф. на ПМФ, Скопје
Проф. д-р Билјана Јанева, ред. проф. на ПМФ, Скопје

Лектор:

Н. Целакоски

Со одлука на Наставно-научниот совет на Природно-математичкиот факултет во Скопје, со одлука бр. 2165 од 09.03.2006 година, го одобри печатењето на овој ракопис како Универзитетски учебник.

CIP – Каталогизација во публикација
Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

512(075.8)(076)

САМАРЏИСКИ, Александар
Решени задачи по алгебра II : [универзитетски учебник] / А. [Александар] Самарџиски, Н. [Наум] Целакоски. – Скопје : Природно-математички факултет, 2006. – V, 234 стр. : 24 см

ISBN 9989-668-53-1
1. Целакоски, Наум
а) Алгебра – Високошколски учебници – Вежби
COBISS.MK-ID 64607242

ПРЕДГОВОР

Оваа збирка преставува продолжение на збирката "Решени задачи по алгебра I ", којашто излезе од печат 1968 година во издание на Универзитетот во Скопје. Збиркава е работена според наставната програма за предметот Алгебра II што се предава на Природно-математичкиот факултет во Скопје, а опфаќа околу две третинки од таа програма.

Материјалот во збиркава се изнесува според предавањата на проф. д-р Ѓорѓи Чупона (умножени во учебната 1969/70 година), т.е. потребните дефиниции и особини се користени од тие предавања, од каде што е земен и еден дел од задачите. Материјалот е поделен на 16 параграфи, слично како во споменатите предавања, а нумерацијата на задачите е спроведена за секој параграф посебно, што го прави поудобно користењето на збиркава.

Задачите се решени, освен некои што се решаваат на сличен начин како некоја претходно решена задача, или пак се непосредни последици од некои особини и задачи. Извесен број задачи се означени со ѕвездичка, што означува дека решението не е едноставно и дека авторите не успеале да најдат згодно решение.

При решавањето на некои задачи, користени се задачи од првата збирка. При повикувањето, на пример, на задачата 29. од првата збирка, пишуваме I .29, а на задачата 29 од § 3 од оваа збирка, пишуваме 3.29.

Се надеваме дека збиркава корисно ќе им послужи на студентите за успешно совладување на материјалот по предметот алгебра.

Авторите ќе им бидат благодарни на сите што ќе достават забелешки (од секаков вид) во врска со задачите.

Авторите

Ноември 1971
СКОПЈЕ

КОН ПРВОТО ИЗДАНИЕ

Подготвениот ракопис за збирката *"Решени задачи по алгебра II"* беше умножен на гештетнер во 1971 година како учебно помагало за "внатрешна употреба" по предметот алгебра II за студентите од математичката група на ПМФ-Скопје. До редовно издание на ракописот не дојде досега, иако многу години успешно се користеше од редица генерации студенти.

Сепак, по иницијатива и сесрдно залагање на проф. д-р Дончо Димовски, шеф на Институтот за математика во периодот 2001–2003 година, а со широко разбирање и поткрепа од проф. д-р Новак Ивановски, главен и одговорен уредник на Издавачкиот совет на ПМФ-Скопје, сега збиркава го доживува своето прво издание. Им благодарам на обајцата, а и на другите личности што придонесоа да се реализира овој потфат.

Ова издание на збиркава "Решени задачи по алгебра II", кое што верно го следи истоимениот ракопис од 1971 година (т.е. тој ракопис овде е отпечатен без измени), се посветува на првиот од авторите, А. Самарџиски, којшто почина во 2001 година.

На крајот од збиркава е даден список на "почесто употребувани ознаки", како и "показател на поими" за поимите што се дефинирани во неа, низ задачите. За другите поими што се користат, а не се дефинирани во збиркава, како и за својствата што се неопходни за решавање на задачите, читателот се упатува на учебникот *"Предавања по алгебра* II " од аворите Г. Чупона и Б. Трпеновски, Скопје, 2000 година (II издание).

Ноември 2005 г.
Скопје

Н. Целакоски

СОДРЖИНА

§ 1. МНОЖЕСТВА

1.1. Да се најде:

а) $\bigcup_{i=1}^{\infty} A_i$; $\bigcap_{i=1}^{\infty} A_i$, $A_i = \{1,2,\ldots, i\}$, $i \in \mathbb{N}$;

б) $\bigcup_{i=0}^{\infty} A_i$; $\bigcap_{i=0}^{\infty} A_i$, $A_0 = \{0\}$, $A_i = \{x \mid x \in \mathbb{R}, 0 \le x < i\}$, $i \in \mathbb{N}$.

Решение. а) Бидејќи $A_1 \subset A_2 \subset \ldots \subset A_i \subset \ldots$, имаме:

$$\bigcup_{i=1}^{\infty} A_i = \mathbb{N}, \quad \bigcap_{i=1}^{\infty} A_i = \{1\}.$$

б) Имаме:

$A_0 = \{0\}, A_1 = [0, 1), \ldots, A_i = [0, i), \ldots$

т.е. $A_0 \subset A_1 \subset A_2 \subset \ldots$, па

$$\bigcup_{i=0}^{\infty} A_i = \mathbb{R}^+ \cup \{0\}, \quad \bigcap_{i=0}^{\infty} A_i = \{0\}.$$

(Со $\mathbb{R}^+$ е означено множеството од позитивни реални броеви).

1.2. Нека е A_n множеството од сите природни броеви што се деливи со природниот број n. Да се најде:

а) $\bigcup_{n \in \mathbb{N}} A_n$;

б) $\bigcap_{n \in \mathbb{N}} A_n$;

в) $A_m \cap A_n$;

г) $\bigcup_{p} A_p$ p – прост број.

Одговор. а) $\mathbb{N}$.

б) $\varnothing$.

в) $A_{[m, n]}$, каде што $[m, n]$ е *најмалиот заеднички содржател* на m и n.

г) $\mathbb{N} \setminus \{1\}$.

1.3. Нека A е множество и нека: $(\forall x \in A)$ $A_x = A \setminus \{x\}$. Да се најде:

а) $\bigcap_{x \in A} A_x$;

б) $\bigcup_{x \in A} A_x$.

Одговор. а) $\varnothing$. б) A.

1.4. Да се докажат следните дистрибутивни закони:

а) $A \cap (\bigcup_i B_i) = \bigcup_i (A \cap B_i)$;

б) $A \cup (\bigcap_i B_i) = \bigcap_i (A \cup B_i)$, каде што $i \in I$, $I \neq \emptyset$.

Решение. а) $x \in A \cap (\bigcup_i B_i) \Leftrightarrow x \in A$ и $(\exists_j \in I)\, x \in B_j \Leftrightarrow x \in \bigcup_i (A \cap B_i)$;

б) Слично како под а).

1.5. Да се покаже дека:

а) $(\bigcup_i A_i) \cap (\bigcup_j B_j) = \bigcup_{i,j} (A_i \cap B_j)$;

б) $(\bigcap_i A_i) \cup (\bigcap_j B_j) = \bigcap_{i,j} (A_i \cup B_j)$,

каде што $\bigcup_{i,j}$ означува $\bigcup_{(i,j) \in I \times J}$.

1.6. Да се покаже дека:

$(A \cap B) \cup (C \cap D) \subseteq (A \cup C) \cap (B \cup D)$.

Решение. $(A \cap B) \cup (C \cap D) = [(A \cap B) \cup C] \cap [(A \cap B) \cup D] =$

$= [(A \cup C) \cap (B \cup C)] \cap [(A \cup D) \cap (B \cup D)] =$

$= (A \cup C) \cap (B \cup D) \cap (B \cup C) \cap (A \cup D) \subseteq$

$\subseteq (A \cup C) \cap (B \cup D)$.

Дека во општ случај не важи равенство се покажува ако се земе:

$A = \{a\} = D$, $B = \{b\}$, $C = \{a, b\}$.

1.7. Ако $\{A_{ik} \mid (i,k) \in I \times K\}$ е фамилија множества, тогаш

$\bigcup_{k \in K} (\bigcap_{i \in I} A_{ik}) \subseteq \bigcap_{i \in I} (\bigcup_{k \in K} A_{ik})$.

Решение. Нека $x \in \bigcup_{k \in K} (\bigcap_{i \in I} A_{ik})$.

Тогаш, постои $k_0 \in K$, таков што $x \in \bigcap_{i \in I} A_{ik_0}$, т.е. $x \in A_{ik_0}$ за секој $i \in I$, а од ова: $x \in \bigcup_{k \in K} A_{ik}$ за секој $i \in I$. На крајот, $x \in \bigcap_{i \in I} (\bigcup_{k \in K} A_{ik})$.

т.е.

$$\bigcup_{k \in K} (\bigcap_{i \in I} A_{ik}) \subseteq \bigcap_{i \in I} (\bigcup_{k \in K} A_{ik})$$

Дека не мора да важи равенство, види го примерот во 1.6.

1.8.* Нека $\{A_i \mid i = 1,\ldots, n\}$ е конечна фамилија множества. За кое било подмножество K од множеството $\{1, 2,\ldots, n\}$ да ставиме:

$$P_K = \bigcup_{i \in K} A_i, \quad Q_K = \bigcap_{i \in K} A_i .$$

Ако F_m е множеството на сите подмножества од $\{1, 2,\ldots, n\}$ кои имаат по m елементи, тогаш:

а) $\bigcup\limits_{K\in F_m} Q_K \supseteq \bigcap\limits_{K\in F_m} P_K$, ако $2m \le n+1$;

б) $\bigcup\limits_{K\in F_m} Q_K \subseteq \bigcap\limits_{K\in F_m} P_K$, ако $2m \ge n+1$.

1.9. Дадени се две (дисјунктни) поделби на множеството A:

$A = \bigcup\limits_{i\in I} B_i$, $A = \bigcup\limits_{j\in J} C_j$.

Да ги земеме само непразните множества од облик $B_i \cap C_j$. Дали оваа фамилија подмножества од A формира дисјунктна поделба на множеството A? (Притоа, за една фамилија дисјунктни подмножества на A велиме дека формира *поделба* на A, ако A е унија на таа фамилија.)

Решение. Имаме:

$$\bigcup_{i,j}(B_i \cap C_j)=\bigcup_j [\bigcup_i (B_i \cap C_j)]=\bigcup_j [(\bigcup_i B_i) \cap C_j]=$$

$$\bigcup_j [A \cap C_j] = \bigcup_j C_j = A\,, \text{ и}$$

$$(B_{i_1} \cap C_{j_1}) \cap (B_{j_2} \cap C_{j_2}) = \varnothing \text{ за } i_1 \ne i_2,\ j_1 \ne j_2,$$

што значи дека фамилијата $\{B_i \cap C_j \mid i\in I\,,\ j\in J\}$ е (дисјунктна) поделба на A.

1.10. Да се покаже дека:

а) $(\bigcup\limits_{i\in I} A_i)' = \bigcap\limits_{i\in I} A_i'$;

б) $(\bigcap\limits_{i\in I} A_i)' = \bigcup\limits_{i\in I} A_i'$.

каде што A_i се подмножества од некое множество M.

(Притоа, ако $B \subseteq M$, тогаш $B' = M \setminus B$ е комплементот на B во M.)

Решение. а) Имаме:

$$x\in(\bigcup_i B_i)' \Leftrightarrow x \notin \bigcup_i B_i \Leftrightarrow (\forall i\in I)\, x\notin B_i \Leftrightarrow (\forall i\in I)\, x\in B_i' \Leftrightarrow$$

$$\Leftrightarrow x\in \bigcap_i B_i'$$

што значи дека даденото равенство е точно.

1.11. Да се покаже дека

$$\bigcap_{n=1}^{\infty} A_n = A_1 \setminus [\bigcup_{n=1}^{\infty} (A_1 \setminus A_n)].$$

Решение. $A_1 \setminus \bigcup_{n=1}^{\infty}(A_1 \setminus A_n) = A_1 \cap [\bigcup_{n=1}^{\infty}(A_1 \setminus A_n)]' =$

$$= A_1 \cap [\bigcap_{n=1}^{\infty}(A_1 \setminus A_n)'] = A_1 \cap [\bigcap_{n=1}^{\infty}(A_1' \cup A_n)] =$$

$$= \bigcap_{n=1}^{\infty}[A_1 \cap (A_1' \cup A_n)] = \bigcap_{n=1}^{\infty}(A_1 \cap A_n) = \bigcap_{n=1}^{\infty} A_n .$$

1.12. Да се покаже дека:

а) $\bigcap_{X\in\mathcal{D}} \mathbb{P}(X) = \mathbb{P}(\bigcap_{X\in\mathcal{D}} X)$;

б) $\bigcap_{X\in\mathcal{D}} \mathbb{P}(X) \subseteq \mathbb{P}(\bigcup_{X\in\mathcal{D}} X)$.

каде што $\mathbb{P}(X)$ е партитивното множество на X, а $\mathcal{D}$ е фамилија подмножества од некое множество M (т.е $\mathcal{D} \subseteq \mathbb{P}(M)$).

1.13. Да се покаже дека:

$X \times Y = X \times Z \wedge X \neq \emptyset \Rightarrow Y = Z$.

1.14. Да се покаже дека:

$$(\bigcap_i A_i) \times (\bigcap_i B_i) = \bigcap_i (A_i \times B_i). \qquad (1)$$

Дали е точно и равенството

$$(\bigcup_i A_i)) \times (\bigcup_i B_i) = \bigcup_i (A_i \times B_i)? \qquad (2)$$

Решение. Точноста на равенството (1) лесно се покажува, а равенството (2) не мора да биде точно (види, на пример, (I.11.б)). Меѓутоа, секогаш важи инклузијата

$$\bigcup_i (A_i \times B_i) \subseteq (\bigcup_i A_i) \times (\bigcup_i B_i).$$

1.15. Да се докаже дека

а) $A \times (\bigcup_i B_i) = \bigcup_i (A \times B_i)$;

б) $A \times (\bigcap_i B_i) = \bigcap_i (A \times B_i)$.

1.16. Нека I и J се две непразни множества, а $\{A_i \mid i \in I\}$ и $\{B_j \mid j \in J\}$ се две фамилии множества. Да се докажат равенствата

а) $(\bigcup_i A_i) \times (\bigcup_j B_j) = \bigcup_{i,j} (A_i \times B_j)$,

б) $(\bigcap_i A_i) \times (\bigcap_j B_j) = \bigcap_{i,j} (A_i \times B_j)$.

1.17. Да се докаже дека:

а) $(A_1 \times A_2) \setminus (B_1 \times B_2) = [(A_1 \setminus B_1) \times A_2] \cup [A_1 \times (A_2 \setminus B_2)]$.

б) $\prod_{i=1}^{n} A_i \setminus \prod_{i=1}^{n} B_i = \bigcup_{i=1}^{n} [A_1 \times \ldots A_{i-1} \times (A_i \setminus B_i) \times A_{i+1} \times \ldots \times A_n]$.

Решение. а) Да ги означиме со L и D левата и десната страна, соодветно.

Ако $(x, y) \in L$, тогаш $(x, y) \in A_1 \times A_2$ и $(x, y) \notin B_1 \times B_2$, а тоа значи дека $x \in A_1$, $y \in A_2$, ($x \notin B_1$ или $y \notin B_2$). Ако $x \notin B_1$, тогаш $x \in A_1 \setminus B_1$, кое заедно со $y \in A_2$ повлекува $(x, y) \in (A_1 \setminus B_1) \times A_2$, т.е. $(x, y) \in D$. Ако пак $y \notin B_2$, тогаш $y \in A_2 \setminus B_2$, па поради $x \in A_1$ имаме $(x, y) \in A_1 \times (A_2 \setminus B_2)$, т.е. $(x, y) \in D$.

Значи: $L \subseteq D$.

Слично добиваме дека и $D \subseteq L$, а одовде $L = D$.

б) Со индукција по n.

1.18. Да се докаже точноста на равенствата:

а) $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$;

б) $A \Delta (A \cap B) = A \setminus B$;

в) $(A \Delta B) \Delta (A \cap B) = A \cup B$.

(Притоа, $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$.)

1.19. Дали од $A \subseteq C$, $B \subseteq D$ следува $A \Delta B \subseteq C \Delta D$?

1.20. Да се покаже дека

а) $A \Delta B \subseteq (A \Delta C) \cup (B \Delta C)$;

б) $(A \setminus B) \Delta (C \setminus D) \subseteq (A \Delta C) \cup (B \Delta D)$.

Решение. а) $(A \Delta C) \cup (B \Delta C) = (A \cap C') \cup (A' \cap C) \cup (B \cap C') \cup (B' \cap C) =$

$= (A \cup B) \cap C'] \cup [C \cap (A' \cup B')] = \ldots =$

$= (A \cup B \cup C) \cap (A' \cup B' \cup C') \supseteq (A \cup B) \cap (A' \cup B') = A \Delta B$

1.21. Да се покаже дека

$(A_1 \Delta A_2 \Delta \ldots \Delta A_n) \cap B = (A_1 \cap B) \Delta (A_2 \cap B) \Delta \ldots \Delta (A_n \cap B)$.

1.22. Да се покаже дека

$(A_1 * A_2 * \ldots * A_n) \Delta (B_1 * B_2 * \ldots * B_n) \subseteq (A_1 \Delta B_1) * \ldots * (A_n \Delta B_n)$,

каде што $*$ е операцијата $\cup$ или $\cap$.

Решение.

$$\left(\bigcup_{i=1}^{n} A_i\right)\Delta\left(\bigcup_{i=1}^{n} B_i\right)=\left[\left(\bigcup_{i=1}^{n} A_i\right)\cap\left(\bigcap_{i=1}^{n} B_i'\right)\right]\cup\left[\left(\bigcap_{i=1}^{n} A_i'\right)\cap\left(\bigcup_{i=1}^{n} B_i\right)\right]=$$
$$=\left[\bigcup_{i=1}^{n}(A_i\cap B_1'\ldots\cap B_n')\right]\cup\left[\bigcup_{i=1}^{n}(A_n'\cap\ldots\cap A_1'\cap B_i)\right]\subseteq$$
$$\subseteq\left[\bigcup_{i=1}^{n}(A_i\cap B_i')\right]\cup\left[\bigcup_{i=1}^{n}(A_i'\cap B_i)\right]=$$
$$=\bigcup_{i=1}^{n}\left[(A_i\cap B_i')\cup(A_i'\cap B_i)\right]=\bigcup_{i=1}^{n}(A_i\Delta B_i)$$

Слично и за пресекот.

I.23. Нека $\mathrm{k}M = 692$, $\mathrm{k}A = 300$, $\mathrm{k}B = 230$, $\mathrm{k}C = 370$, $\mathrm{k}(A\cap B) = 150$, $\mathrm{k}(A\cap C) = 180$, $\mathrm{k}(B\cap C) = 90$, $\mathrm{k}(A\cap B'\cap C') = 10$, при што $A, B, C\subseteq M$, $X' = M\setminus X$, а kX го означува бројот на елементите на множеството X. Да се најде:

а) $\mathrm{k}(A\cap B\cap C)$;

б) $\mathrm{k}(A'\cap B\cap C')$;

в) $\mathrm{k}(A'\cap B'\cap C')$;

г) $\mathrm{k}[(A\cup B)\cap(B\cup C))\cap(C\cup A)]$.

Решение. Нека A, B, C се конечни множества. За кардиналниот број на унијата од две множества A и B имаме

$$\mathrm{k}(A\cup B) = \mathrm{k}A + \mathrm{k}B - \mathrm{k}(A\cap B) \qquad (1)$$

? → (види I.29.а).

Користејќи ја оваа формула имаме

$$\mathrm{k}(A\cup B\cup C) = \mathrm{k}[(A\cup B)\cup C] = \mathrm{k}(A\cup B) + \mathrm{k}C - \mathrm{k}[(A\cup B)\cap C] =$$
$$= \mathrm{k}A + \mathrm{k}B + \mathrm{k}C - \mathrm{k}(A\cap B) - \mathrm{k}[(A\cap C)\cup(B\cap C)], \quad \text{т.е.}$$
$$\mathrm{k}(A\cup B\cup C) =$$
$$= \mathrm{k}A + \mathrm{k}B + \mathrm{k}C - \mathrm{k}(A\cap B) - \mathrm{k}(B\cap C) - \mathrm{k}(C\cap A) + \mathrm{k}(A\cap B\cap C) \qquad (2)$$

а) Бидејќи множествата $A\setminus(B\cup C)$ и $B\cup C$ се дисјунктни, а $A\cup B\cup C = [A\setminus(B\cup C)]\cup(B\cup C)$, според (1), имаме:

$$\mathrm{k}(A\cup B\cup C) = \mathrm{k}\{[A\setminus(B\cup C)]\cup(B\cup C)\} = \mathrm{k}[A\setminus(B\cup C)] + \mathrm{k}(B\cup C) =$$
$$= \mathrm{k}(A\cap B'\cap C') + \mathrm{k}B + \mathrm{k}C - \mathrm{k}(B\cap C) = 520$$

Според (2) имаме:

$$\mathrm{k}(A\cap B\cap C) =$$
$$= \mathrm{k}(A\cup B\cup C) + \mathrm{k}(A\cap B) + \mathrm{k}(B\cap C) + \mathrm{k}(C\cap A) - \mathrm{k}A - \mathrm{k}B - \mathrm{k}C = 40$$

б) Бидејќи за $X\subseteq Y$ важи равенството

$\mathrm{k}(Y\setminus X) = \mathrm{k}Y - \mathrm{k}X$ (види I.29.б)

имаме $\mathrm{k}A' = 392$, $\mathrm{k}B' = 462$, $\mathrm{k}C' = 322$.

Бидејќи според (1)

$$\mathrm{k}(A'\cap B\cap C') =$$
$$= \mathrm{k}(A'\cup B\cup C') - \mathrm{k}A' - \mathrm{k}B - \mathrm{k}C' + \mathrm{k}(A'\cap B) + \mathrm{k}(B\cap C') + \mathrm{k}(C'\cap A),$$

ќе ги пресметаме собироците од десната страна на равенството. Имаме:

$$\mathrm{k}(A' \cap B) = \mathrm{k}(B \cap (A' \cup B')) = \mathrm{k}(B \setminus (A \cap B)) = \mathrm{k}B - \mathrm{k}(A \cap B) = 80;$$

$$\mathrm{k}(B \cap C') = \mathrm{k}B - \mathrm{k}(B \cap C) = 140;$$

$$\mathrm{k}(C' \cap A') = \mathrm{k}(M \setminus (A \cup C)) = \mathrm{k}M - \mathrm{k}A - \mathrm{k}C + \mathrm{k}(A \cap C) = 220;$$

$$\mathrm{k}(A' \cup B \cup C') = \mathrm{k}(B \cup (A \cap C)') = \mathrm{k}[(B \setminus (A \cap C)') \cup (A \cap C)'] =$$
$$= \mathrm{k}(A \cap B \cap C) + \mathrm{k}M - \mathrm{k}(A \cap C) = 552.$$

Според тоа, $\mathrm{k}(A' \cap B \cap C') = 30$.

в) $\mathrm{k}(A' \cap B' \cap C') = \mathrm{k}(M \setminus (A \cup B \cup C)) = \mathrm{k}M - \mathrm{k}(A \cup B \cup C) = 172$.

г) Бидејќи важи равенството

$(A \cup B) \cap (B \cup C) \cap (C \cup A) = (A \cap B) \cup (B \cap C) \cup (C \cap A)$,

имаме

$$\mathrm{k}[(A \cup B) \cap (B \cup C) \cap (C \cup A)] =$$
$$= \mathrm{k}(A \cap B) + \mathrm{k}(B \cap C) + \mathrm{k}(C \cap A) - 2\mathrm{k}(A \cap B \cap C) = 340.$$

1.24. Нека X е конечно множество и нека со $\mathrm{k}X$ е означен бројот на елементите во множеството X. Да се покаже дека:

$$\mathrm{k}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \mathrm{k}A_i - \sum_{i<j} \mathrm{k}(A_i \cap A_j) + \ldots + (-1)^{n+1}\, \mathrm{k}\left(\bigcap_{i=1}^{n} A_i\right).$$

Упатство. Вршејќи индукција по n. (За $n = 3$, равенството е докажано во претходната задача.)

1.25. Користејќи ја формулата од претходната задача да се најде бројот $\phi(n)$ од сите природни броеви помали или еднакви на n, заемно прости со n.

Решение. Ако $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, каде што p_i, $i = 1, 2, \ldots r$, се различни прости броеви, нека ставиме $A = \{1, 2, \ldots, n\}$, а A_i нека е подмножеството од A, чии елементи се делат со простиот број p_i, $i = 1, 2, \ldots, r$. Тогаш имаме

$$\mathrm{k}A_i = \frac{n}{p_i},\quad \mathrm{k}(A_i \cap A_j \cap \ldots \cap A_m) = \frac{n}{p_1 p_2 \cdots p_m}.$$

Бидејќи е $\phi(n) = \mathrm{k}(A \setminus (\bigcup_{i=1}^{r} A_i))$, имаме

$$\phi(n) = \mathrm{k}(A \setminus (\bigcup_{i=1}^{r} A_i)) = \mathrm{k}A - \mathrm{k}(\bigcup_{i=1}^{r} A_i) =$$

$$n-\sum_i \mathrm{k}A_i+\sum_{i<j}\mathrm{k}(A_i\cap A_j)-\sum_{i<j<m}\mathrm{k}(A_i\cap A_j\cap A_m)+\cdots+(-1)^n\mathrm{k}(\bigcap_i A_i)=$$
$$=n-\sum_i\frac{n}{p_i}+\sum_{i<j}\frac{n}{p_ip_j}-\sum_{i<j<m}\frac{n}{p_ip_jp_m}+\ldots+(-1)^n\frac{n}{p_1p_2\ldots p_r}=$$
$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right).$$

1.26. Ако множествата A_i, $i=1,\ldots,n$ се конечни, тогаш:

$$\mathrm{k}(A_1\Delta A_2\,\Delta\ldots\Delta A_n)=$$
$$\sum_i \mathrm{k}A_i-2\sum_{i,j}\mathrm{k}(A_i\cap A_j)+4\sum_{i,j,p}\mathrm{k}(A_i\cap A_j\cap A_p)-$$
$$-8\sum_{i,j,p,q}\mathrm{k}(A_i\cap A_j\cap A_p\cap A_q)+\ldots+(-1)^{n-1}2^{n-1}\mathrm{k}(A_1\cap A_2\cap\ldots\cap A_n).$$

Решение. За $n=2$ имаме:

$$\mathrm{k}(A_1\Delta A_2)=\mathrm{k}((A_1\cup A_2)\setminus((A_1\cap A_2))=\mathrm{k}(A_1\cup A_2)-\mathrm{k}(A_1\cap A_2)=$$
$$=\mathrm{k}A_1+\mathrm{k}A_2-2\mathrm{k}(A_1\cap A_2)\,;$$

а потоа врщејќи индукција по n.

§ 2. ПРЕСЛИКУВАЊА

2.1. Да се провери кои од следните пресликувања се сурјекции, инјекции, биекции:

а) $f: \mathbb{C} \to \mathbb{R}$ дефинирано со: $f(a+ib) = a^2 + b^2$.

б) $f: \mathbb{Z} \to \mathbb{N}$ дефинирано со: $f(n) = n^2 + 1$

в) $f: \mathbb{N} \to \mathbb{Q}$ дефенирано со: $f(n) = \dfrac{n}{2n+1}$.

Решение. а) Пресликувањето не е сурјекција, бидејќи, на пример, -1 не е слика на ниту еден елемент од $\mathbb{C}$ а не е ни инјекција, зашто, на пример, имаме $1 + i \neq 1 - i$, но $f(1+i) = f(1-i) = 2$

б) Не е ниту инјекција, ниту сурјекција.

в) Пресликувањето е инјекција, но не е сурјекција.

2.2. Нека m е фиксен природен број и нека $f: \mathbb{Z} \to \mathbb{Z}_m$ е дефинирано со:

$(\forall n \in \mathbb{Z})$ $f(n) = r \Leftrightarrow r$ е остатокот при делењето на n со m.

Да се докаже дека :

а) f е сурјекција.

б) ако $n_1, n_2 \in \mathbb{Z}$, тогаш $f(n_1 n_2) = f(f(n_1) f(n_2))$.

Решение. Имајќи предвид дека за секој природен број n постојат еднозначно определени броеви q и r, такви што $n = qm + r$, $0 \le r < m$, заклучуваме дека f е пресликување.

а) Бидејќи $0, 1, \ldots, m-1$ со f се пресликуваат во $0, 1, \ldots$, f е сурјекција

б) Нека $f(n_1) = r_1$ и $f(n_2) = r_2$ тогаш имаме:

$$n_1 n_2 = (q_1 m + r_1)(q_2 m + r_2) = (q_1 q_2 m + r_1 q_2 + r_2 q_1) m + r_1 r_2.$$

Ставајќи $r_1 r_2 = q_3 m + r_3$ добиваме

$$f(n_1 n_2) = r_3 = f(r_1 r_2) = f(f(n_1) f(n_2)).$$

2.3. Нека X е множеството од сите отворени интервали (a, b), а Y множеството од сите сегменти $[a, b]$, каде што $a, b \in \mathbb{R}$ и нека $f: X \to Y$ е дефинирано со $f((a, b)) = [a, b]$. Да се провери дали f е сурјекција или инјекција.

Решение. Јасно е дека f е пресликување.

Пресликувањето f е инјекција, зашто од $[a, b] = [c, d]$ следува $a = c$, $b = d$, т.е. $(a, b) = (c, d)$;

f е и сурјекција, па значи и биекција.

2.4. Нека S е множеството од сите непрекинати функции, дефинирани на $\mathbb{R}$ и нека $\varphi : S \to S$ е дефинирано со:

$$\varphi : f(x) \to (x^2 - 1) f(x) .$$

Да се покаже дека φ е инјекција но, не и сурјекција. Дали е битно барањето за непрекинатост?

Решение. Пресликувањето не е сурјекција, бидејќи, на пример, функцијата $\sin x$ не е слика (при φ) на ниедна непрекината функција.

Ако $f, g \in S$ и $f \neq g$, тогаш $(x^2 - 1) f \neq (x^2 - 1) g$, т.е. φ е инјекција.

2.5. Да се најдат подмножества S и T од $\mathbb{R}$, така што пресликувањето:

а) $f(x) = \cos x$; б) $g(x) = \sin x$ в) $h(x) = \operatorname{tg} x$

да биде биекција од S во T. Дали f, g, h, се пресликувања од $\mathbb{R}$ во $\mathbb{R}$?

Решение. а) $S = [0, \pi]$, $T = [-1,1]$. б) $S = [-\frac{\pi}{2}, \frac{\pi}{2}]$, $T = [-1,1]$.

в) $S = (-\frac{\pi}{2}, \frac{\pi}{2})$, $T = \mathbb{R}$. f и g се пресликувања од $\mathbb{R}$ во $\mathbb{R}$, а h не е.

2.6. Ако A е непразно множество, да се покаже дека тоа е бесконечно ако и само ако множеството $\mathcal{J}_A$ од сите трансформации на A е бесконечно.

Решение. Ако A е конечно множество со n елементи, тогаш $\mathcal{J}_A$ содржи точно n^n елементи, па значи, ако $\mathcal{J}_A$ е бесконечно, тогаш и A е бесконечно.

Обратно, нека A е бесконечно. За секој $a \in A$, го дефинираме пресликувањето $f_a : A \to A$ со

$$(\forall x \in A)\ f_a(x) = a.$$

Јасно е дека множеството $\{f_a \mid a \in A\}$ е бесконечно, а бидејќи е подмножество од $\mathcal{J}_A$, следува дека и $\mathcal{J}_A$ е бесконечно.

2.7. Нека f е пресликување од X во Y. Да се утврди каков е односот меѓу множествата:

а) $f(\bigcup_i A_i)$ и $\bigcup_i f(A_i)$;

б) $f(\bigcap_i A_i)$ и $\bigcap_i f(A_i)$;

в) $f(X \setminus A)$ и $Y \setminus f(A)$;

каде што $A_i, A \subseteq X$.

Решение. а) Важи равенство.

б) $f(\bigcap_i A_i) \subseteq \bigcap_i f(A_i)$.

Дека во општ случај не важи равенство, покажува следниот пример. Нека $X = Y = \mathbb{R}$, $f(x) = x^2$, $A_1 = (-\infty, 0]$ и $A_2 = [0, +\infty)$; имаме:

$f(A_1 \cap A_2) = f(\{0\}) = \{0\} \subset [0, +\infty) = f(A_1) \cap f(A_2)$.

Но, ако f е инјекција, тогаш важи равенство.

в) Во општ случај множествата $f(X \setminus A)$ и $Y \setminus f(A)$ не се споредливи, што се гледа од примерот во б) земајќи $A = A_1$.

Ако f е инјекција, тогаш $f(X \setminus A) \subseteq Y \setminus f(A)$, а ако е f сурјекција, тогаш $f(X \setminus A) \supseteq Y \setminus f(A)$, па значи равенство важи во случај f да е биекција.

2.8. Ако $f: X \to Y$ е пресликување, тогаш:

а) $f^{-1}(\bigcup_i B_i) = \bigcup_i f^{-1}(B_i)$;

б) $f^{-1}(\bigcap_i B_i) = \bigcap_i f^{-1}(B_i)$;

в) $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$,

за секои $B, B_i \subseteq Y$.

2.9. Нека f, g, h, се пресликувања од $\mathbb{Q}$ во $\mathbb{Q}$ дефинирани со:

$$f(x) = \frac{x}{2}, \quad g(x) = x + 1, \quad h(x) = x - 1.$$

Да се покаже дека $g(f(h(x))) = \dfrac{x+1}{2}$. Дали $f_{\mathbb{N}} = f_{\mathbb{Z}}$?

(f_M е рестрикцијата на f врз $M \subseteq \mathbb{Q}$.)

Решение. Имаме:

$$g(f(h(x))) = g(f(x-1)) = g\left(\frac{x-1}{2}\right) = \frac{x-1}{2} + 1 = \frac{x+1}{2}.$$

$$f_{\mathbb{N}} = \frac{n}{2}, \; f_{\mathbb{Z}} = \frac{z}{2}, \; n \in \mathbb{N}, \; z \in \mathbb{Z}.$$

Бидејќи $f_{\mathbb{N}} : \mathbb{N} \to \mathbb{Q}$, $f_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}$, $f_{\mathbb{N}}$ и $f_{\mathbb{Z}}$ не се еднакви, но $(f_{\mathbb{Z}})_{\mathbb{N}} = f_{\mathbb{N}}$.

2.10. Нака A е подмножество од множеството X и нека $f: X \to Y$ е пресликување. Да се покаже дека:

а) f е инјекција $\Rightarrow f_A$ е инјекција;

б) f_A е сурјекција $\Rightarrow f$ е сурјекција.

Решение. а) Нека f е инјекција; тогаш за кои било $a, b \in A$, $a \neq b$, имаме $f(a) \neq f(b)$. Бидејќи $f_A(a) = f(a)$, $f_A(b) = f(b)$, добиваме $f_A(a) \neq f_A(b)$, т.е. и f_A е инјекција.

б) Нека $f_A : A \to Y$ е сурјекција. Тогаш за секој $y \in Y$ постои $a \in A$ таков што $f_A(a) = y$, а тоа значи и $f(a) = y$ т.е. f е сурјекција.

2.11. Нека f, g, h се пресликувања, при што h е проширување од g, а g е проширување од f. Да се покаже дека h е проширување и од f.

Решение. Нека $A \subseteq S \subseteq X$ и нека $f : A \to Y$, $g : S \to Y$, $h : X \to Y$ се пресликувања како во условот на задачата, т.е. $f = g_A$, $g = h_S$. За кој било $a \in A$ имаме:

$$f(a) = g_A(a) = g(a) = h_S(a) = h(a),$$

па значи h се поклопува со f на A, т.е. h е проширување на f.

2.12. Нека $f : 2\mathbb{N} \to \mathbb{N}$ е пресликување. Во кој случај постои биекција од $\mathbb{N}$ во $\mathbb{N}$, која е проширување од f?

Одговор. f мора да биде инјекција, а множеството $\mathbb{N} \setminus f(2\mathbb{N})$ бесконечно.

2.13. Нека $f : X \to Y$ е пресликување и $A \subseteq X$. Покажи дека, ако $g = f_A$, тогаш

$$B \subseteq Y \Rightarrow g^{-1}(B) = A \cap f^{-1}(B).$$

2.14. Нека $f : \mathbb{Q} \to \mathbb{Q}$ е дефинирано со $f(a) = a^2 + 2$, а $g : \mathbb{Q} \to \mathbb{Q}$ со $g(a) = \frac{a}{2} - 2$. Да се пресметаат fg и gf. Дали $fg = gf$? Да се пресметаат $f(gf)$ и $(fg)f$.

Одговор. $(fg)(a) = \frac{a^2}{4} - 2a + 6$; $(gf)(a) = \frac{a^2}{2} - 1$;

$$(f(gf))(a) = ((fg)f)(a) = \frac{a^4}{4} - a^2 + 3.$$

2.15. Нека $f : X \to Y$ е пресликување и $A \subseteq X$, $B \subseteq Y$. Каков е односот меѓу множествата

а) $f^{-1}(f(A))$ и A; б) $f(f^{-1}(B))$ и B?

Одговор. а) $A \subseteq f^{-1}(f(A))$; б) $f(f^{-1}(B)) \subseteq B$.

Дека не мора да важи равенство ни во а), ни во б) покажува следниот пример:

$f : X \to Y$,

$X = \{x_1, x_2\}, Y = \{y_1, y_2\}, f(x_1) = f(x_2) = y_1, \quad A = \{x_1\}, \quad B = Y.$

2.16. Нека $f: X \to Y$ е пресликување и нека $f_* : \mathbb{P}(X) \to \mathbb{P}(Y)$ и $f^* : \mathbb{P}(Y) \to \mathbb{P}(X)$ се дефинирани со:
$f_*(A) = f(A), \quad f^*(B) = f^{-1}(B).$
при кои услови важи $f^* f_* = 1$ и $f_* f^* = 1$?

Решение. Според претходните задачи, заклучуваме дека за кое било пресликување $f: X \to Y$ важат релациите:

$$A \in \mathbb{P}(X) \Rightarrow f^* f_* (A) \supseteq A, \tag{1}$$

$$B \in \mathbb{P}(Y) \Rightarrow f_* f^* (B) \subseteq B, \tag{2}$$

Во (1) важи равенство ако и само ако f е инјекција, а во (2) ако и само ако f е сурјекција. Значи имаме:

$f^* f_* = 1 \Leftrightarrow f$ е инјекција,

$f_* f^* = 1 \Leftrightarrow f$ е сурјекција.

2.17. Ако $f: X \to Y$, и $g: Y \to Z$ се сурјекции (инјекции), тогаш и gf е сурјекција (инјекција).

2.18. Нека $f: X \to Y$, и $g: Y \to X$ се пресликувања, такви што $gf = 1_X$, $fg = 1_Y$. Да се покаже дека f и g се биекција и дека $f^{-1} = g$.

Решение. Ќе покажеме дека f е биекција, а слично се покажува и за g.

Да покажеме прво дека f е инјекција:

$f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (gf)(x_1) = (gf)(x_2) \Rightarrow$
$\Rightarrow 1_X(x_1) = 1_X(x_2) \Rightarrow x_1 = x_2.$

Да покажеме дека f е и сурјекција. Затоа, нека y е произволен елемент од Y, а $x = g(y)$. Тогаш имаме:

$f(x) = f(g(y)) = (fg)(y) = 1_Y(y) = y,$

т.е. f е сурјекција.

За да покажеме дека g е инверзно на f, треба да покажеме дека

$g(y) = x \Leftrightarrow f(x) = y.$

$g(y) = x \Rightarrow f(x) = y$ е покажано погоре.

Обратно, нека x е произволен елемент од X, а $y = f(x)$. Тогаш имаме $g(y) = g(f(x)) = (gf)(x) = x$, т.е. $f^{-1} = g$.

2.19. Нека $f: X \to Y$, $g: Y \to Z$ се пресликувања. Да се покаже дека:

а) Ако gf е инјекција, тогаш и f е инјекција.

б) Ако gf е сурјекција, тогаш и g е сурјекција.

Решение. а) Нека gf е инјекција и $f(x_1) = f(x_2)$. Тогаш имаме:

$$f(x_1) = f(x_2) \Rightarrow g(f(x_1)) = g(f(x_2)) \Rightarrow (gf)(x_1) = (gf)(x_2) \Rightarrow x_1 = x_2,$$

што значи дека f е инјекција.

б) Нека gf е сурјекција и z произволен елемент од Z. Тогаш постои $x \in X$, таков што $(gf)(x) = z$, т.е. постои елемент $f(x) = y \in Y$, таков што $g(y) = z$, што значи дека g е сурјекција.

2.20. Пресликувањето $f : X \to Y$ е инјекција ако и само ако постои пресликување $g : Y \to X$, такво што $gf = 1_X$.

Упатство. Види 2.18.

2.21. Пресликувањето $f : X \to Y$ е сурјекција ако и само ако постои пресликување $h : Y \to X$, такво што $fh = 1_Y$.

Упатство. Види 2.18.

2.22. Нека $f : A \to B$ е пресликување. Да се покаже дека постои сурјекција g и инјекција h, такви што $f = hg$.

Решение. Нека $C = f(A) \subseteq B$, а пресликувањата $g : A \to C$ и $h : C \to B$ да ги дефинираме со:

$$(\forall a \in A)\ g(a) = f(a), \quad (\forall b \in C)\ h(b) = b.$$

Јасно е дека h е инјекција, g е сурјекција и $f = hg$.

2.23. Да се покаже дека пресликувањето $f : X \to Y$ е инјекција ако и само ако за кое било множество U и кои било пресликувања $g_1, g_2 : U \to X$ е исполнет условот

$$fg_1 = fg_2 \Rightarrow g_1 = g_2 \qquad (1)$$

Решение. Нека $f : X \to Y$ е инјекција, а $g_1, g_2 : U \to X$ кои било пресликувања со својството $fg_1 = fg_2$. Тогаш, за секој $u \in U$, имаме

$$fg_1 = fg_2 \Rightarrow (fg_1)(u) = (fg_2)(u) \Rightarrow f(g_1(u)) = f(g_2(u)) \Rightarrow$$
$$\Rightarrow g_1(u) = g_2(u) \Rightarrow g_1 = g_2.$$

Обратно, нека за пресликувањето f е исполнет условот (1) за кое било U и кои било пресликувања $g_1, g_2 : U \to X$.

Ако f не би било инјекција, ќе постојат елементи $x_1, x_2 \in X$, $x_1 \neq x_2$, за кои $f(x_1) = f(x_2)$. Ставајќи $U = \{x_1, x_2\}$, $g_1(x_1) = x_1$, $g_1(x_2) = x_2$, $g_2(x_1) = g_2(x_2) = x_1$, тогаш $fg_1 = fg_2$, но $g_1 \neq g_2$.

2.24. Да се покаже дека пресликувањето $f : X \to Y$ е сурјекција ако и само ако за кое било множество Z и кои било пресликувања $h_1, h_2 : Y \to Z$ е исполнет условот

$$h_1 f = h_2 f \Rightarrow h_1 = h_2. \qquad (1)$$

Решение. Нека f е сурјекција и $h_1 f = h_2 f$, за кои било пресликувања $h_1, h_2 : Y \to Z$. Треба да покажеме дека $h_1 = h_2$, т.е. дека за секој $y \in Y$, $h_1(y) = h_2(y)$. Затоа, нека y е произволен елемент од Y, а x е еден од оние елементи од X за кои $f(x) = y$. Тогаш имаме:

$$h_1 f = h_2 f \Rightarrow (h_1 f)(x) = (h_2 f)(x) \Rightarrow h_1(f(x)) = h_2(f(x)) \Rightarrow$$
$$\Rightarrow h_1(y) = h_2(y) \Rightarrow h_1 = h_2.$$

Обратно, нека за пресликувањето f е исполнет условот (1) за кое било множество Z и кои било пресликувања $h_1, h_2 : Y \to Z$. Ако f не е сурјекција, тогаш ќе постои барем еден елемент $y_0 \in Y \setminus f(X)$. Ставајќи $Z = Y$ и

$$h_1(y) = \begin{cases} y_1 \neq y_0, & \text{за} \quad y = y_0 \\ y, & \text{за} \quad y \neq y_0 \end{cases} \qquad h_2(y) = y,$$

добиваме дека $h_1 f(x) = h_2 f(x)$. Според (1) треба да е и $h_1(y) = h_2(y)$ за секој $y \in Y$, но тоа не е точно, на пример, за $y = y_0$, што претставува противречност на (1). Значи, f е сурјекција.

2.25. Слично како во претходните две задачи, да се даде карактеристика и за биекциите.

Решение. Според претходните две задачи, заклучуваме дека пресликувањето $f : X \to Y$ е биекција, ако и само ако, за кои било множества U и Z и кои било пресликувања

$g_1, g_2 : U \to X$ и $h_1, h_2 : Y \to Z$ се исполнети условите:

$f g_1 = f g_2 \Rightarrow g_1 = g_2$, $h_1 f = h_2 f \Rightarrow h_1 = h_2$.

2.26. Да се покаже дека:

$X^Y = Y^X \Rightarrow X = Y$.

Решение. Нека $f \in X^Y$; тогаш f е пресликување од Y во X, а бидејќи $X^Y = Y^X$ следува дека f е пресликување и од X во Y. Значи, $X = Y$.

2.27. Нека f е пресликување од X во Y, а A непразно множество. Со помош на f да се определат пресликувања $f^0 : A^Y \to A^X$ и $f_0 : X^A \to Y^A$.

Решение. Нека $f : X \to Y$ е дадено пресликување и нека φ е произволен елемент од A^Y, т.е. $\varphi : Y \to A$ е произволно пресликување. Тогаш φf е пресликување од X во A, па ставајќи:

$$f^0(\varphi) = \varphi f,$$

добиваме пресликување $f^0 : A^Y \to A^X$.

Нека ψ е произволен елемент од X^A, т.е. ψ е пресликување од A во X. Тогаш и $f\psi$ е пресликување од A во Y, па ставајќи

$f_0(\psi) = f\psi$,

добиваме пресликување $f_0 : X^A \to Y^A$.

2.28. За две множества A и B велиме дека се *еквивалентни* (или дека имаат ист кардинален број), пишуваме $A \sim B$, ако постои биекција од A во B. Да се покаже дека:

а) $A \sim A$.

б) $A \sim B \Rightarrow B \sim A$.

в) $A \sim B \wedge B \sim C \Rightarrow A \sim C$.

Решение. а) Бидејќи $1_A : A \to A$ е биекција, следува дека $A \sim A$.

б) Нека $A \sim B$; тоа значи дека постои биекција f од A во B, а бидејќи f^{-1} е бијекција од B во A, следува дека $B \sim A$.

в) Нека $A \sim B$ и $B \sim C$; тоа значи дека постојат биекции f од A во B и g од B во C. според 2.17, gf е биекција од A во C, па значи $A \sim C$.

2.29. Ако A е конечно множество, тогаш пресликувањето $f : A \to A$ е инјекција ако и само ако е сурјекција.

2.30. Да се покаже дека секое бесконечно множество содржи еквивалентно вистинско подмножество.

2.31. Секое множество A, коешто е еквивалентно со множеството $\mathbb{N}$ од природните броеви се вика *пребројливо* множество.

Да се докаже дека секое подмножество од едно пребројливо множество е пребројливо или конечно.

Решение. Нека A е пребројливо множество, а B е подмножество од A. Множеството A можеме да го запишеме во обликот

$A = \{ a_1, a_2, \ldots, a_n, \ldots \}$

а множеството B во обликот

$B = \{ a_{n_1}, a_{n_2}, \ldots \}$

Ако меѓу броевите $n_1, n_2, \ldots$ има најголем, тогаш B е конечно, а во спротивниот случај B е пребројливо.

2.32. Да се покаже дека секое бесконечно множество има пребројливо подмножество.

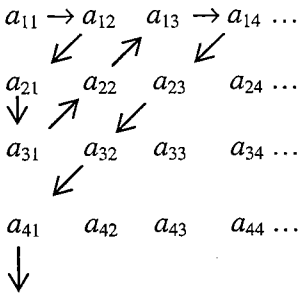
2.33. Ако $f : X \to Y$ е пресликување и X е пребројливо, тогаш множеството $f(X)$ е пребројливо или конечно.

2.34. Ако секое множество од фамилијата $\{A_i \mid i \in I\}$, каде што I е конечно или пребројливо е пребројливо, тогаш и множеството $A = \bigcup_i A_i$ е пребројливо.

Решение. Можеме да претпоставиме дека множествата A_i се пар по пар дисјунктни, т.е. дека $A_i \cap A_j = \emptyset$ за $i \neq j$, зашто во спротивниот случај можеме да ги разгледуваме множествата A_1, $A_2 \setminus A_1$, $A_3 \setminus (A_1 \cup A_2)$,..., секое од кои е конечно или пребројливо, а нивната унија го дава множеството A. Елементите од множествата A_1, A_2 ,... можеме да ги напишеме во следната шема:

$$\begin{array}{lll} a_{11} & a_{12} \ldots a_{1n} \ldots \\ a_{21} & a_{22} \ldots a_{2n} \ldots \\ \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2} \ldots a_{nn} \ldots \\ \vdots & \vdots \quad \vdots \end{array}$$

каде што во првата редица се елементите од A_1, во втората се елементите од A_2 итн. Сите овие елементи да ги индексираме "дијагонално", т.е. за прв елемент да го земеме a_{11}, за втор a_{12}, итн., одејќи по стрелките од шемата:



Јасно е дека притоа секој елемент ќе добие и свој индекс, т.е. има биекција a од A во $\mathbb{N}$, а тоа значи дека A е пребројливо.

2.35. Ако $\{A_i \mid i = 1, 2, \ldots, n\}$ е конечна фамилија од пребројливи множества, тогаш и множеството $A = \prod_i A_i$ е пребројливо.

Решение. Бидејќи секое од множествата A_i е пребројливо, наместо $\prod_1^n A_i$ ќе го разгледаме n–тиот декартов степен од едно пребројливо

множество M. Значи треба да докажеме дека множеството $M^n = M \times M \times \ldots \times M$, е пребројливо.

За $n = 1$, $M^1 = M$ е пребројливо по услов. Да претпоставиме дека M^{n-1} е пребројливо. Тогаш елементите од $M^{n-1} \times M$ се од облик (x, y), каде што $x \in M^{n-1}$ и $y \in M$. За секое фиксирано x, множеството од парови (x, y), кога y се менува во M, е пребројливо. Такви множества има точно толку колку што има елементи во M^{n-1}, а тоа според индуктивната претпоставка е пребројливо. Значи $M^{n-1} \times M$ е составено од пребројливо многу пребројливи множества, па според 2.34. тоа е пребројливо. Бидејќи множествата $M^{n-1} \times M$ и M^n се еквивалентни, следува дека и M^n е пребројливо.

2.36. Да се докаже дека множеството од сите полиноми со рационални коефициенти е пребројливо.

Решение. Секој полином од n-ти степен, $a_0 + a_1 x + \ldots a_n x^n$, може да се разгледува како подредена $(n + 1)$–ка $(a_0, a_1, \ldots, a_n)$ од рационални броеви. Множеството од сите полиноми, за секој фиксен природен број n, според задачата 2.35, е пребројливо. Ако n се менува во $\mathbb{N}$, добиваме пребројливо многу пребројливи множества, па според 2.34, добиваме дека множеството од сите полиноми со рационални коефициенти е пребројливо.

2.37. Ако M е бесконечно множество, а A пребројливо, тогаш $\mathrm{k}M = \mathrm{k}(M \cup A)$.

Решение. Нека M е произволно бесконечно множество, а $A = \{a_1, a_2, \ldots\}$ пребројливо множество, такво што $M \cap A = \varnothing$. Секое бесконечно множество содржи пребројливо подмножество (2.32.), па нека $B = \{b_1, b_2, \ldots,\}$ е пребројливо подмножество од M. Ставајќи $C = M \setminus B$, добиваме $M = C \cup B$, $M \cup A = C \cup (B \cup A)$.

Пресликувањето $f: M \cup A \to M$, дефинирано со:

$$f(x) = \begin{cases} x, & \text{ако } x \in C \\ b_{2k}, & \text{ако } x \in B \ \ (k \in \mathbb{N}) \\ b_{2k-1}, & \text{ако } x \in A \end{cases}$$

е биекција од $M \cup A$ во M, па значи $\mathrm{k}(M \cup A) = \mathrm{k}M$.

2.38. Ако A е бесконечно множество, $\mathrm{k}A > \mathrm{k}\mathbb{N}$, а B е конечно или пребројливо, тогаш $\mathrm{k}(A \setminus B) = \mathrm{k}A$.

Упатство. Следува од 2.37.

2.39. Бројот x се вика *алгебарски* број ако тој е корен на некој полином со рационални коефициенти, а во спротивен случај x се вика *трансцендентен* број.

Да се докаже дека множеството од сите алгебарски броеви е пребројливо, а множеството од сите трасцендентни броеви е непребројливо.

Решение. Според основната теорема на алгебрата, секој полином од n–ти степен има најмногу n различни корени. Бидејќи множеството полиноми со рационални коефициенти е пребројливо (2.36.), добиваме дека множеството од алгебарски броеви, како унија од пребројливо многу конечни множества, е пребројливо.

Да го означиме со T множеството трансцендентни броеви, а со A множеството од алгебарските броеви. Тогаш $T = \mathbb{R} \setminus A$, па бидејќи $\mathbb{R}$ е непребројливо, според 2.38., добиваме дека и T е непребројливо.

2.40. Да се покаже дека за секое бесконечно множество постои поделба на пребројливо многу бесконечни множества.

Решение. Нека е A бесконечно множество. Според 2.32, A има пребројливо подмножество, па за поедноставно изразување, ќе сметаме дека $\mathbb{N}$ е подмножество од A. За секој прост број p го формираме подмножеството

$$M_p = \{p^n \mid n \in \mathbb{N}\}.$$

Јасно е дека M_p е бесконечно и $\{M_p \mid p\text{–прост}\}$ е пребројлива фамилија. Ако ставиме $B = A \setminus (\cup M_p)$, тогаш добиваме дека B е бесконечно, $A = B \cup (\cup M_p)$, $B \cap M_p = \varnothing$ за секој p и $M_p \cap M_q = \varnothing$, за $p \neq q$, т.е. фамилијата составена од B и M_p е поделба на A што го исполнува условот на задачата.

2.41. Ако A е дадено множество, а $B = \mathbb{P}(A)$, тогаш $\mathrm{k}B > \mathrm{k}A$.

Решение. Бидејќи множеството $C = \{X \mid X = \{x\}, x \in A\}$, е подмножество од B еквивалентно со A, заклучуваме дека $\mathrm{k}B \geq \mathrm{k}A$. Ќе поажеме дека не може да биде $\mathrm{k}B = \mathrm{k}A$, од каде што ќе следува $\mathrm{k}B > \mathrm{k}A$.

За таа цел, нека $f : A \to B$ е која било инјекција, а X она подмножество од A, чии елементи не припаѓаат на своите слики, т.е.

$$X = \{x \mid x \in A, x \notin f(x)\}. \qquad (1)$$

Јасно е дека $X \in B$. Да претпоставиме дека за некој $a \in A$, имаме $f(a) = X$. Ако $a \in X$ тогаш од (1) следува дека $a \notin X$, а ако пак $a \notin X$, тогаш според (1), следува $a \in X$. Значи елементот $a \in A$, за кој $f(a) = X$, треба истовремено и да му припаѓа и да не му припаѓа на X. Според тоа, таков елемент не постои, т.е. инјекцијата f не е сурјекција. Значи, не постои биекција од A во B, т.е. A и B не се еквивалентни.

2.42. Ако множеството B има барем два елемента, тогаш за множествата A и $C = B^A$ важи $\mathrm{k}C > \mathrm{k}A$.

Решение. Бидејќи множеството B содржи барем два елемента, два од неговите елементи да ги обележиме со 0 и 1. Ако $D = \{0,1\}^A$, тогаш е јасно дека $\mathrm{k}D \leq \mathrm{k}C$. Но множествата $\mathbb{P}(A)$ и D се еквивалентни, бидејќи пресликувањето $f: \mathbb{P}(A) \to D$, дефинирано со

$$(\forall X \in \mathbb{P}(A))\ f(X) = \varphi \Leftrightarrow (\,(\forall x \in X)\ \varphi(x) = 1,$$

е биекција т.е. $|\,\mathbb{P}(A)\,| = |\,D\,|$. Според претходната задача имаме $\mathrm{k}A < \mathrm{k}\mathbb{P}(A) = \mathrm{k}D \leq \mathrm{k}C$, т.е. $\mathrm{k}A < \mathrm{k}C$.

2.43. Нека A и B се две множества, такви што $\mathrm{k}A \leq \mathrm{k}B$ и $\mathrm{k}B \leq \mathrm{k}A$. Да се покаже дека $\mathrm{k}A = \mathrm{k}B$.

Решение. Од $\mathrm{k}A \leq \mathrm{k}B$ следува дека постои инјекција $f: A \to B$, а од $\mathrm{k}B \leq \mathrm{k}A$ следува дека постои инјекција $g: B \to A$. Да ставиме $A_1 = g(B)$, $B_1 = f(A)$. Тогаш множеството $gf(A) = g(B_1) = A_2$ е подмножество од A_1 и е еквивалентно со A. Исто така множеството $fg(B) = f(A_1) = B_2$ е подмножество од B_1 и е еквивалентно со B. Продолжувајќи така, ги добиваме множествата $A_3, A_4, \ldots$, со особината $gf(A_k) = A_{k+2}$ и притоа $A \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_k \supseteq \ldots$. Да ставиме

$$D = \bigcap_1^\infty A_k.$$

Множеството A можеме да го претставиме на следниот начин

$$A = D \cup (A \setminus A_1) \cup (A_1 \setminus A_2) \cup \ldots \cup (A_k \setminus A_{k+1}) \cup \ldots,$$

при што множествата во унијата се, пар по пар дисјункти. Исто така имаме

$$A_1 = D \cup (A_1 \setminus A_2) \cup \ldots \cup (A_k \setminus A_{k+1}) \cup \ldots.$$

Да ги напишеме изразите за A и A_1 во обликот

$$A = D \cup [(A_1 \setminus A_2) \cup (A_3 \setminus A_4) \cup \ldots] \cup [(A \setminus A_1) \cup (A_2 \setminus A_3) \cup \ldots], \qquad (1)$$

$$A_1 = D \cup [(A_1 \setminus A_2) \cup (A_3 \setminus A_4) \cup \ldots] \cup [(A_2 \setminus A_3) \cup (A_4 \setminus A_5) \cup \ldots], \qquad (2)$$

Од $gf(A \setminus A_1) = gf(A) \setminus gf(A_1) = A_2 \setminus A_3$, следува дека множествата $A \setminus A_1$ и $A_2 \setminus A_3$ се еквивалентни. Слично добиваме дека множествата $A_2 \setminus A_3$ и $A_4 \setminus A_5$ се еквивалентни итн. Затоа, множествата во вторите делови од (1) и (2) се еквивалентни, а бидејќи првите

делови им се исти, следува дека множествата A и A_1 се еквивалентни. Но, A_1 и B се еквивалентни, па значи такви се и множествата A и B.

Да забележиме дека биекција φ од A во A_1 може да биде дадена со:

$$\varphi(x)=\begin{cases} g^{-1}(x) & \text{ако } x\in D\cup(A_1\setminus A_2)\cup(A_3\setminus A_4)\cup\ldots \\ f(x) & \text{ако } x\in(A\setminus A_1)\cup(A_2\setminus A_3)\cup\ldots \end{cases}$$

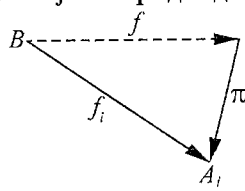
2.44. Нека $M=M_1\times M_2\times\ldots\times M_n$, $S=M_{\alpha_1}\times M_{\alpha_2}\times\ldots\times M_{\alpha_n}$, каде што $\alpha: i\to\alpha_i$ е пермутација на множеството $\{1,2,\ldots,n\}$. Да се покаже дека $\mathrm{k}M=\mathrm{k}S$.

Решение. Пресликувањето $f: M\to S$, дефинирано со:

$f(x_1,\ldots,x_n)=(x_{\alpha_1},\ldots,x_{\alpha_n})$ е биекција, па $\mathrm{k}M=\mathrm{k}S$

2.45. Нека $\{A_i \mid i\in I\}$ е произволна фамилија, B е кое било множество и $f_i: B\to A_i$ која било фамилија пресликувања. Да се покаже дека постои еднозначно определено пресликување $f: B\to P=\prod_i A_i$, такво што $\pi_i f=f_i$, каде што π_i е $i-$тата проекција од P на A_i.

Решение. Нека $x\in B$ е произволен елемент и $f(x)=x_i$. Така, за секој $x\in B$, со помош на фамилијата f_i, можеме да ја формираме низата (x_i). Имајќи предвид дека тоа е елемент од P, ќе дефинираме пресликување $f: B\to P$ со: $(\forall x\in B)\, f(x)=(x_i)$, при што $x_i=f_i(x)$ и $\pi_i((x_i))=x_i$. Ако $(y_i)\in P$ и $f(x)=(y_i)$, тогаш би било: $y_i=\pi_i((y_i))=f_i(x)=x_i$, т.е. $(x_i)=(y_i)$, што значи дека f е пресликување.



Ако $g: B\to P$ би било друго пресликување, со особината $\pi_i g=f_i$, при што $g(x)=(y_i)$, би имале $f_i(x)=x_i$ и $\pi_i g(x)=\pi_i((y_i))=y_i$. Поради $\pi_i g=f_i$ имаме $x_i=y_i$, т.е. $g=f$.

2.46. Нека $\{A_i \mid i\in I\}$ е фамилија множества, A дадено множество и $\varphi_i: A\to A_i$, $i\in I$, фамилија пресликувања, така што за секое множество B и секоја фамилија пресликувања $f_i: B\to A_i$ постои еднозначно определено пресликување $f: B\to A$, така што

$$\varphi_i f=f_i,\qquad \forall i\in I.$$

Да се докаже дека е $A\sim P=\prod_i A_i$.

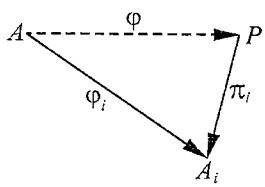
Решение. Според условот на задачата за множеството P и фамилијата пресликувања $\pi_i : P \to A_i$, постои еднозначно определено пресликување $g : P \to A$, такво што

$$\varphi_i g = \pi_i. \tag{1}$$

Но, според претходната задача, за кое било множество A и која било фамилија пресликувања $\varphi_i : A \to A_i$, постои еднозначно определено пресликување $\varphi : A \to P$ со својството

$$\pi_i \varphi = \varphi_i. \tag{2}$$

Од (1) и (2) имаме $\pi_i = \pi_i(\varphi g)$ и $\varphi_i = \varphi_i(g\varphi)$. Ако во дијаграмот



ставиме $A = P$ и $\varphi_i = \pi_i$, за $\varphi : P \to P$ можеме да го земеме $1_P : P \to P$, а бидејќи φ е единствено, од $\pi_i = \pi_i 1_P$ и $\pi_i = \pi_i(\varphi g)$, добиваме $\varphi g = 1_P$. Слично добиваме и $g\varphi = 1_P$, па значи φ е биекција од A на P.

§ 3. КОРЕСПОНДЕНЦИИ И РЕЛАЦИИ

3.1. Да се напишат сите кореспонденции од $A = \{1, 2, 3\}$ во $B = \{b\}$.

Решение. $\varnothing$, $\{(1, b)\}$, $\{(2, b)\}$, $\{(3, b)\}$, $\{(1, b), (2, b)\}$, $\{(1, b), (3, b)\}$, $\{(2, b), (3, b)\}$, $A \times B$.

3.2. Ако A е множество со m елементи, а B множество со n елементи, да се најде бројот на кореспонденциите од A во B.

Решение. Бидејќи секоја кореспонденција е подмножество од $A \times B$, а $A \times B$ има mn елементи, бројот на кореспонденциите од A во B е 2^{mn}.

3.3. Нека α е кореспонденција од $A = \{2, 3, 5, 6\}$ во $B = \{3, 4, 6, 9\}$ дефинирана со:

$x \alpha y \Leftrightarrow x \mid y$.

а) Да се напише кореспонденцијата α експлицитно.

б) Да се најде кореспонденцијата α^{-1}.

в) Да се најде $\alpha(\{2, 6\})$.

Решение. а) $\alpha = \{(2, 4), (2, 6), (3, 3), (3, 6), (3, 9), (6, 6)\}$.

б) $\alpha^{-1} = \{(4, 2), (6, 2), (3, 3), (6, 3), (9, 3), (6, 6)\}$.

в) $\alpha(\{2, 6\}) = \{4, 6\}$.

3.4. Ако $\alpha \subseteq A \times B$ е кореспонденција, а $\{C_i \mid i \in I\}$ е фамилија подмножества од A, да се покаже дека:

а) $\alpha(\bigcup_i C_i) = \bigcup_i \alpha(C_i)$.

б) $\alpha(\bigcap_i C_i) \subseteq \bigcap_i \alpha(C_i)$.

Решение. а) Нека $y \in \alpha(\bigcup_i C_i)$; тоа значи дека има барем еден $x \in (\bigcup_i C_i)$, така што $x \alpha y$, т.е. дека $x \alpha y$ за некој $i_0 \in I$ и $x \in C_{i_0}$ односно $y \in \bigcup_i \alpha(C_{i_0})$ за некој $i_0 \in I$. На крајот, имаме $y \in \bigcup_i \alpha(C_i)$, т.е.

$$\alpha(\bigcup_i C_i) \subseteq \bigcup_i \alpha(C_i) \tag{1}$$

Обратно, нека $y \in \bigcup_i \alpha(C_i)$; тогаш постои $i_1 \in I$, така што $y \in \alpha(C_{i_1})$, односно постои барем еден $x \in C_{i_1}$, така што $x \alpha y$, што значи дека $y \in \alpha(\bigcup_i C_i)$ т.е.

$$\alpha(\bigcup_i C_i) \supseteq \bigcup_i \alpha(C_i) \qquad (2)$$

Од (1) и (2) следува равенството.

б) Слично како под а).

Дека не мора да важи равенство, покажува следниот пример. Нека $A = \{a_1, a_2\}$, $B = \{b\}$, $\alpha = A \times B$, $C_1 = \{a_1\}$, $C_2 = \{a_2\}$. Тогаш имаме:

$\alpha(C_1 \cap C_2) = \alpha(\varnothing) = \varnothing$, $\alpha(C_1) \cap \alpha(C_2) = \{b\}$.

3.5. Нека α е кореспонденција од A во B, а $\{\beta_i \mid i \in I\}$ е фамилија кореспонденции од A во B. Да се покаже дека:

а) $(\alpha^{-1})^{-1} = \alpha$;

б) $(\bigcup_i \beta_i)^{-1} = \bigcup_i \beta_i^{-1}$;

в) $(\bigcap_i \beta_i)^{-1} = \bigcap_i \beta_i^{-1}$.

Решение. б) $(b, a) \in (\bigcup_i \beta_i)^{-1} \Leftrightarrow (a, b) \in (\bigcup_i \beta_i) \Leftrightarrow (\exists i \in I)(a, b) \in \beta_i \Leftrightarrow$

$\Leftrightarrow (\exists i \in I)\,(b, a) \in \beta_i^{-1} \Leftrightarrow (b, a) \in \bigcup_i \beta_i^{-1}$.

3.6. Нека α е кореспонденција од $A = \{2, 3, 4, 5\}$ во $B = \{3, 6, 7, 10\}$ дефинирана со:

$x \,\alpha\, y \Leftrightarrow x \mid y$,

а β кореспонденција од $C = \{3, 7, 10\}$ во C дефинирана со:

$x \,\beta\, y \Leftrightarrow x + y = 13$.

Да се најде $\beta\alpha$.

Одговор. $\beta\alpha = \{(3, 10)\}$.

3.7. Ако α е кореспонденција од A во B, а $\{\beta_i \mid i \in I\}$ фамилија кореспонденции од C во D, да се покаже дека:

а) $(\bigcup_i \beta_i)\alpha = \bigcup_i (\beta_i \alpha)$

б) $(\bigcap_i \beta_i)\alpha \subseteq \bigcap_i (\beta_i \alpha)$

Решение. а) Нека $(a, d) \in (\bigcup_i \beta_i)\alpha$; тоа значи дека постои $b \in B \cap C$, таков што $(a, b) \in \alpha$ и $(b, d) \in \bigcup_i \beta_i$, т.е. постои $i_o \in I$, таков што $(b, d) \in \beta_{i_o}$.

Од $(a, b) \in \alpha$ и $(b, d) \in \beta_{i_o}$ следува дека $(a, d) \in \beta_{i_o}\alpha$, т.е.

$(a, d) \in \bigcup_i (\beta_i \alpha)$. Според тоа:

$$(\bigcup_i \beta_i)\alpha \subseteq \bigcup_i (\beta_i \alpha). \quad (1)$$

На сличен начин се покажува дека

$$(\bigcup_i \beta_i)\alpha \supseteq \bigcup_i (\beta_i \alpha), \quad (2)$$

што значи дека даденото равенство е точно.

б) Како и под а). Дека во општ случај не мора да важи равенство покажува следниов пример.

Ако е $A = \{a\}$, $B = \{b, c\} = C$, $D = \{d\}$, $\alpha = \{(a, b), (a, c)\}$, $\beta_1 = \{(b, d)\}$, $\beta_2 = \{(c, d)\}$, тогаш имаме:

$$\beta_1 \cap \beta_2 = \varnothing,\ (\beta_1 \cap \beta_2)\alpha = \varnothing,\ \beta_1\alpha \cap \beta_2\alpha = \{(a, d)\}.$$

3.8. Кореспонденцијата $\varphi \subseteq A \times B$ е пресликување ако и само ако $\Delta_A \subseteq \varphi^{-1}\varphi$, $\varphi\varphi^{-1} \subseteq \Delta_B$.

Решение. Лесно се воочува дека:

$$\Delta_A \subseteq \varphi^{-1}\varphi \Leftrightarrow (\forall a \in A)\ (\exists b \in B)\ (a, b) \in \varphi,$$

$$\varphi\varphi^{-1} \subseteq \Delta_B \Leftrightarrow ((a, b_1),\ (a, b_2) \in \varphi \Rightarrow b_1 = b_2),$$

од каде што следува горното тврдење.

3.9. Ако b_1 и b_2 се две дадени прави од една афина рамнина, тогаш постои најмногу една точка, којашто лежи и на двете прави.

Решение. Нека b_1 и b_2 се две различни прави од афината рамнина α; да претпоставиме дека постојат две различни точки a_1 и a_2 што лежат на правите b_1 и b_2. Според дефиницијата на афина рамнина, за кои било две различни точки постои единствена права на којашто тие лежат, па значи за точките a_1 и a_2 постои единствена права b што минува низ a_1 и a_2. Но, правите b_1 и b_2 се такви, па значи имаме $b = b_1 = b_2$, спротивно на претпоставката дека $b_1 \neq b_2$. Според тоа, постои најмногу една точка a, којашто лежи на двете различни прави b_1 и b_2.

3.10. Во која било афина рамнина постојат барем четири точки, така што кои било три не лежат на иста права.

Решение. Нека точките a_1, a_2, a_3 се такви што да не лежат на иста права. Нека b_1 е единствената права што минува низ точките a_2 и a_3, а b_2 единствената права што минува низ точките a_3 и a_1. Точката a_1 не лежи на правата b_1, па постои единствена права b_3, којашто минува низ a_1 и е паралелна со b_1. Точката a_2 не лежи на правата b_2 па постои единствена права b_4, којашто минува низ правата a_2 и е паралелна со правата b_2. Јасно е дека правите b_3 и b_4 не се паралелни, па според 3.9. тие имаат единствена заедничка точка.

Нека е тоа точката a_4. Точките a_i, $i = 1, 2, 3, 4$, се такви што кои било три од нив не лежат на иста права.

3.11. Нека кореспонденцијата α гради структура на афина рамнина над множествата A и B и нека постои права b_0 на која лежат точно n точки. Да се покаже дека:

а) На секоја права лежат точно n точки.

б) Низ секоја точка минуваат точно $n + 1$ права.

в) Во рамнината постојат точно n^2 точки и $n^2 + n$ прави.

Решение. а) Нека на правата b_0 лежат точно n точки и нека a е точка, којашто не лежи на правата b_0. Која било точка a_i, $i = 1,..., n$ од правата b_0 и точката a определуваат единствена права b_i, $i = 1, 2,..., n$. Бидејќи правата b_0 не минува низ точката a, низ точката a минува единствената права b_{n+1}, која што е паралелна со правата b_0. Значи, низ точката a минуваат барем $n + 1$ права. Ако b е произволна права низ a, тогаш таа е, или паралелна со правата b_0, или ја сече во единствена точка, т.е. или $b = b_{n+1}$, или $b = b_i$, за некое $i = 1,..., n$. Според тоа, низ точката a, којашто не лежи на правата b_0 минуваат точно $n + 1$ права.

Нека сега b е произволна права, различна од b_0. Според 3.10. постои точка a_0, којашто не лежи ниту на правата b ниту на правата b_0. Бидејќи a_0 не лежи на b_0, низ неа минуваат точно $n + 1$ права. Една од тие прави е паралелна со правата b, а секоја друга, од останатите n ја сече правата b во единствена точка, т.е. на секоја права лежат точно n точки.

б) Нека a е произволна точка. Можеме да претпоставиме дека точката a лежи на правата b_0, зашто другиот случај е разгледан во а). Значи, нека точката a лежи на правата b_0 и нека b е права што не минува низ a. Правата b е различна од b_0 и, според а) , на неа лежат точно n точки. Бидејќи точката a не лежи на правата b, слично како под а), заклучуваме дека и низ точката a минуваат точно $n + 1$ права.

в) Нека a е која било точка од рамнината. Која било друга точка лежи само на една права којашто минува низ точката a. Низ точката a минуваат точно $n + 1$ права и секоја од нив содржи точно n точки. Бидејќи точката a лежи на сите овие прави, во рамнината постојат точно $n(n + 1) - n = n^2$ точки.

Слично добиваме дека во рамнината постојат точно $n^2 + n$ прави.

3.12. Нека A е непразно множество, а $B = \{A_i \mid i \in I\}$ е фамилија подмножества од A, со следните својства.

1) За кои било два елемента a, $b \in A$, постои едно и само едно множество $A_i \in B$, така што $a, b \in A_i$.

2) Ако $a \in A$, $A_i \in B$ и ако $a \notin A_i$ тогаш постои само едно $A_j \in B$, такво што $a \in A_j$ и $A_i \cap A_j = \emptyset$.

3) Постојат три елементи a, b, $c \in A$, коишто не припаѓаат на едно исто множество $A_i \in B$.

Да се покаже дека кореспонденцијата α, дефинирана со

$(a, A_i) \in \alpha \Leftrightarrow a \in A_i$,

дефинира афина рамнина над A и B.

3.13. Нека $A = \{a, b, c, d\}$ и нека $B = \{A_i \mid i = 1, 2, ..., 6\}$, каде што $A_1 = \{a, b\}$, $A_2 = \{c, d\}$, $A_3 = \{a, c\}$, $A_4 = \{b, d\}$, $A_5 = \{a, d\}$, $A_6 = \{b, c\}$. Да се провери дали се добива афина рамнина во смисла на претходната задача.

Решение. Да ги провериме својствата 1), 2) и 3) од претходната задача.

1) Лесно се гледа дека кои било два елемента припаѓаат на само едно од множествата A_i. Така, на пример елементите a и b му припаѓаат само на множеството A_1; елементите a и c му припаѓаат само на множеството A_3; итн.

2) И овде да дадеме само еден пример. Елементот b не му припаѓа на множеството A_3 и множеството A_4 е единствено со својството $b \in A_4$ и $A_3 \cap A_4 = \emptyset$.

3) Ова својство очигледно е исполнето, зашто ни едно од множествата A_i не содржи три елементи. Значи кои било три елементи од A се такви што не припаѓаат на исто множество од множествата A_i.

3.14. Нека $A = \{a_{ij} \mid i, j = 1, 2, 3\}$ е множество со девет елементи и нека ги формираме следните подмножества од A:

$A_1 = \{a_{11}, a_{12}, a_{13}\}$, $A_2 = \{a_{21}, a_{22}, a_{23}\}$, $A_3 = \{a_{31}, a_{32}, a_{33}\}$,

$A_4 = \{a_{11}, a_{21}, a_{31}\}$, $A_5 = \{a_{12}, a_{22}, a_{32}\}$, $A_6 = \{a_{13}, a_{23}, a_{33}\}$,

$A_7 = \{a_{11}, a_{22}, a_{33}\}$, $A_8 = \{a_{12}, a_{21}, a_{33}\}$, $A_9 = \{a_{13}, a_{21}, a_{23}\}$,

$A_{10} = \{a_{11}, a_{23}, a_{32}\}$, $A_{11} = \{a_{12}, a_{23}, a_{31}\}$, $A_{12} = \{a_{13}, a_{21}, a_{31}\}$

Да се покаже дека со тоа е добиена структура на афина рамнина.

3.15. Слично како во претходната задача, да се конструира афина рамнина, чие множество точки е множеството $A = \{a_{ij} \mid i,j = 1,2,3,4\}$.

Решение. Бидејќи бројот на точките е $16 = 4^2$, според 3.11, бројот на правите е $4^2 + 4 = 20$, а секоја права ќе содржи по 4 точки. На начинот како во претходната задача ги добиваме следниве подмножества (прави) од A:

$A_1 = \{a_{11}, a_{12}, a_{13}, a_{14}\}$, $A_2 = \{a_{21}, a_{22}, a_{23}, a_{24}\}$,

$A_3 = \{a_{31}, a_{32}, a_{33}, a_{34}\}$, $A_4 = \{a_{41}, a_{42}, a_{43}, a_{44}\}$,

$A_5 = \{a_{11}, a_{21}, a_{31}, a_{41}\}$, $A_6 = \{a_{12}, a_{22}, a_{32}, a_{42}\}$,

$A_7 = \{a_{13}, a_{23}, a_{33}, a_{43}\}$, $A_8 = \{a_{14}, a_{24}, a_{34}, a_{44}\}$,

$A_9 = \{a_{11}, a_{22}, a_{33}, a_{44}\}$, $A_{10} = \{a_{12}, a_{23}, a_{34}, a_{41}\}$,

$A_{11} = \{a_{13}, a_{24}, a_{31}, a_{42}\}$, $A_{12} = \{a_{14}, a_{21}, a_{32}, a_{43}\}$,

$A_{13} = \{a_{11}, a_{23}, a_{31}, a_{43}\}$, $A_{14} = \{a_{12}, a_{24}, a_{32}, a_{44}\}$,

$A_{15} = \{a_{13}, a_{21}, a_{33}, a_{41}\}$, $A_{16} = \{a_{14}, a_{22}, a_{34}, a_{42}\}$,

$A_{17} = \{a_{11}, a_{24}, a_{33}, a_{42}\}$, $A_{18} = \{a_{12}, a_{21}, a_{34}, a_{43}\}$,

$A_{19} = \{a_{13}, a_{22}, a_{31}, a_{44}\}$, $A_{20} = \{a_{14}, a_{23}, a_{32}, a_{41}\}$.

3.16. Нека релациите α и β во $\mathbb{C}$ се дефинирани со:

$z_1 \alpha z_2 \Leftrightarrow |z_1| \leq |z_2|$,

$z_1 \beta z_2 \Leftrightarrow \arg z_1 = \arg z_2$.

Да се најде $\alpha \cap \alpha^{-1}$, $\alpha \cup \alpha^{-1}$, $\alpha \cap \alpha^{-1} \cap \beta$.

Решение. Нека $z_1 \alpha \cap \alpha^{-1} z_2$; тоа значи дека $z_1 \alpha z_2$ и $z_1 \alpha^{-1} z_2$, т.е. $|z_1| \leq |z_2|$ и $|z_2| \leq |z_1|$, од каде што следува дека $|z_1| = |z_2|$. Значи,

$z_1 \alpha \cap \alpha^{-1} z_2 \Leftrightarrow |z_1| = |z_2|$

Слично добиваме дека $\alpha \cup \alpha^{-1} = \mathbb{C} \times \mathbb{C}$, $\alpha \cap \alpha^{-1} \cap \beta = \Delta_{\mathbb{C}}$.

3.17. Нека $G = \mathbb{R}^n$, а α_{ij} $(i, j = 1, 2, \ldots, n)$ нека се релации во G, дефинирани со:

$(a_1, \ldots, a_n)\ \alpha_{ij}\ (b_1, \ldots, b_n) \Leftrightarrow a_1 + \ldots + a_i = b_1 + \ldots + b_j$.

Да се најдат релациите:

а) $\alpha = \alpha_{11} \cap \alpha_{21} \cap ... \cap \alpha_{n1}$;
б) $\beta = \alpha_{11} \cap \alpha_{22} \cap ... \cap \alpha_{nn}$;
в) $\gamma = \bigcap\limits_{i,j} \alpha_{ij}$

Решение. а) $(a_1, ... ,a_n)\ \alpha\ (b_1, ... , b_n) \Leftrightarrow a_1 = b_1,\ a_2 = ... = a_n = 0.$
б) $\beta = \Delta_C$.
в) $(a_1, ... , a_n)\ \gamma\ (b_1,..., b_n) \Leftrightarrow a_1 = b_1,\ a_2 = ... = a_n = b_2 = ... = b_n = 0.$

3.18. Кои од својствата: рефлексивност, симетричност, антисиметричност и транзитивност ги има релацијата α_i во $\mathbb{N}$, дефинирана со:
а) $m\alpha_1 n \Leftrightarrow m = n^2$;
б) $m\alpha_2 n \Leftrightarrow m$ и n се заемно прости;
в) $m\alpha_3 n \Leftrightarrow m < n$;
г) $m\alpha_4 n \Leftrightarrow |m - n| = 4$.

Одговор. а) Антисиметрична; б) симетрична; в) нерефлексивна и транзитивна; г) симетрична.

3.19. Нека α_i, $i = 1, 2, 3, 4$, се дефинирани како во 3.18. Да се најде:
α_2^2, α_3^2, $\alpha_3\alpha_4$, $\alpha_4\alpha_3$.

Одговор. $\alpha_2^2 = \mathbb{N} \times \mathbb{N}$; $m\alpha_3^2 n \Leftrightarrow n - m > 1$; $m\alpha_3\alpha_4 n \Leftrightarrow m < n + 4$;
$\alpha_4\alpha_3 = \alpha_3\alpha_4$.

3.20. Нека α_1, α_2 и β се релации во множеството A, при што $\alpha_1 \subseteq \alpha_2$. Да се покаже дека
$\beta\alpha_1 \subseteq \beta\alpha_2$, $\alpha_1\beta \subseteq \alpha_2\beta$.

Решение. Да покажеме дека $\beta\alpha_1 \subseteq \beta\alpha_2$, а другото се докажува слично.
Нека $x\beta\alpha_1 y$; тоа значи дека постои некој елемент $z \in A$, таков што $x\beta z$ и $z\alpha_1 y$. Бидејќи $\alpha_1 \subseteq \alpha_2$, од $z\alpha_1 y$ следува $z\alpha_2 y$, кое заедно со $x\beta z$, дава $x\beta\alpha_2 y$. Значи, важи $\beta\alpha_1 \subseteq \beta\alpha_2$.

3.21. Ако α е релација во A, тогаш: $\alpha^2 \cap \alpha = \varnothing$ ако и само ако од $a\alpha b$ и $b\alpha c$ следува $a\alpha' c$.

3.22. Нека α е релација во множеството A и нека
$a^\alpha = \{x \mid x \in A, x\alpha a\}$.
Ако $A = \bigcup\limits_{a \in A} a^\alpha$ да се покаже дека релацијата $\alpha\alpha^{-1}$ е рефлексивна.

Решение. Нека x е произволен елемент од A; тогаш имаме:

$$x\in A \Leftrightarrow x\in \bigcup_{a\in A} a^{\alpha} \Rightarrow (\exists a\in A)\, x\in a^{\alpha} \Rightarrow$$

$$\Rightarrow (\exists a\in A)\, x\alpha a \Rightarrow (\exists a\in A)\, a\alpha^{-1}x$$

Понатаму, од $x\alpha a$ и $a\alpha^{-1}x$, следува $x\alpha\alpha^{-1}x$, за секој $x\in A$, т.е. релацијата $\alpha\alpha^{-1}$е рефлексивна.

3.23. Релацијата α е симетрична ако и само ако $\alpha^{-1} = \alpha$, а антисиметрична ако и само ако $\alpha^{-1} \cap \alpha = \Delta_A$.

Решение. Ако релацијата α е симетрична, тогаш јасно е дека $\alpha^{-1} = \alpha$.

Обратно, нека $\alpha^{-1} = \alpha$. Од $\alpha^{-1} = \alpha$ и $x\alpha y$ следува дека $x\alpha^{-1}y$ т.е $y\alpha x$ што значи релацијата α е симетрична.

Слично и другото тврдење.

3.24. Ако α е релација во множеството A, тогаш релацијата $\alpha\alpha^{-1}$ е симетрична.

Решение. Бидејќи $(\alpha\alpha^{-1})^{-1} = (\alpha^{-1})^{-1}\alpha^{-1} = \alpha\alpha^{-1}$, според претходната задача, следува дека релацијата $\alpha\alpha^{-1}$ е симетрична.

3.25. Ако α е релација во множеството A, тогаш α е транзитивна ако и само ако $\alpha^2 \subseteq \alpha$.

Решение. Нека релацијата α е транзитивна. Ако $x\alpha^2 y$, следува дека постои елемент $z\in A$, таков што $x\alpha z$ и $z\alpha y$, а од транзитивноста на α, следува дека и $x\alpha y$. Значи, имаме $\alpha^2 \subseteq \alpha$.

Обратно, нека $\alpha^2 \subseteq \alpha$. Ако $x\alpha z$ и $z\alpha y$, тогаш следува дека $x\alpha^2 y$, а од $\alpha^2 \subseteq \alpha$, следува дека и $x\alpha y$ т.е. релацијата α е транзитивна.

3.26. Нека α и β се релации во A. Ако α, β се рефлексивни, или симетрични, или транзитвни, дали и $\alpha\beta$ го има соодветното својство?

Решение. Нека релациите α и β се рефлексивни. Тогаш $\Delta_A \subseteq \alpha$ и $\Delta_A \subseteq \beta$. Од $\Delta_A \subseteq \alpha$, според 3.20. имаме $\Delta_A\beta \subseteq \alpha\beta$, и $\Delta_A \subseteq \beta = \Delta_A\beta \subseteq \alpha\beta$, а тоа значи дека и $\alpha\beta$ е рефлексивна.

Производ од симетрични (транзитивни) релации не мора да биде симетрична (транзитивна) релација. На пример, ако:

$A = \{a, b, c, d, e\}$, $\alpha = \{(b, c), (c, b)\}$, $\beta = \{(a, b), (b, a)\}$,

$\gamma = \{(e, c), (d, a)\}$ $\delta = \{(b, e), (c, d)\}$, тогаш $\alpha\beta = \{(a, c)\}$ и

$\gamma\delta = \{(b, c), (c, a)\}$. Релациите α и β се симетрични, но $\alpha\beta$ не е симетрична. Релациите γ и δ се транзитивни, но $\gamma\delta$ не е транзитивна.

3.27. Ако α,β се релации во A, тогаш $\alpha \subseteq \beta \Leftrightarrow \alpha^{-1} \subseteq \beta^{-1}$.

Решение. Нека $\alpha \subseteq \beta$; тоа значи дека од $h\alpha u$ следува $h\beta u$, а тоа е еквивалентно со:

$u\alpha^{-1}h \Rightarrow u\beta^{-1}h$,

т.е. $\alpha^{-1} \subseteq \beta^{-1}$.

Бидејќи $(\alpha^{-1})^{-1} = \alpha$, според претходното имаме:

$\alpha^{-1} \subseteq \beta^{-1} \Rightarrow (\alpha^{-1})^{-1} \subseteq (\beta^{-1})^{-1} \Rightarrow \alpha \subseteq \beta$.

3.28. Ако α и β се симетрични релации во A и $\alpha\beta \subseteq \beta\alpha$, тогаш и релацијата $\alpha\beta$ е симетрична, при што важи $\alpha\beta = \beta\alpha$.

Решение. Имаме

$$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = \beta\alpha \supseteq \alpha\beta. \qquad (1)$$

Од друга страна

$\alpha\beta = \alpha^{-1}\beta^{-1} = (\beta\alpha)^{-1}$,

а според претходната задача,

$$\alpha\beta = (\beta\alpha)^{-1} \supseteq (\alpha\beta)^{-1}. \qquad (2)$$

Од (1) и (2) следува $(\alpha\beta)^{-1} = \alpha\beta$, што значи, според 3.23, релацијата $\alpha\beta$ е симетрична. Потоа, имаме:

$\alpha\beta = (\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1} = \beta\alpha$.

3.29. Релацијата α во A е подредување ако и само ако се исполнети следниве услови:

$$\alpha \cap \alpha^{-1} = \Delta_A, \qquad \alpha^2 \subseteq \alpha .$$

Решение. Релацијата α е подредување ако таа е рефлексивна, антисиметрична и транзитивна. Од $\alpha \cap \alpha^{-1} = \Delta_A$, следува $\Delta_A \subseteq \alpha$, што претставува потребен и доволен услов релацијата α да е рефлексивна.

Нека $x\alpha y$ и $y\alpha x$. Тоа значи дека $x\alpha^{-1}y$, т.е. $x\ \alpha \cap \alpha^{-1}\ y$, а поради $\alpha \cap \alpha^{-1} = \Delta_A$, имаме $x\ \Delta_A\ y$, т.е. $x = y$. Значи, релацијата α е антисиметрична. Обратно ако релацијата α е антисиметрична, тогаш јасно е дека $\alpha \cap \alpha^{-1} = \Delta_A$

Условот $\alpha^2 \subseteq \alpha$ е потребен и доволен за релацијата α да е транзитивна (3.25.)

3.30. Пресек на произволна фамилија подредувања на множеството A е подредување на A. Дали унија на подредувања е подредување?

Решение. Нека $\{\alpha_i \mid i \in I\}$ е произволна фамилија подредувања на множеството A. Да ставиме

$\alpha = \bigcap_i \alpha_i$

Од тоа што α_i се рефлексивни, следува дека и α_i^{-1} се рефлексивни па $\Delta_A \subseteq \alpha_i$ и $\Delta_A \subseteq \alpha_i^{-1}$ за секој $i \in I$, т.е.

$\Delta_A \subseteq \bigcap_i \alpha_i = \alpha$ и $\Delta_A \subseteq \bigcap_i \alpha_i^{-1} = \alpha^{-1}$, што значи

$\Delta_A \subseteq \alpha \cap \alpha^{-1}$. (1)

Од антисиметричноста на α_i, следува дека $\alpha_i \cap \alpha_i^{-1} = \Delta_A$ за секој $i \in I$, па

$$\alpha \cap \alpha^{-1} = (\bigcap_i \alpha_i) \cap (\bigcap_i \alpha_i)^{-1} = (\bigcap_i \alpha_i) \cap (\bigcap_i \alpha_i^{-1}) =$$

$$= \bigcap_{i,j} (\alpha_i \bigcap \alpha_j^{-1}) \subseteq \bigcap_i (\alpha_i \cap \alpha_i^{-1})) = \Delta_A$$

т.е. $\Delta_A \supseteq \alpha \cap \alpha^{-1}$. (2)

Од (1) и (2) имаме $\Delta_A = \alpha \cap \alpha^{-1}$, т.е. релацијата α е рефлексивна и антисиметрична.

Од транзитивноста на α_i следува дека $\alpha_i^2 \subseteq \alpha_i$ за секој $i \in I$, па имаме

$$\alpha^2 = (\bigcap_i \alpha_i)^2 = (\bigcap_i \alpha_i)(\bigcap_j \alpha_j) \subseteq$$

$$\bigcap_j ((\bigcap_i \alpha_i)\alpha_j) \subseteq \bigcap_{i,j} (\alpha_i \alpha_j) \subseteq \bigcap_i \alpha_i^2 \subseteq \bigcap_i \alpha_i = \alpha$$

што значи дека релацијата α е транзитивна.

Од сето тоа следува дека релацијата α е подредување, т.е. пресек на произволна фамилија подредувања е подредување.

Унијата на подредувања не мора да е подредување. Имено, унија на рефлексивни релации е рефлексивна, но унија на антисиметрични односно транзитивни релации не мора да биде антисиметрична односно транзитивна. На пример, ако $A = \{1, 2, 3, 4\}$, тогаш релациите

$\alpha_1 = \{(2, 3), (3, 1), (2, 1)\}$ и $\alpha_2 = \{(1, 1), (1, 2), (2, 3), (1, 3)\}$

се антисиметрични и транзитивни, но релацијата $\alpha_1 \cup \alpha_2$ не е ни антисиметрична, ни транзитивна.

3.31. Нека Π_1 и Π_2 се поделби на X. Π_1 е *пофина* од Π_2 ако и само ако $A \in \Pi_1$ имплицира $A \subseteq B$ за некој $B \in \Pi_2$. Да се покаже дека релацијата "е пофина" е подредување во множеството од сите поделби на X.

Решение. Нека $\mathbb{P}$ е множество од сите поделби на X, а α нека е релација дефинирана со:

$(\forall \Pi_1, \Pi_2 \in \mathbb{P})$ $\Pi_1 \alpha \Pi_2 \Leftrightarrow \Pi_1$ е пофина од Π_2.

Ако $\Pi \in \mathbb{P}$ тогаш за секое $A \in \Pi$ имаме $A \subseteq A$, т.е. $\Pi \alpha \Pi$, што значи α е рефлексивна.

Нека $\Pi_1 \alpha \Pi_2$, $\Pi_2 \alpha \Pi_1$ и A е произволен елемент од Π_1. Од $\Pi_1 \alpha \Pi_2$ следува дека постои елемент $B \in \Pi_2$, така што $A \subseteq B$. Од $\Pi_2 \alpha \Pi_1$, за B постои некое $A_1 \in \Pi_1$, така што $B \subseteq A_1$. Бидејќи Π_1 е поделба на X следува дека $A \cap A_1 = \emptyset$ или $A = A_1$. Но од $A \subseteq B \subseteq A_1$ следува дека $A \cap A_1 = A \neq \emptyset$, па значи $A = A_1 = B$. Значи, за секое $A \in \Pi_1$ постои $B \in \Pi_2$, така што $A = B$, т.е. $\Pi_1 = \Pi_2$, а тоа значи дека α е антисиметрична.

Од транзитивноста на релацијата "$\subseteq$" кај множествата следува дека и релацијата α е транзитивна.

Од сето тоа следува дека α е подредување.

3.32. Ако α е подредување на множеството A, тогаш релацијата

$$\beta = \alpha \cap \Delta'_A \tag{1}$$

е стриктно подредување на A и притоа важи

$$\alpha = \beta \cup \Delta_A \tag{2}$$

Ако пак β е стриктно подредување на A, тогаш релацијата α дефинирана со (2) е подредување на A и притоа важи (1).

3.33. Да го означиме со $\mathbb{Q}[x]$ множеството од сите полиноми со рационални коефициенти. Да дефинираме релација на $A = \mathbb{Q}[x] \setminus \mathbb{Q}$ на следниов начин: за секој пар $f, g \in A$, $f \alpha g$ ако и само ако $g = qf$ за некој $q \in A$. Да се покаже дека α е стриктно подредување на A. Дали $\alpha \cup \Delta_A$ е потполно подредување на A?

Решение. Лесно се проверува дека α е нерефлексивна и транзитивна, т.е. дека α е стриктно подредување. Исто така лесно се покажува дека $\alpha \cup \Delta_A$ е подредување, но не и потполно, зашто, на пример полиномите $f(x) = x - 1$ и $g(x) = x + 1$ не се во релација $\alpha \cup \Delta_A$.

3.34. Нека α е стриктно подредување на A, а β стриктно подредување на B. На $A \times B$ дефинираме релација γ на следниот начин:

$(a_1, b_1)\, \gamma\, (a_2, b_2) \Leftrightarrow b_1\, \beta\, b_2$ или $(a_1\, \alpha\, a_2$ и $b_1 = b_2)$.

Да се покаже дека γ е стриктно подредување на $A \times B$.

3.35. Да се покаже дека Δ_A е единствената релација на A, којашто е еквивалентност и подредување.

Решение. Нека α е релација во множеството A, којашто е еквивалентност и подредување. Тоа значи дека α е рефлексивна,

симетрична, антисиметрична и транзитивна. Од симетричноста на α следува дека $\alpha = \alpha^{-1}$, а од рефлексивноста и антисиметричноста следува дека $\alpha \cap \alpha^{-1} = \Delta_A$. Значи, имаме:

$$\alpha = \alpha \cap \alpha = \alpha \cap \alpha^{-1} = \Delta_A.$$

3.36. Да се покаже дека една релација α во множеството A е еквивалентност ако и само ако се исполнети условите:

(i) $\alpha = \alpha^{-1}$;

(ii) $(\forall a \in A)\ (\exists b \in B)\ a\alpha b$;

(iii) $a\alpha b \wedge c\alpha b \Rightarrow a\alpha c$.

Решение. Ако α е еквивалентност, јасно е дека условите (i) – (iii) се исполнети.

Обратно, за релацијата α нека се исполнети условите (i) – (iii). Од $\alpha = \alpha^{-1}$ следува дека α е симетрична. Нека a е произволен елемент од A; од (ii) следува дека постои барем еден елемент $b \in A$, така што $a\alpha b$, а според (iii), од $a\alpha b$ и $a\alpha b$ следува $a\alpha a$, т.е. α е рефлексивна. Потоа нека $a\alpha b$ и $b\alpha c$. Поради симетричноста на α, имаме $a\alpha b$ и $c\alpha b$, а според (iii) добиваме и $a\alpha c$, т.е. α е транзитивна.

3.37. Релацијата α во A е еквивалентност ако и само ако:

(i) $\Delta_A \subseteq \alpha$;

(ii) $\alpha = \alpha^{-1}$;

(iii) $\alpha\,\alpha \subseteq \alpha$.

Упатство. Види 3.23. и 3.25.

3.38. Релацијата α е еквивалентност на A ако и само ако

$$\Delta_A \subseteq \alpha, \quad \alpha\alpha^{-1} \subseteq \alpha. \tag{1}$$

Решение. Ако α е еквивалентност, тогаш $\Delta_A \subseteq \alpha$, $\alpha^{-1} = \alpha$, $\alpha\alpha \subseteq \alpha$, па добиваме $\alpha\alpha^{-1} = \alpha\alpha \subseteq \alpha$.

Обратно, нека релацијата α ги исполнува условите (1). За да покажеме дека α е еквивалентност, доволно е да покажеме дека α е симетрична, т.е. $\alpha^{-1} = \alpha$. Имаме:

$$\alpha^{-1} = \Delta_A\,\alpha^{-1} \subseteq \alpha\alpha^{-1} \subseteq \alpha.$$

Од друга страна $\alpha = (\alpha^{-1})^{-1} \subseteq \alpha^{-1}$, што значи дека $\alpha^{-1} = \alpha$.

3.39. Пресек на произволна фамилија еквивалентности е еквивалентност. Дали унија на еквивалентности е еквивалентност?

Решение. Нека $\{\alpha_i \mid i \in I\}$ е произволна фамилија еквивалентности на A. Од тоа што α_i е еквивалентност на A следува дека

$\Delta_A \subseteq \alpha_i$, $\alpha_i^{-1} = \alpha_i$, $\alpha_i^2 \subseteq \alpha_i$

за секој $i \in I$. Од $\Delta_A \subseteq \alpha_i$ за секој $i \in I$ следува дека $\Delta_A \subseteq \bigcap_i \alpha_i = \alpha$, т.е. α е рефлексивна. Од $\alpha^{-1} = (\bigcap_i \alpha_i)^{-1} = \bigcap_i \alpha_i = \alpha$ следува дека α е симетрична, а поради:

$$\alpha^2 = \alpha\alpha = (\bigcap_i \alpha_i)(\bigcap_i \alpha_i) \subseteq \bigcap_{i,j} \alpha_i\alpha_j \subseteq \bigcap_i \alpha_i\alpha_i \subseteq \bigcap \alpha_i = \alpha$$

добиваме дека α е и транзитивна. Значи, α е еквивалентност.

Во 3.30 видовме дека унија на транзитивни релации не мора да е транзитивна, па според тоа и унија на еквивалентности не мора да е еквивалентност.

3.40. Нека $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ и $S = \mathbb{Z} \times \mathbb{Z}^*$. Да се покаже дека релацијата

$$\alpha = \{((x, y), (u, v)) \mid xv = yu\}$$

е еквивалентност во S.

3.41. Нека $S = \mathbb{N}^2$. Покажи дека релацијата

$$\alpha = \{((x, y), (u, v)) \mid x + v = y + u\}$$

е еквивалентност во S. Да се најде $(4, 7)^\alpha$.

Одговор. $(4,7)^\alpha = \{(x, y) \mid y - x = 3\}$.

3.42. Нека α е еквивалентност во A, β еквивалентност во B и нека релацијата γ во $A \times B$ е дефинирана со:

$(a_1, b_1)\ \gamma\ (a_2, b_2) \Leftrightarrow a_1\ \alpha\ a_2,\ b_1\ \beta\ b_2$.

Да се покаже дека γ е еквивалентност.

3.43. Производот $\alpha\beta$ на еквивалентностите α, β ги содржи α и β и се содржи во секоја еквивалентност γ што ги содржи α и β.

Решение. Бидејќи α и β се еквивалентности, имаме

$\Delta_A \subseteq \alpha$, $\Delta_A \subseteq \beta$,

па според 3.20, множејќи ја првата инклузија со β оддесно, а втората со α одлево, добиваме

$\beta \subseteq \alpha\beta$, $\alpha \subseteq \alpha\beta$.

Нека γ е произволна еквивалентност што ги содржи α и β. Бидејќи $\beta \subseteq \gamma$ следува дека и $\gamma\beta \subseteq \gamma$, па според тоа добиваме

$\alpha \subseteq \gamma \Rightarrow \alpha\beta \subseteq \gamma\beta \subseteq \gamma$.

3.44. Ако α и β се еквивалентности во A, тогаш $\alpha\beta$ е еквивалентност во A, ако и само ако е $\alpha\beta = \beta\alpha$.

3.45. Ако α и β се еквивалентности, тогаш $\alpha \cup \beta$ е еквивалентност ако и само ако $a^{\alpha} \cap b^{\beta} = \emptyset$ или $a^{\alpha} \subseteq b^{\beta}$ или $b^{\beta} \subseteq a^{\alpha}$. Ако $\alpha \cup \beta$ е еквивалентност, тогаш $\alpha \cup \beta = \alpha\beta$.

Решение. Да претпоставиме дека за еквивалентностите α, β постојат класи x^{α} и y^{β}, такви што $a \in x^{\alpha} \cap y^{\beta}$, $x^{\alpha} \not\subseteq y^{\beta}$, $y^{\beta} \not\subseteq x^{\alpha}$. Во овој случај постојат елементи b и c такви што $b\alpha a$, $b\beta' a$, $c\beta a$, $c\alpha' a$. Од $b\alpha a$ и $c\beta a$ следува дека и $b(\alpha \cup \beta)a$, $a(\alpha \cup \beta)c$. Ако би било $b(\alpha \cup \beta)c$, тогаш би имале $b\alpha c$ или $b\beta c$. Ако $b\alpha c$, бидејќи $b\alpha a$, добиваме $c\alpha a$, спротивно на $c\alpha' a$; ако пак $b\beta c$, тогаш поради $c\alpha a$, добиваме дека $b\beta a$, спротивно на $b\beta' a$. Значи, $b(\alpha \cup \beta)' c$, т.е. релацијата $\alpha \cup \beta$ не е транзитивна, па според тоа не е еквивалентност. Значи ако $\alpha \cup \beta$ е еквивалентност тогаш е исполнет еден од условите

$$a^{\alpha} \cap b^{\beta} = \emptyset, \quad a^{\alpha} \subseteq b^{\beta}, \quad b^{\beta} \subseteq a^{\alpha}. \tag{1}$$

Нека сега α и β се еквивалентности, но $\alpha \cup \beta$ не е еквивалентност. Тоа значи дека $\alpha \cup \beta$ не е транзитивна, т.е. постојат елементи $a, b, c \in A$ за кои

$$b(\alpha \cup \beta)a, \quad a(\alpha \cup \beta)c, \quad b(\alpha \cup \beta)' c.$$

Но, тогаш класите a^{α} и b^{β} имаат непразен пресек и ни едната не е подмножество од другата. Значи, ако е исполнет еден од условите (1), тогаш $\alpha \cup \beta$ е еквивалентност.

3.46. Нека X е множество и $J \subseteq \mathbb{P}(X)$, $J \neq \emptyset$, што ги задоволува следниве услови

(i) $(Y \subseteq Z) \wedge Z \in J \Rightarrow Y \in J$;

(ii) $Y, Z \in J \Rightarrow Y \cup Z \in J$.

Ако J е фиксирано во $\mathbb{P}(X)$, дефинираме релација α со:

$A \alpha B \Leftrightarrow A \Delta B \in J$.

Да се покаже дека:

а) α е еквивалентност во $\mathbb{P}(X)$;

б) од $A\alpha B$ следува $A \cup C \,\alpha\, B \cup C$, $A \cap C \,\alpha\, B \cap C$, $A \setminus C \,\alpha\, B \setminus C$ и $C \setminus A \,\alpha\, C \setminus B$, каде што C е произволно подмножество од X.

Решение. а) Јасно е дека од $J \neq \emptyset$ и (i) следува $\emptyset \in J$. Бидејќи $A \Delta A = \emptyset \in J$, за секој $A \in \mathbb{P}(X)$, следува дека $A\alpha A$, т.е. α е рефлексивна. Од комутативноста на Δ следува симетричноста на α, а од $A\alpha B$ и $B\alpha C$ користејќи ја инклузијата

$$A \Delta C \subseteq (A \Delta B) \cup (B \Delta C),$$

добиваме и $A\alpha C$, т.е. дека α е и транзитивна. Значи, α е еквивалентност.

б) Ако $A \alpha B$, да покажеме, на пример, дека $A \cup C \; \alpha \; B \cup C$. Поради $(A \cup C) \Delta (B \cup C) \subseteq A \Delta B$, според (i), следува дека $(A \cup C) \Delta (B \cup C) \in J$ т.е. $A \cup C \; \alpha \; B \cup C$.

3.47. Секоја рефлексивна и транзитивна релација се вика *претподредување*. Ако α е претподредување во A, да се покаже дека:

а) релацијата $\beta = \alpha \cap \alpha^{-1}$ е еквивалентност;

б) релацијата $\overline{\alpha}$ во A/β, дефинирана со

$a^\beta \overline{\alpha} \, b^\beta \Leftrightarrow (\exists \, a_1 \in a^\beta, b_1 \in b^\beta) \, a_1 \alpha b_1$,

е подредување.

Решение. а) Бидејќи α е рефлексивна и транзитивна, следува дека и β е таква, а бидејќи

$\beta^{-1} = (\alpha \cap \alpha^{-1})^{-1} = \alpha^{-1} \cap (\alpha^{-1})^{-1} = \alpha^{-1} \cap \alpha = \alpha \cap \alpha^{-1} = \beta$,

следува дека β е и симетрична. Значи, релацијата β е еквивалентност.

б) Од рефлексивноста и транзитивноста на α, следува дека и $\overline{\alpha}$ е таква. Да покажеме дека $\overline{\alpha}$ е антисиметрична.

Нека $a^\beta \overline{\alpha} \, b^\beta$ и $b^\beta \overline{\alpha} \, a^\beta$; тоа значи дека постојат $a_1, a_2 \in a^\beta$ и $b_1, b_2 \in b^\beta$, такви што $a_1 \alpha b_1$ и $b_2 \alpha a_2$ т.е. $a_1 \alpha b_1$ и $a_2 \alpha^{-1} b_2$.

Бидејќи $b_1, b_2 \in b^\beta$, $a_1, a_2 \in a^\beta$, следува дека $b_1 \beta b_2$ и $a_1 \beta a_2$, а според тоа имаме и $b_1 \alpha b_2$ и $a_2 \alpha a_1$. Од $a_1 \alpha b_1$ и $b_1 \alpha b_2$ добиваме $a_1 \alpha b_2$, а од $a_1 \alpha^{-1} a_2$ и $a_2 \alpha^{-1} b_2$ добиваме и $a_1 \alpha^{-1} b_2$. Значи, имаме $a_1 \beta b_2$, т.е. $a_1^\beta = b_2^\beta$, па и $a^\beta = a_1^\beta = b_2^\beta = b^\beta$.

Од сето тоа следува дека $\overline{\alpha}$ е подредување.

3.48. Во множеството $\mathbb{Z}$ на целите броеви е определена релација α со:

$a \alpha b \Leftrightarrow (\exists \; c \in \mathbb{Z}) \; b = ac$.

а) Да се покаже дека α е претподредување.

б) Да се најде еквивалентноста $\beta = \alpha \cap \alpha^{-1}$, фактор–множеството $\mathbb{Z}/\beta$, и подредувањето $\overline{\alpha}$ во $\mathbb{Z}/\beta$ во смисла на претходната задача.

Одговор. б) $m \beta n \Leftrightarrow m = n$ или $m = -n$, $m, n \in \mathbb{Z}$;

$\mathbb{Z}/\beta = \{A_n \mid A_n = \{n, -n\}, n \in \mathbb{N}^0\}$;

$m^\beta \overline{\alpha} \, n^\beta \Leftrightarrow (\exists k \in \mathbb{Z}) \; n = km$.

3.49. Да се покаже дека множеството X е бесконечно ако и само ако постојат бесконечно многу еквивалентности во X.

Решение. Ако множеството X е конечно, на пример, со n елементи, тогаш бројот на еквивалентности во X е најмногу 2^{n^2}, па според

тоа, ако во множеството X постојат бесконечно многу еквивалентности, тогаш и множеството X е бесконечно.

Обратно, нека множеството X е бесконечно. За секој пар елементи $a, b \in X$, $a \neq b$, во X ја дефинираме релацијата $\alpha_{a,b}$ на следниов начин:

$x\alpha_{a,b}y \Leftrightarrow x = y \vee (x, y) = (a, b) \vee (x, y) = (b, a)$.

Лесно се покажува дека релацијата $\alpha_{a,b}$ е еквивалентност, а бидејќи

$\alpha_{a,b} = \alpha_{c,d} \Leftrightarrow (a, b) = (c, d)$,

заклучуваме дека во X постојат бесконечно многу еквивалентности.

3.50. Нека $f : A \to B$ е пресликување и нека во A дефинираме релација α со:

$a_1 \alpha a_2 \Leftrightarrow f(a_1) = f(a_2)$.

Да се покаже дека α е еквивалентност во A. (Релацијата α се вика *јадро на пресликувањето* f и се означува со $\ker f$.)

Решение. Бидејќи $f(a) = f(a)$ за секој $a \in A$, имаме $a \alpha a$, т.е. α е рефлексивна.

Нека $a_1 \alpha a_2$; тоа значи дека $f(a_1) = f(a_2)$, па тогаш и $f(a_2) = f(a_1)$, т.е. $a_2 \alpha a_1$. Значи, α е симетрична.

Нека $a_1 \alpha a_2$ и $a_2 \alpha a_3$; тогаш $f(a_1) = f(a_2) = f(a_3)$, т.е. $a_1 \alpha a_3$ па α е транзитивна.

Според тоа, α е еквивалентност.

3.51. Ако $f : A \to B$ е пресликување, тогаш $\ker f = f^{-1} f$.

3.52. Нека $f : A \to B$, $g : B \to C$ се пресликувања. Каков е односот меѓу релациите $\ker f$ и $\ker gf$?

Одговор. $\ker f \subseteq \ker gf$.

3.53. Нека $f : A \to B$ е пресликување и α еквивалентност во A, така што $\alpha \subseteq \ker f$. Да се покаже дека постои едно и само едно пресликување $f^* : A/_\alpha \to B$ за кое важи $f = f^* \text{nat}\, \alpha$.

Решение. Нека $f^* : A/_\alpha \to B$ е дефинирано со:

$$(\forall a^\alpha \in A/_\alpha)\ f^*(a^\alpha) = f(a). \qquad (1)$$

Ако $a^\alpha = a_1^\alpha$, тогаш од $\alpha \subseteq \ker f$, имаме

$f(a) = f(a_1)$, т.е. $f^*(a^\alpha) = f^*(a_1^\alpha)$. Значи, со (1) е дефинирано пресликување $f^* : A/_\alpha \to B$. Потоа имаме:

$(\forall a \in A)\ (f^* \text{nat} \alpha)\ (a) = f^*(\text{nat}\ \alpha(a)) = f^*(a^{\alpha}) = f(a)$,

т.е. $f^* \text{nat}\ \alpha = f$.

Ако $g : A/_{\alpha} \to B$ е друго пресликување, со особината $g\ \text{nat}\ \alpha = f$ ќе имаме:

$$f^*(a^{\alpha}) = f(a) = (g\ \text{nat}\ \alpha)(a) = g(\text{nat}\ \alpha(a)) = g(a^{\alpha}),$$

т.е. $f^* = g$.

Значи, пресликувањето $f : A/_{\alpha} \to B$, дефинирано со (1), е единствено што го задоволува условот $f^* \text{nat}\ \alpha = f$.

3.54. Нека α, β се еквивалентности во A, такви што $\alpha \subseteq \beta$. Да се покаже дека постои едно и само едно пресликување $f : A/_{\alpha} \to A/_{\beta}$, така што $f\ \text{nat}\ \alpha = \text{nat}\ \beta$.

Решение. Од $\alpha \subseteq \beta$, следува дека $a^{\alpha} \subseteq a^{\beta}$ за секој $a \in A$, па $f : A/_{\alpha} \to A/_{\beta}$ дефинирано со $f(a^{\alpha}) = a^{\beta}$ е пресликување и притоа имаме:

$(\forall a \in A)\ (f\ \text{nat}\ \alpha)(a) = f(\text{nat}\ \alpha(a)) = f(a^{\alpha}) = a^{\beta} = \text{nat}\ \beta(a)$,

т.е. $f\ \text{nat}\ \alpha = \text{nat}\ \beta$.

Ако $g : A/_{\alpha} \to A/_{\beta}$ е друго пресликување со особината $g\ \text{nat}\ \alpha = \text{nat}\ \beta$, тогаш имаме:

$(\forall a \in A)\ f(a^{\alpha}) = \text{nat}\ \beta(a) = g(\text{nat}\ \alpha(a)) = g(a^{\alpha})$,

т.е. $f = g$.

3.55. Да се покаже дека транзитивното проширување на секоја рефлексивна релација е претподредување.

3.56. Нека $A = \{1, 2, \ldots, 9\}$ и нека релацијата α е определена со:

$\alpha = \Delta_A \cup \{(1, 3), (3, 1), (1, 5), (5, 3), (1, 7), (7, 1), (1, 9), (2, 4), (4, 2)\}$

Да се најдат:

а) транзитивното проширување α^*;

б) еквивалентноста $\beta = \alpha^* \cap (\alpha^*)^{-1}$;

в) фактор–множеството $A/_{\beta}$ и соодветното подредување $\overline{\alpha}^*$.

Одговор. а) $\alpha^* = \alpha \cup \{(3, 5), (3, 7), (3, 9), (5, 1), (7, 3), (7, 5), (7, 9), (5, 7), (5, 9)\}$.

б) $(\alpha^*)^{-1} = \alpha^{-1} \cup \{(5, 3), (7, 3), (9, 3), (1, 5), (3, 7), (5, 7), (9, 7), (7, 5), (9,5)\}$;

$\beta = \alpha^* \cap (\alpha^*)^{-1} = \Delta_A \cup \{(1, 3), (3, 1), (1, 7), (7, 1), (2, 4), (4, 2), (7, 3), (3, 7), (5, 7), (7, 5), (5, 3), (1,5), (5, 1), (3, 5)\}$.

в) $A/_{\beta} = \{\{1, 3, 5, 7\}, \{2, 4\}, \{6\}, \{8\}, \{9\}\}$.

$\overline{\alpha}^* = \Delta_{A/\beta} \cup \{(\{1, 3, 5, 7\}, \{9\})\}$.

3.57. Да се најде транзитивното проширување на релацијата $(\alpha \cap \alpha^{-1}) \cup \beta$, при што $\alpha,\beta \subseteq \mathbb{C} \times \mathbb{C}$ се дефинирани со:
$z_1 \alpha z_2 \Leftrightarrow |z_1| \leq |z_2|$, $z_1 \beta z_2 \Leftrightarrow \arg z_1 = \arg z_2$.

Одговор.. $\mathbb{C} \times \mathbb{C}$.

3.58. Да се покаже дека транзитивното проширување на:
а) рефлексивна релација е рефлексивна.
б) симетрична релација е симетрична.

Решение. а) Нека α е рефлексивна релација и α^* нејзиното транзитивно проширување. Тогаш имаме $\alpha \subseteq \alpha^*$ и $\Delta_A \subseteq \alpha$, па $\Delta_A \subseteq \alpha^*$, што значи дека α^* е рефлексивна.

б) Нека α е симетрична и $a\alpha^* b$. Тогаш имаме:

$$a\alpha^* b \Rightarrow (\exists a_1, \ldots, a_k \in A)\ a\alpha a_1, a_1\alpha a_2, \ldots, a_k \alpha b \Rightarrow$$
$$\Rightarrow (\exists a_1, \ldots, a_k \in A)\ b\alpha a_k, \ldots, a_1 \alpha a \Rightarrow b\alpha^* a,$$

т.е. α^* е симетрична.

3.59. Да се покаже дека транзитивното проширување на рефлексивна и симетрична релација е еквивалентност.

3.60. Ако α, β се релации во A, такви што $\alpha \subseteq \beta$, тогаш и $\alpha^* \subseteq \beta^*$.

3.61. Нека α е произволна релација во A и нека

$$\alpha^* = \bigcup_1^\infty \alpha^n,\ \alpha^n = \underbrace{\alpha\alpha\ldots\alpha}_{n}$$

Да се покаже дека α^* е транзитивното проширување на α.

Решение. Нека τ е транзитивното проширување на α. Да покажеме дека $\alpha^* \subseteq \tau$ и $\tau \subseteq \alpha^*$.

Имаме:

$a\alpha^* b \Rightarrow a\alpha^n b \Rightarrow (\exists a_1, \ldots, a_n \in A)\ a\alpha a_1,\ a_1\alpha a_2, \ldots, a_n \alpha b \Rightarrow a\tau b$,

т.е. $\alpha^* \subseteq \tau$;

$a\tau b \Rightarrow (\exists u_1, \ldots, u_k \in A)\ a\alpha u_1, u_1\alpha u_2, \ldots, u_k \alpha b \Rightarrow a\alpha^k b \Rightarrow a\alpha^* b$,

т.е. $\tau \subseteq \alpha^*$.

Значи имаме $\alpha^* = \tau$.

3.62. За произволна релација α во A да ставиме $\beta = \alpha \cup \alpha^{-1} \cup \Delta_A$.
Ако β^* е транзитивното проширување на β, тогаш:
а) $\alpha \subseteq \beta^*$

б) β^* е еквивалентност во A;

в) Ако γ е еквивалентност во A што ја содржи α, тогаш $\beta^* \subseteq \gamma$.

(Со други зборови, γ е минималната еквивалентност во A, што ја содржи α.)

Решение. а) Бидејќи $\beta = \alpha \cup \alpha^{-1} \cup \Delta_A$, следува дека $\alpha \subseteq \beta$, а бидејќи β^* е транзитивното проширување на β, имаме $\beta \subseteq \beta^*$. Значи $\alpha \subseteq \beta^*$.

б) Од $\Delta_A \subseteq \beta$ и $\beta^{-1} = (\alpha \cup \alpha^{-1} \cup \Delta_A)^{-1} = \alpha^{-1} \cup \alpha \cup \Delta_A = \beta$, следува дека β е рефлексивна и симетрична, па бидејќи транзитивното проширување на рефлексивна и симетрична релација е рефлексивна, симетрична и транзитивна, следува дека β^* е еквивалентност.

в) Нека γ е еквивалентност во A што ја содржи α. Од $\alpha \subseteq \gamma$ следува $\alpha^{-1} \subseteq \gamma$, па и $\beta = \alpha \cup \alpha^{-1} \cup \Delta_A \subseteq \gamma$.

Од $\beta \subseteq \gamma$ следува и $\beta^* \subseteq \gamma^* = \gamma$.

3.63. Нека $A = \{1, 2, \ldots, 18\}$,

$\alpha = \{(1, 5), (5, 9), (9, 13), (13,17), (2, 6), (6, 10), (10, 14),$
$(14, 18), (3, 7), (7, 11), (11, 15), (4, 8), (8, 12), (12, 16)\}$,

$\beta = \{(1, 7), (7, 13), (2, 8), (8, 14), (3, 9), (9, 15), (4, 10),$
$(10, 16), (5, 11), (11, 17), (6, 12), ((12,1\ 8)\}$,

$\gamma = \{(1, 13), (2, 14), (3, 15), (4, 16), (5, 17), (6, 18)\}$.

Да се најдат:

а) транзитивните проширувања $\alpha^*, \beta^*, \gamma^*$ на α, β, γ

б) минималните еквивалентности $\alpha_1, \beta_1, \gamma_1$ што ги содржат α, β, γ.

в) фактор–множествата $A/_{\alpha 1}, A/_{\beta 1}, A/_{\gamma 1}$;

г) пресликувањата nat α_1, nat β_1, nat γ_1;

д) транзитивниот производ на α и β.

Решение. Можеме да забележеме дека:

$\alpha = \{(m, n) \mid m, n \in A,\ n - m = 4\}$

$\beta = \{(m, n) \mid m, n \in A,\ n - m = 6\}$

$\gamma = \{(m, n) \mid m, n \in A,\ n - m = 12\}$.

а) $\alpha^* = \{(m, n) \mid m, n \in A, n - m = 4, 8, 12, 16\}$;

$\beta^* = \{(m, n) \mid m, n \in A, n - m = 6, 12\}$; $\gamma^* = \gamma$.

б) Според 3.62. имаме:

$\alpha_1 = (\alpha \cup \alpha^{-1} \cup \Delta_A) = \Delta_A \cup \{(m, n) \mid m, n \in A, \mid m - n \mid = 4, 8, 12, 16\}$;

$\beta_1 = (\beta \cup \beta^{-1} \cup \Delta_A) = \Delta_A \cup \{(m, n) \mid m, n \in A, \mid m - n \mid = 6, 12\}$;

$\gamma_1 = (\gamma \cup \gamma^{-1} \cup \Delta_A) = \Delta_A \cup \{(m, n) \mid m, n \in A, \mid m - n \mid = 12\}$.

в) $A/_{\alpha_1} = \{\{1, 5, 9, 13, 17\}, \{2, 6, 10, 14, 18\}, \{3, 7, 11, 15\}, \{4, 8, 12, 16\}\} = \{A_1, A_2, A_3, A_4\}$;

$A/_{\beta_1} = \{\{1, 7, 13\}, \{2, 8, 14\}, \{3, 9, 15\}, \{4, 10, 16\}, \{5, 11, 17\}, \{6, 12, 18\}\} = \{B_1, B_2, \ldots, B_6\}$;

$A/_{\gamma_1} = \{\{1, 13\}, \{2, 14\}, \{3, 15\}, \{4, 16\}, \{5, 17\}, \{6, 18\}, \{7\}, \{8\}, \{9\}, 10\}, \{11\}, \{12\}\} = \{C_1, C_2, \ldots, C_{12}\}$.

г) nat α_1: $1, 5, 9, 13, 17 \to A_1$; $2, 6, 10, 14, 18 \to A_2$; $3, 7, 11, 15 \to A_3$; $4, 8, 12, 16 \to A_4$.

nat β_1: $1, 7, 13 \to B_1$; $2, 8, 14 \to B_2$; $3, 9, 15 \to B_3$ $4, 10, 16 \to B_4$; $5, 11, 17 \to B_5$; $6, 12, 18 \to B_6$.

nat γ_1: $1, 13 \to C_1$; $2, 14 \to C_2$; $3, 15 \to C_3$; $4, 16 \to C_4$; $5, 17 \to C_5$; $6, 18 \to C_6$; $i \to C_i$, $i = 7, \ldots, 12$.

д) Нека τ е транзитивниот производ на α и β. Имаме:

$\tau = (\alpha \cup \beta)^* = \{(m, n) \mid m, n \in A, |m - n| = 4, 6, 8, \ldots, 16\}$.

3.64. Нека α_i, $i = 1, 2, 3$, се релации во $\mathbb{N}$, определени со:

$\alpha_i = \{(x, x + m_i) \mid x \in \mathbb{N}\}$, $i = 1, 2, 3$,

каде што m_1, m_2, m_3, се дадени природни броеви.

а) Да се најдат транзитивните проширувања α_i^*, $i = 1, 2, 3$.

б) Да се најдат минималните еквивалентности β_i што ги содржат α_i, $i = 1, 2, 3$.

в) Во кој случај $\beta_1 \subseteq \beta_2$?

г) Во кој случај $\beta_1 = \beta_2 \cap \beta_3$?

Решение. а) $\alpha_i^* = \bigcup_{k \in \mathbb{N}} \{(x, x + km_i) \mid x \in \mathbb{N}\}$, $i = 1, 2, 3$.

б) $\beta_i = \equiv (\mathrm{mod} m_i)$, $i = 1, 2, 3$

в) $m_2 \mid m_1$.

г) $m_1 = [m_2, m_3]$, каде што $[m_2, m_3]$ го означува најмалиот заеднички содржател на m_2 и m_3.

§ 4. ПОДРЕДЕНИ МНОЖЕСТВА

4.1. Да се направат дијаграми за следниве подредени множества:

а) $A = \{a, b, c, d, e\}$ и $\alpha = \Delta_A \cup \{(a, b), (a, c), (b, c), (a, d), (a, e), (d, e)\}$;

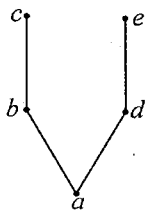
б) $A = \{(a, b, c, d, e\}$ и $\alpha = \Delta_A \cup \{(a, b), (a, c), (a, d), (a, e), (b, e), (c, e), (d, e)\}$;

в) $A = \{a, b, c, d, e, f, g\}$ и $\alpha = \Delta_A \cup \{(a, b), (a, d), (b, e), (f, g), (a, e)\}$;

г) $A = \mathbb{P}(\{a, b, c\})$ и $\alpha = (\subseteq)$.

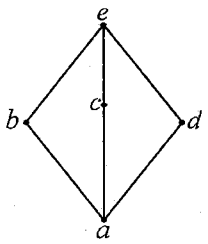
За секој пример да се напише кој елемент е максимален; минимален; најголем; најмал.

Решение. а)



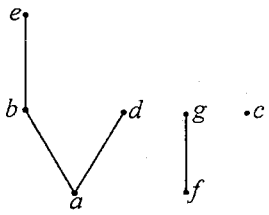
a најмал
c, e максимални

б)



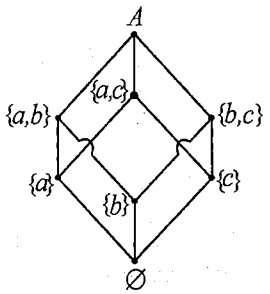
a најмал
e најголем

в)



a, c, f минимални
d, e, c, g максимални

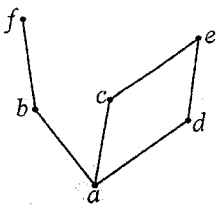
г)



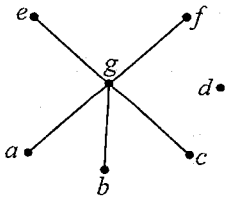
$\varnothing$ најмал
A најголем

4.2. Кое множество A и подредување α одговара на дијаграмот

а)



б)



Решение. а) $A=\{a, b, c, d, e, f\}$,

$\alpha = \Delta_A \cup \{(a, b), (a, c), (a, d), (a, e), (a, f), (b, f), (c, e), (d, e)\}$.

б) $A = \{a, b, c, d, e, f, g\}$,

$\alpha = \Delta_A \cup \{(a, g), (a, e), (a, f), (b, g), (b, e), (b, f), (c, g), (c, e), (c, f), (g, e), (g, f)\}$.

4.3. Да се покаже дека не секоја антисиметрична релација може да се прошири до подредување.

Решение. За да го покажеме тоа ќе дадеме еден пример.

Нека $M = \{a, b, c\}$ и $\alpha = \{(a, b), (b, c), (c, a)\}$. Релацијата α е антисиметрична. За релацијата α да ја проширime до подредување β, треба β да биде рефлексивна, антисиметрична и транзитивна и притоа $\alpha \subseteq \beta$. Јасно е дека $a\beta b$. Од $b\beta c$ и $c\beta a$, следува и $b\beta a$, а тоа значи дека β нема да биде антисиметрична.

4.4. Нека е $\{\alpha_i \mid i \in I\}$ непразна фамилија подредувања на X потполно подредени по инклузија. Да се покаже дека $\bigcup_i \alpha_i$ е подредување на X.

Решение. Да ставиме $\alpha = \bigcup_i \alpha_i$.Бидејќи релацијата α_i е рефлексивна, за секој $i \in I$, имаме $\Delta_X \subseteq \alpha_i$, за секој $i \in I$, па и

$$\Delta_X \subseteq \bigcup_i \alpha_i = \alpha,$$

т.е. α е рефлексивна.

Да покажеме дека релацијата α е антисиметрична. Затоа, нека $a\ \alpha\ b$ и $b\ \alpha\ a$. Тоа значи дека постојат $i, j \in I$, такви што $a\ \alpha_i\ b$ и $b\ \alpha_j\ a$. Но, фамилијата $\{\alpha_i \mid i \in I\}$ е потполно подредена по инклузија, па или $\alpha_i \subseteq \alpha_j$ или $\alpha_j \subseteq \alpha_i$. Можеме да претпоставиме дека $\alpha_i \subseteq \alpha_j$. Тогаш од $a\ \alpha_i\ b$ следува дека $a\ \alpha_j\ b$, а од $a\alpha_j b$ и $b\ \alpha_j\ a$, според антисиметричноста на α_j, следува дека $a = b$, т.е. α е антисиметрична.

Останува да покажеме дека релацијата α е транзитивна. Затоа, ако $a\alpha b$ и $b\alpha c$, правејќи ја истата дискусија како и погоре, добиваме дека $a\alpha c$, т.е. α е транзитивна.

4.5. Нека α е подредување на множеството M, и $A \subseteq M$. Да се покаже дека:

а) $\beta = \alpha \cap (A \times A)$ е подредување на A.

б) Ако α е потполно подредување на M, тогаш β е потполно подредување на A.

в) Може да се случи β да е потполно подредување на A, а α да не е потполно подредување на M.

4.6. Во кој случај секој елемент од едно подредено множество е минимален?

Решение. Нека M е подредено множество, така што секој елемент во M е минимален. Ако a и b се два различни елемента од M, тогаш, бидејќи a е минимален, не може да биде $b \leq a$, а бидејќи и b е минимален, не може да биде $a \leq b$. Значи, кои било два различни елементи од M не се споредливи. Во овој случај за подреденото множество M велиме дека е *потполно неподредено*.

4.7. Да се покаже дека во секое конечно подредено множество има барем еден максимален и барем еден минимален елемент. Дали истото важи за бесконечните множества?

Решение. Нека $A = \{a_1, a_2, \ldots, a_n\}$ е конечно подредено множество. Нека a_i е произволен елемент од A; ако $a_j \not\leq a_i$ за кој било $j \neq i$, тогаш a_i е минимален елемент; ако пак постои некој a_k, така што $a_k \leq a_i$, тогаш истата дискусија може да се направи за елементот a_k.

Но, оваа постапка може да се повтори само конечен број пати, што значи дека во A постои барем еден минимален елемент. Слично за максимален.

За бесконечните множества ова не мора да важи. На пример, $\mathbb{R}$ во однос на обичното подредување.

4.8. Да се даде пример на подредено множество со само еден максимален елемент што не е најголем. Дали постои конечно подредено множество со тоа својство?

Решение. Нека $M = \{a_1, a_2, \ldots, a_n, \ldots\}$ и нека подредувањето во M е зададено со:

$a_1 \leq a_5 \leq a_6 \leq \ldots \leq a_n \ldots$

$a_1 \leq a_2 \leq a_3 \leq a_4$.

Во така подреденото множество M елементот a_4 е единствен максимален, но не и најголем.

Ако M е конечно множество со единствен максимален елемент, тогаш тој е и најголем елемент.

4.9. Да се покаже дека, ако во една мрежа постои максимален (минимален) елемент, тогаш тој е и најголем (најмал) елемент.

Решение. Нека подреденото множество M е мрежа и нека m е максимален елемент во M; тоа значи дека m не е помал нити од еден елемент од M. Ако a е произволен елемент од M, тогаш, бидејќи m е максимален, имаме $a \cup m = m$ и $a \leq a \cup m = m$. Значи, секој елемент од M е помал од m, т.е. m е најголем елемент во M.

Слично и за минимален.

4.10. Ако M е мрежа и A е конечно подмножество од M, тогаш постојат $\sup A$ и $\inf A$.

Решение. Нека M е мрежа и $A = \{a_i \mid i=1, 2,\ldots n\}$ конечно подмножество од M. Тогаш постојат елементите:

$$b_2 = a_1 \cap a_2, \quad b_3 = b_2 \cap a_3, \ \ldots\ , b_n = b_{n-1} \cap a_n,$$

и притоа имаме $b_n \leq a_i$, за секој $i = 1, 2,\ldots, n$, т.е. b_n е минорант за A. Ако c е друг минорант за множеството A, тогаш имаме:

$$c \leq a_1 \cap a_2 = b_2, \quad c \leq b_2 \cap a_3, \ \ldots, c \leq b_{n-1} \cap a_n = b_n,$$

т.е. b_n е најголемиот минорант. Значи, имаме $\inf A = b_n$.

Слично се покажува дека постои и $\sup A$.

4.11. Да се покаже дека секоја конечна мрежа е комплетна.

Решение. Нека M е конечна мрежа. Бидејќи секое подмножество A од M е конечно, според претходната задача, постојат $\sup A$ и $\inf A$, па M е комплетна мрежа.

4.12. Нека M е множеството од сите претподредувања на множеството A. Да се покаже дека M е комплетна мрежа.

Решение. Множеството M е подредено по инклузија. Да покажеме прво дека M е мрежа. Ако α и β се две претподредувања на множеството A, тогаш имаме $\inf\{\alpha, \beta\} = \alpha \cap \beta$ и $\sup\{\alpha, \beta\} = (\alpha \cup \beta)^*$, каде што $(\alpha \cup \beta)^*$ е транзитивното проширување на $\alpha \cup \beta$. Значи, M е мрежа.

Останува да покажеме дека мрежата M е комплетна. Навистина, релацијата $A \times A$ е претподредување и притоа таа е најголем елемент во M. Ако $\{\alpha_i \mid i \in I\}$ е произволна фамилија претподредувања на A, тогаш $\bigcap_i \alpha_i$ е исто така претподредување на A и притоа имаме $\bigcap_i \alpha_i = \inf\{\alpha_i \in I\}$.

Од сето тоа следува дека мрежата M е комплетна.

4.13. Дали сите потполни подредувања на A формираат мрежа?

Решение. Нека M е множеството од сите потполни подредувања на A. Множеството M не е мрежа, зашто на пример, ако α е кое било потполно подредување на A, тогаш и α^{-1} е потполно подредување на A, но $\alpha \cap \alpha^{-1}$ не е потполно подредување туку потполно неподредување. Значи, множеството M не е мрежа.

4.14. Ако е $M = \{a, b, c\}$, да се определат сите:

а) еквивалентности на M.

б) подредувања на M.

Потоа да се направат дијаграмите на овие подредени множества. Дали некое од овие подредени множества е мрежа?

Решение. Еквивалентностите на множеството M се:

$\alpha_1 = \Delta_M$, $\alpha_2 = \Delta_M \cup \{(a, b), (b, a)\}$, $\alpha_3 = \Delta_M \cup \{(a, c), (c, a)\}$,

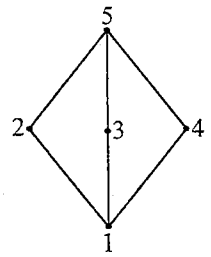
$\alpha_4 = \Delta_M \cup \{(b, c), (c, b)\}$, и $\alpha_5 = M \times M$.

б) Подредувањата на множествата M се:

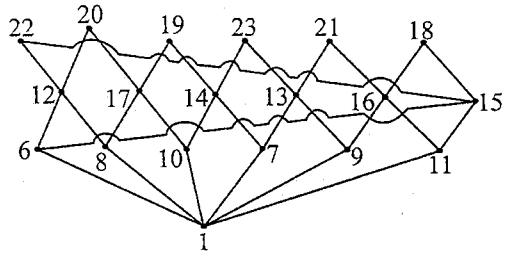
$\alpha_1 = \Delta_M$, $\alpha_6 = \Delta_M \cup \{(a, b)\}$, $\alpha_7 = \alpha_6^{-1}$, $\alpha_8 = \Delta_M \cup \{(a, c)\}$, $\alpha_9 = \alpha_8^{-1}$,
$\alpha_{10} = \Delta_M \cup \{(b, c)\}$, $\alpha_{11} = \alpha_{10}^{-1}$, $\alpha_{12} = \Delta_M \cup \{(a, b), (a, c)\}$, $\alpha_{13} = \alpha_{12}^{-1}$,
$\alpha_{14} = \Delta_M \cup \{(b, a), (b, c)\}$, $\alpha_{15} = \alpha_{14}^{-1}$, $\alpha_{16} = \Delta_M \cup \{(c, a), (c, b)\}$,
$\alpha_{17} = \alpha_{16}^{-1}$, $\alpha_{18} = \Delta_M \cup \{(a, b), (c, a), (c, b)\}$, $\alpha_{19} = \alpha_{18}^{-1}$,
$\alpha_{20} = \Delta_M \cup \{(a, b), (a, c), (b, c)\}$,
$\alpha_{21} = \alpha_{20}^{-1}$, $\alpha_{22} = \Delta_M \cup \{(a, b), (a, c), (c, b)\}$, $\alpha_{23} = \alpha_{22}^{-1}$.

Дијаграмите на овие подредени множества се:

а)



б)



Множеството од сите еквивалентности на M е мрежа, но множеството од сите подредувања на M не е мрежа.

4.15. Ако M е множеството од сите подредувања на множеството A, да се покаже дека α е максимален елемент во M ако и само ако α е потполно подредување на A.

Решение. Нека α е потполно подредување на A и нека $\beta \in M$, така што $\alpha \subseteq \beta$. Ако $x \beta y$, тогаш, бидејќи α е потполно подредување, имаме

$x\alpha y$ или $y\alpha x$. Ако $y\alpha x$, тогаш и $y\beta x$, односно $x = y$. Значи, имаме $x\alpha y$, т.е. $\alpha = \beta$. Значи, ако α е потполно подредување на A, тогаш α е максимален елемент во M.

Да претпоставиме сега дека подредувањето α не е потполно. Тоа значи дека постојат барем два елемента $a, b \in A$, такви што

$a \alpha' b$ и $b \alpha' a$. Дефинираме релација β во A со:

$\beta = \alpha \cup \{(x, y) \mid x, y \in A,\ x \alpha a,\ b \alpha y\}$.

Јасно е дека $\alpha \subset \beta$, па ако покажеме дека β е подредување на A, ќе следува дека α не е максимален елемент во M.

Од $\Delta_A \subseteq \alpha \subset \beta$, следува дека β е рефлексивна. Да покажеме дека е антисиметрична. Нека $x \beta y$ и $y \beta x$.

Ако $x\alpha y$ и $y\alpha x$, бидејќи α е подредување, следува дека $x = y$.

Ако $x \alpha' y$ и $y\alpha x$, тогаш $x\alpha a$, $b\alpha y$ и $y\alpha x$. Од $b\alpha y$ и $y\alpha x$ следува $b\alpha x$, а потоа од $b\alpha x$ и $x\alpha a$ следува $b\alpha a$, коешто не е можно. Слично добиваме дека не е можен и случајот $x \alpha y$, $y \alpha' x$.

Ако $x \alpha' y$ и $y \alpha' x$, тогаш $x\alpha a$, $b\alpha y$, $y\alpha a$, $b\alpha x$, т.е. $b\alpha a$, коешто не е можно.

Значи, ако $x\beta y$ и $y\beta x$, тогаш $x\alpha y$ и $y\alpha x$, па $x = y$ т.е. β е антисиметрична.

Правејќи слична дискусија се добива дека β е и транзитивна, т.е. β е подредување на A што го содржи подредувањето α.

4.16. Ако M е мрежа и ако $a, b \in M$, $a \le b$, тогаш $[a, b]$ се определува со: $[a, b] = \{x \mid x \in M, a \le x \le b\}$.

а) Да се покаже дека $[a, b]$ е подмрежа од M и дека, ако M е комплетна мрежа, тогаш $[a, b]$ е нејзина комплетна подмрежа.

б) Нека пресликувањата $f, g : M \to [a, b]$ се определени со:

$f(x) = (x \cap b) \cup a$, $g(x) = (x \cup a) \cap b$.

Да се покаже дека $gf = f^2 = f$, $fg = g^2 = g$.

Решение. а) Нека $x, y \in [a, b]$; тоа значи дека $a \le x \le b$ и $a \le y \le b$. Затоа,

$a \le x \le x \cup y$, $b \ge x \ge x \cap y$.

Понатаму, од $x \le b$ и $y \le b$, имаме $x \cup y \le b \cup b = b$, а од $a \le x$ и $a \le y$, имаме $a = a \cap a \le x \cap y$. Значи имаме

$a \le x \cup y \le b$ и $a \le x \cap y \le b$,

т.е. $[a, b]$ е подмрежа од M.

Да претпоставиме сега дека мрежата M е комплетна и A подмножество од $[a, b]$. Нека $\sup_M A = c$, $\inf_M A = d$. За секој $x \in A$ имаме $a \le x \le b$, па значи a е еден минорант, а b еден мајорант за A во M. Но, c е најмалиот мајорант на A во M, па $c \le b$, а јасно е

дека $a \le c$. Значи, $c \in [a, b]$. Слично, добиваме дека $d \in [a, b]$, т.е. $[a, b]$ е комплетна подмрежа од M.

б) Ако $x \in [a, b]$, тогаш имаме:

$f(x) = (x \cap b) \cup a = x \cup a = x$, $g(x) = (x \cup a) \cap b = x \cap b = x$.

Нека сега x е произволен елемент од M. Тогаш имаме:

$$gf(x) = g((x \cap b) \cup a) = (x \cap b) \cup a = f(x),$$

$f^2(x) = f((x \cap b) \cup a) = (x \cap b) \cup a = f(x)$,

$fg(x) = f((x \cup a) \cap b) = (x \cup a) \cap b = g(x)$,

$g^2(x) = g((x \cup a) \cap b) = (x \cup a) \cap b = g(x)$,

т.е. $gf = f^2 = f$, $fg = g^2 = g$.

4.17. Ако M е мрежа и $a, b, c \in M$, такви што $a \le b$, да се покаже дека

$$(c \cap b) \cup a \le (c \cup a) \cap b. \tag{1}$$

Решение. Имаме:

$a \le b \Rightarrow c \cap b \le (c \cup a) \cap b$,

$a \le b \Rightarrow a = a \cap b \le (c \cup a) \cap b$,

од каде што следува (1).

4.18. Да се покаже дека една мрежа M е модуларна ако и само ако е исполнет условот

$$b \le c, \quad a \cap b = a \cap c, \quad a \cup b = a \cup c \Rightarrow b = c. \tag{1}$$

Решение. Ако мрежата M е модуларна и ако $b \le c$, $a \cap b = a \cap c$, $a \cup b = a \cup c$, тогаш имаме:

$b = b \cup (b \cap a) = b \cup (c \cap a) = c \cap (b \cup a) = c \cap (c \cup a) = c$.

Обратно, нека во мрежата M е исполнет условот (1) и нека x, y, z се произволни елементи од M, при што $x \ge y$. Од $x \ge y$, според 4.17, имаме

$$(z \cap x) \cup y \le (z \cup y) \cap x. \tag{2}$$

Понатаму имаме

$(x \cap (y \cup z)) \cap z = x \cap ((y \cup z) \cap z) = x \cap z$,

а бидејќи $x \ge y$, имаме и $x \ge y \cup (x \cap z)$, па

$x \cap z \ge (y \cup (x \cap z)) \cap z \ge (x \cap z) \cap z = x \cap z$,

т.е. $(y \cup (x \cap z)) \cap z = x \cap z$. Значи, добиваме

$$x \cap (y \cup z)) \cap z = (y \cup (x \cap z)) \cap z \tag{3}$$

Ако во (3) ги смениме местата на x и y, како и на $\cap$ и $\cup$, добиваме

$$(x \cap (y \cup z)) \cup z = (y \cup (x \cap z)) \cup z. \tag{4}$$

Применувајќи го (1) на (2), (3) и (4), добиваме

$x \cap (y \cup z) = y \cup (x \cap z)$,

што значи дека мрежата M е модуларна.

4.19. Да се покаже дека една мрежа е дистрибутивна ако и само ако е исполнет условот

$a \cap b = a \cap c, a \cup b = a \cup c \Rightarrow b = c.$

4.20. Нека M е комплетна мрежа и f е монотоно пресликување од M во M. Да се покаже дека постои $a \in M$, таков што $f(a) = a$. Ако S е множеството од сите такви елементи, да се покаже дека S е комплетна мрежа во однос на подредувањето индуцирано од подредувањето на M. Дали оваа мрежа е и подмрежа од M ?

Решение. Нека M комплетна мрежа, а $f : M \to M$ монотоно пресликување. Ако

$A = \{x \mid x \in M,\ x \leq f(x)\},$

нека $a = \sup A$. Значи, за кој било $x \in A$, имаме $x \leq a$, па и $x \leq f(a)$, т.е. $f(a)$ е исто така еден мајорант на A. Но, a е најмалиот мајорант, па имаме $a \leq f(a)$, $a \in A$. Од $a \leq f(a)$, следува $f(a) \leq f(f(a))$ т.е. $f(a) \in A$, а тоа значи дека $f(a) \leq a$. На крајот, од $a \leq f(a)$ и $f(a) \leq a$, следува $a = f(a)$.

Нека сега, S е множеството од сите такви елементи, а B нека е подмножество од S. Ако

$C = \{y \mid y \in M, y \leq f(y), y$ е минорант на $B\},$

да ставиме $c = \sup C$. Тогаш имаме

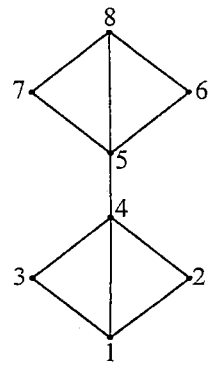
$y \leq c \Rightarrow f(y) \leq f(c),$

т.е. $y \leq f(c)$.Тоа значи дека $f(c)$ е мајорант на C, т.е. $c \leq f(c)$, $c \in C$. Понатаму имаме

$c \leq f(c) \Rightarrow f(c) \leq f(f(c)),$

т.е. $f(c) \in C$. Бидејќи $c = \sup C$, следува дека $f(c) \leq c$, т.е. $f(c) = c$, па $c \in S$. Јасно е дека c е минорант на B. Ако d е друг минорант на B со особината $f(d) = d$, тогаш $d \in C$, па $d \leq c$, т.е. $c = \inf B$.

Од друга страна множеството S има најголем елемент, па значи S е комплетна мрежа.



Мрежата S во општ случај не е подмрежа од M. За да го покажеме тоа ќе дадеме еден пример.

Нека $M = \{1, 2, \ldots, 8\}$, подредувањето во M нека е дадено со дијаграмот. Јасно е дека M е комплетна мрежа. Пресликувањето f од M во M, дефинирано со:

f : 1→2, 2→2, 3→3, 4→5, 5→6, 6→6, 7→7, 8→8, е монотоно и притоа имаме

$S = \{2, 3, 6, 7, 8\}$. Ако $B = \{2, 3\}$, тогаш имаме $\inf_S B = 2$, а $\inf_M B = 1$.

Значи, мрежата S не е подмрежа од M.

4.21. Нека M е подредено множество. За подмножеството A од M велиме дека е *почетен сегмент*, ако е исполнет условот:

$a \in A, x \in M, x \leq a \Rightarrow x \in A$.

Да се покаже дека фамилијата $\mathbb{L}(M)$, од сите почетни сегменти на M, е комплетна мрежа.

Решение. Нека $\{A_i \mid i \in I\}$ е произволна фамилија елементи од $\mathbb{L}(M)$, т.е. произволна фамилија почетни сегменти од M. Множеството

$$A = \bigcap_i A_i ,$$

е исто така почетен сегмент од M и притоа A е минорант за фамилијата $\{A_i \mid i \in I\}$. Ако B е друг минорант, тогаш од $B \subseteq A_i$, за секој $i \in I$, добиваме дека $B \subseteq A$, т.е. $A = \inf\{A_i \mid i \in I\}$.

Бидејќи M е најголем елемент во $\mathbb{L}(M)$, следува дека $\mathbb{L}(M)$ е комплетна мрежа.

4.22. Нека M е подредено множество и нека за секој $a \in M$ се дефинирани множествата $(-\infty, a]$ и $(-\infty, a)$ со:

$(-\infty, a] = \{x \mid x \in M, x \leq a\}$, $(-\infty, a) = \{x \mid x \in M, x < a\}$.

Да се покаже дека:

а) $(-\infty, a]$ и $(-\infty, a)$ се почетни сегменти.

б) $\bigcup_{a \in M} (-\infty, a) \subseteq M$, $\bigcup_{a \in M} (-\infty, a] = M$.

в) ако $M \neq \emptyset$, тогаш $\bigcap_{a \in M} (-\infty, a) = \emptyset$ и

$$\bigcap_{a \in M} (-\infty, a] = \begin{cases} m, \text{ ако } m \text{ е најмал елемент на M} \\ \emptyset, \text{ ако } M \text{ нема најмал елемент.} \end{cases}$$

4.23. Ако M е подредено множество, во мрежата $\mathbb{L}(M)$ (в.4.21) определуваме релација $\equiv$ со:

$$A \equiv B \Leftrightarrow A = B \vee (\exists a \in M)\{[A = (-\infty, a] \wedge B = (-\infty, a)\ ] \vee$$
$$\vee [A = (-\infty, a) \wedge B = (-\infty, a]\ ]\ \}$$

а) Да се покаже дека релацијата $\equiv$ е еквивалентност и дека класите на еквивалентност се едноелементни или двоелементни множества.

б) Фактор–множеството $\mathbb{L}(M) / \equiv$ да го означиме со $\mathbb{L}^*(M)$. Да се покаже дека постои само едно подредување на $\mathbb{L}^*(M)$, такво што

природното пресликување nat≡ да биде монотоно и притоа, $\mathbb{L}^*(M)$ е комплетна мрежа во однос на тоа подредување.

в) Што преставува $\mathbb{L}^*(M)$, ако $M = \mathbb{N}$, $M = \mathbb{Q}$, односно $M = \mathbb{R}$?

Решение. а) Дека релацијата ≡ е рефлексивна и симетрична е јасно. Да покажеме дека е и транзитивна. Нека $A \equiv B$ и $B \equiv C$. Ако $A = B$ или $B = C$, тогаш јасно е дека $A \equiv C$. Затоа нека $A \neq B$ и $B \neq C$. Можни се следниве два случаја:

$A = (-\infty, a), B = (-\infty, a], C = (-\infty, a)$;

$A = (-\infty, a], B = (-\infty, a), C = (-\infty, a]$;

па значи во секој случај $A \equiv C$. Значи, релацијата ≡ е еквивалентност.

Од доказот на транзитивноста на релацијата ≡ се гледа дека класите на еквивалентност се или едноелементни или двоелементни множества. Едноелементни се, на пример, класите $\{A\}$, за секое подмножество A од M, коешто не е од облик $A = (-\infty, a)$ или $A = (-\infty, a]$. Ако во M нема најголем елемент, тогаш е и $M^{\equiv} = \{M\}$ едноелементно множество.

б) Ако во $\mathbb{L}^*(M)$ дефинираме подредување со :

$$A^{\equiv} \leq B^{\equiv} \Leftrightarrow A \subseteq B\,, \tag{1}$$

тогаш, јасно е дека пресликувањето nat ≡ е монотоно. Ако пак nat ≡ треба да е монотоно, тогаш имаме:

$$A \subseteq B \Rightarrow \text{nat} \equiv (A) \leq \text{nat} \equiv (B) \Rightarrow A^{\equiv} \leq B^{\equiv},$$

т.е. само подредувањето дефинирано со (1) е такво што природното пресликување nat ≡ е монотоно.

Да покажеме дека $\mathbb{L}^*(M)$ е комплетна мрежа во однос на подредувањето дефинирано со (1). Јасно е дека $M^{\equiv}$ е најголем елемент во $\mathbb{L}^*(M)$. Понатаму, ако $\left\{A_i^{\equiv} \mid i \in I\right\}$ е подмножество од $\mathbb{L}^*(M)$, тогаш $\bigcup_i A_i^{\equiv} \subseteq \mathbb{L}(M)$. Но, $\mathbb{L}(\mathrm{M})$ е комплетна мрежа, па ако $A = \inf(\bigcup_i A_i^{\equiv})$, тогаш $A^{\equiv} = \inf\left\{A_i^{\equiv} \mid i \in I\right\}$ Значи, $\mathbb{L}^*(M)$ е комплетна мрежа.

в) $\mathbb{L}^*(\mathbb{N})$ е изоморфно со проширеното множество $\mathbb{N} \cup \{\infty\}$ на природните броеви, каде што $(\forall n \in \mathbb{N}) n < \infty$. $\mathbb{L}^*(\mathbb{Q})$, како и $\mathbb{L}^*(\mathbb{R})$, е изоморфно со проширеното множесво $\mathbb{R} \cup \{-\infty, \infty\}$ на реалните броеви при што $(\forall x \in \mathbb{R})\ -\infty < x < \infty$.

4.24. а) Да се покаже дека пресликувањето $f : a \to (-\infty, a]$ е монотона инјекција од M во $\mathbb{L}(M)$ и од тоа да се заклучи дека $\{(-\infty, a] \mid a \in M\}$ е подмножество од $\mathbb{L}(M)$ изоморфно со M.

б) Да се определи монотона инјекција од M во $\mathbb{L}^*(M)$.

Решение. а) Јасно е дека пресликувањето f е инјекција. Понатаму имаме:

$$a \leq b \Rightarrow (-\infty, a] \subseteq (-\infty, b] \Rightarrow f(a) \leq f(b),$$

т.е. инјекцијата f е монотона.

Нека $A = \{(-\infty, a] \mid a \in M\}$. Бидејќи $f(M) = A$, пресликувањето $f : M \to A$ е биекција. Значи, постои пресликување $f^{-1} : A \to M$, коешто е исто така биекција и притоа монотона, па значи A е подмножество од $\mathbb{L}(M)$, изоморфно со M.

б) Пресликувањето $g : M \to \mathbb{L}^*(M)$, определено со

$g(a) = \{(-\infty, a), (-\infty, a]\}$,

е монотона инјекција од M во $\mathbb{L}^*(M)$.

4.25. Да се покаже дека секое подредено множество е изоморфно со подредено подмножество од некоја комплетна мрежа.

Решение. Ако M е подредено множество, тогаш $\mathbb{L}(M)$ е комплетна мрежа (4.21), а според 4.24, множеството $A = \{(-\infty, a] \mid a \in M\}$ е подмножество од $\mathbb{L}(M)$, изоморфно со M. Затоа, подреденото множество M може да се смета како подредено подмножество од комплетната мрежа $\mathbb{L}(M)$.

4.26. Нека M е подредено множество, а S непразно подмножество од M. Велиме дека S е *секаде густо* во M ако за секои $a, b \in M$, $a < b$, постои барем еден елемент $s \in S$, таков што $a < s < b$. За M велиме дека е *густо подредено*, ако M е секаде густо во M. Ако пак за секои $a,b \in$ M, $a < b$, множеството $(a,b) = \{x \mid x \in M, a < x < b\}$, е конечно, при што може да биде и празно, тогаш велиме дека M е *дискретно подредено*. Да се покаже дека:

а) $\mathbb{Q}$ и $\mathbb{R}$ се густо подредени множества, при што $\mathbb{Q}$ е секаде густо во $\mathbb{R}$.

б) $\mathbb{Z}$ и $\mathbb{N}$ се дискретно подредени.

в) секое конечно подредено множество е дискретно.

г) секое густо подредено множество е бесконечно.

4.27. Да се покаже дека сите потполни подредувања на едно конечно множество се изоморфни. Дали важи истото и за делумните подредувања, односно потполните подредувања на бесконечните множества?

Решение. Нека $M = \{a_1\, a_2, \ldots, a_n\}$, е конечно множество, а

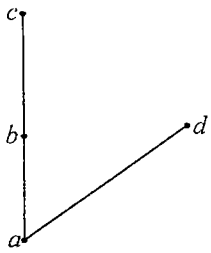
$$\alpha_1 : a_1 \le a_2 \le \ldots \le a_n \text{ и } \alpha_2 : a_{i_1} \le a_{i_2} \le a_{i_n},$$

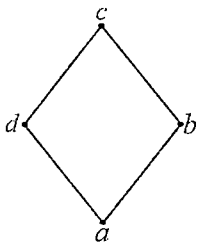
се две потполни подредувања на M. Пресликувањето $f : M \to M$, дефинирано со:

$$f(a_k) = a_{i_k},$$

е биекција и притоа f и f^{-1} се монотони подредувања. Значи потполните подредувања α_1 и α_2 на M се изоморфни.

Делумните подредувања на едно множество M не мора да се изоморфни. На пример, нека $M = \{a, b, c, d\}$, а две делумни подредувања на M се дадени со дијаграмите:





овие две подредувања не се изморфни.

Исто така, потполните подредувања на едно бесконечно множество не мораат да бидат изоморфни. На пример, подредувањата:

$1 < 2 < 3 < \ldots < n < \ldots$, и

$1 < 3 < 5 < \ldots < 2 < 4 < 6 < \ldots$

на множеството $\mathbb{N}$ се потполни, но не се изоморфни.

4.28. Да се покаже дека секој отворен интервал (a, b), $a < b$, од $\mathbb{Q}$ односно $\mathbb{R}$, е изоморфно подредено со $\mathbb{Q}$, односно $\mathbb{R}$.

Упатство. Докажи дека, на пример, пресликувањето

$$f(x) = \frac{b-a}{2} \frac{x}{1+|x|} + \frac{b+a}{2},$$

е монотона биекција од $\mathbb{R}$ во (a, b), ако $(a, b) \subset \mathbb{R}$, односно од $\mathbb{Q}$ во (a, b), ако е $(a, b) \subset \mathbb{Q}$.

4.29. Да се окарактеризираат сите дискретно потполни подредени множества.

Решение. Нека M е дискретно потполно подредено множество. Доволно е да се разгледаат следните три случаи:

i) M има најмал и најголем елемент;

ii) M има најмал но нема најголем елемент;

iii) M нема најмал и нема најголем елемент,

зашто во случај M да нема најмал, а има најголем елемент може да се разгледува инверзното подредување, коешто е исто така дискретно и потполно.

i) Нека a е најмалиот, а b најголемиот елемент во M. Бидејќи M е дискретно подредено, интервалот (a,b) е конечен, а бидејќи M е потполно подредено, имаме $(a, b) = M$. Значи M е конечно множество.

ii) Нека a_1 е најмалиот елемент во M. Јасно е дека множеството M не е конечно, зашто во тој случај, поради потполната подреденост во M би постоел најголем елемент. Нека b е произволен елемент од M, $b \neq a_1$. Интервалот (a_1, b) е конечен, па ако има $n-2$ елемента, елементот b ќе го означиме со a_n. Така ја добиваме низата

$$A = \{a_1, a_2, \dots, a_n, \dots\} \subseteq M, \tag{1}$$

при што

$$a_i \leq a_j \Leftrightarrow i \leq j. \tag{2}$$

Ако a е произволен елемент од M и ако постои барем едно $a_i \in A$, такво што $a < a_i$, тогаш $a \in (a_1, a_i)$, па значи $a \in A$. Затоа, ако $c \in M \setminus A$, ќе имаме $a_n < c$ за секој $n \in \mathbb{N}$. Значи, интервалот (a_1, c) не би бил конечно множество, што значи дека не постои елемент $c \in M \setminus A$, т.е. имаме $A = M$.

Пресликувањето $f : \mathbb{N} \to M$, дефинирано со $f(n) = a_n$ е биекција, а според (2), следува дека f е изоморфизам. Значи, множеството M е изоморфно со множеството $\mathbb{N}$ од природните броеви.

iii) Нека a е произволен елемент од множеството M. Множеството $A = M \setminus (-\infty, a]$, е дискретно потполно подредено со најмал елемент, но без најголем елемент, па значи, тоа е изоморфно со множеството $\mathbb{N}$. Нека тој изоморфизам е f. Множеството $(-\infty, a)$ е дискретно потполно подредено без најмал, но со најголем елемент.

Како во (ii), може да се покаже дека множеството $(-\infty, a)$ е изоморфно со множеството од негативните цели броеви. Нека тој изоморфизам е g.

Пресликувањето $h : \mathrm{M} \to \mathbb{Z}$, дефинирано со

$$h(x)=\begin{cases}0 & \text{ако } x=a\\ f(x), & \text{ако } x\in A,\\ g(x), & \text{ако } x\in(-\infty,a)\end{cases}$$

е изоморфизам, т.е. M е изоморфно со множеството $\mathbb{Z}$ од целите броеви.

4.30. За едно потполно подредено множество велиме дека е *непрекинато подредено*, ако секое мајорирано подмножество има супремум, а секое минорирано подмножество има инфимум. Да се покаже дека множеството $\mathbb{R}$ е непрекинато подредено.

4.31. Множеството комплексни броеви го подредуваме со:

$a+ib<c+id \Leftrightarrow a<c \vee (a=c \wedge b<d)$.

а) Да се покаже дека со тоа комплексните броеви се потполно подредени.

б) Дали тоа подредување е: (i) густо; (ii) непрекинато; (iii) изоморфно со подредувањето на $\mathbb{R}$?

Решение. Нека $a+ib$ и $c+id$ се кои било два комплексни броја; можни се следните случаи:

1) $a<c$; 2) $a=c, b<d$; 3) $a=c, b>d$; 4) $c<a$.

Во првиот и вториот случај имаме $a+ib<c+id$, а во третиот и четвртиот случај $c+id<a+id$. Значи множеството комплексни броеви е потполно подредено.

б) (i) Нека $a+ib$ и $c+id$ се кои било два комплексни броја, при што $a+ib<c+id$. Ако $a<c$, тогаш имаме:

$$a+ib<\frac{a+c}{2}+ib<c+id,$$

а ако $a=c$ и $b<d$, тогаш имаме:

$$a+ib<a+i\,\frac{b+d}{2}<c+id,$$

т.е. ова подредување е густо.

(ii) Подредувањето не е непрекинато, зашто на пример, множеството $S=\{x+iy \mid x, y\in\mathbb{R},\ 0\le x\le 1\}$ е мајорирано но, не постои $\sup S$. Секој комплексен број $a+ib$, $a>1$, е мајорант за S.

(iii) Бидејќи подредувањето не е непрекинато, следува дека тоа не е изоморфно со подредувањето на $\mathbb{R}$.

4.32. Дали следното множество рационални броеви, подредени по големина, е добро подредено?

а) Множеството од сите цели негативни броеви.

б) Множеството од сите броеви од видот $\frac{n}{n+1}$, $n\in\mathbb{N}$.

в) Множеството броеви од видот $\left(\frac{4}{3}\right)^n$, $n\in\mathbb{N}$.

г) Множеството броеви од видот $\left(\frac{3}{4}\right)^n$, $n\in\mathbb{N}$.

д) Множеството броеви од видот $-\frac{1}{n}$, $n\in\mathbb{N}$.

Одговор. а) Не. б) Да. в) Да. г) Не. д) Да.

4.33. Да се покаже дека едно густо подредено множество M не може да биде добро подредено.

Решение. Нека M е густо подредено множество и нека $a,b\in M$, $a < b$. Да го разгледаме множеството

$(a, b) = \{x \mid x\in M, a < x < b\}$.

Бидејќи M е густо подредено, следува дека множеството (a, b) не е празно. За секој елемент $c\in(a, b)$ множеството (a, c) не е празно па значи во (a, b) нема најмал елемент, т.е. M не е добро подредено.

4.34. Какво е множеството A ако во него постои потполно подредување α, такво што α и α^{-1} се добри подредувања ?

Решение. Нека α е потполно подредување на множеството A, така што α и α^{-1} се добри подредувања. Бидејќи множеството A е потполно и добро подредено во однос на α, тоа е дискретна верига со најмал елемент. Од тоа што и α^{-1} е добро подредување следува дека A има и најголем елемент ($[a, b] \subset \mathbb{R}$, $a < b$ е верига со најмал и најголем елемент но не и конечна). Но, која било дискретна верига со најмал и со најголем елемент е конечна, па значи, множеството A е конечно.

4.35. Нека M е добро подредено множество со најмал елемент a и нека S е подмножество од M со следниве особини:

(i) $a\in S$;

(ii) $(\forall x\in M)\ \{[a, x) \subseteq S \Rightarrow x\in S$, при што $[a, x) = \{y \mid y\in M,\ a \le y < x\}\}$.

Да се покаже дека $S = M$ (Оваа особина е позната како *принцип на трансфинитна индукција.)*

Решение. Да го разгледаме множеството S'_M. Бидејќи M е добро подредено, во S'_M имаме најмал елемент; да го означиме со s. Така имаме $[a, s) \subseteq S$; но, според (ii), имаме $s \in S$, спротивно на тоа дека s е најмал во S'_M. Од ова следува дека во S'_M нема најмал елемент, па $S'_M = \varnothing$, т.е. $S = M$.

4.36. Нека M_1 и M_2 се добро подредени множества, со најмали елементи a_1 и a_2, а $f: M_1 \to M_2$ нека е изоморфизам. Да се покаже:

а) $f(a_1) = a_2$;

б) f е единствениот изоморфизам од M_1 во M_2.

Решение. а) Нека $f: M_1 \to M_2$ е изоморфизам и нека $f(a_1) = x_2$. Од $a_2 \le x_2$ следува $f^{-1}(a_2) \le f^{-1}(x_2)$, т.е. $f^{-1}(a_2) \le a_1$. Но, a_1 е најмал елемент во M_1, па $f^{-1}(a_2) = a_1$ т.е. $f(a_1) = a_2$.

б) Да препоставиме дека $g: M_1 \to M_2$ е исто така изоморфизам. Ќе покажеме дека $f = g$. За таа цел, нека S е подмножество од M_1, определено со:

$x \in S \Rightarrow f(x) = g(x)$.

Јасно е дека $f(a_1) = g(a_1) = a_2$, па значи $a_1 \in S$. Да претпоставиме дека $[a, x) \subseteq S$. Тоа значи дека, за секој $y \in [a, x)$, $f(y) = g(y)$. Нека $f(x) = x'$, $g(x) = x''$ и притоа $x' < x''$. Постои елемент $x_1 \in M_1$, таков што $g(x_1) = x'$. Од $g(x_1) < g(x)$, следува дека $x_1 < x$, т.е. $x_1 \in [a, x)$, а од претпоставката $[a, x) \subseteq S$, следува дека $f(x_1) = g(x_1) = x'$, т.е. $f(x) = f(x_1)$, па значи $x = x_1$. Ова противречи на препоставката $x_1 < x$, па значи имаме $f(x) = g(x)$, односно $x \in S$.

Според претходната задача, имаме $S = M_1$, па значи:

$(\forall x \in M_1)\ f(x) = g(x)$, т.е. $f = g$.

4.37. Да се покаже дека две произволни добро подредени множества се изоморфни, или пак едното од нив е изоморфно со некој почетен сегмент од другото.

Решение. Нека M_1 и M_2 се две добро подредени множества. Ако M_1 и M_2 се изоморфни, тогаш нема што да се покажува. Затоа да претпоставиме дека тие не се изоморфни. Во овој случај ќе покажеме дека едното од нив е изоморфно со некој почетен сегмент на другото.

Нека X е множеството од сите пресликувања, такви што секое од нив е изоморфизам од некој почетен сегмент од M_1 на секој

почетен сегмент од M_2. Ако $f : A_1 \to B_1$, $g : A_2 \to B_2$ (A_1 и A_2 се почетни сегменти од M_1, а B_1 и B_2 се почетни сегменти од M_2) се два такви изоморфизма, тогаш ставаме:

$$f \leq g \Leftrightarrow A_1 \subseteq A_2. \qquad (1)$$

Јасно е дека со (1) е дадено едно подредување на множеството X. Бидејќи, произволна унија на почетни сегменти од множеството M_1 е пак почетен сегмент од M_1, заклучуваме дека произволна верига од X е мајорирана. Според лемата на Цорн, добиваме дека во X постои максимален елемент. Нека е тоа изоморфизмот $h : A \to B$. Ако $A \neq M_1$ и $B \neq M_2$, нека е a најмалиот елемент во $M_1 \setminus A$, а b најмалиот елемент во $M_2 \setminus B$. Множествата $A \cup \{a\}$ и $B \cup \{b\}$, се почетни сегменти од M_1 и M_2 соодветно и пресликувањето $\mathrm{k} : A \cup \{a\} \to B \cup \{b\}$, дефинирано со :

$$\mathrm{k}(x) = \begin{cases} h(x), & \text{ако} \quad x \in A \\ b, & \text{ако} \quad x = a, \end{cases}$$

е изоморфизам и притоа имаме $h \leq \mathrm{k}$, спротивно на претпоставката дека h е максимален елемент во X. Значи, или $A = M_1$, или $B = M_2$, т.е. едното од добро подредените множества M_1, M_2 е изоморфно со некој почетен сегмент на другото.

4.38. Ако M_1 и M_2 се две произволни множества, да се покаже дека еден од следниве услови е исполнет: $\mathrm{k}M_1 = \mathrm{k}M_2$, $\mathrm{k}M_1 \leq \mathrm{k}M_2$, $\mathrm{k}M_1 \geq \mathrm{k}M_2$.

Решение. Бидејќи, според аксиомата на Цермело, секое множество може добро да се подреди, множествата M_1 и M_2 можеме да ги сметаме за добро подредени. Според претходната задача, добро подредените множества или се изоморфни, или пак едното од нив е изоморфно со некој почетен сегмент на другото.

Ако M_1 и M_2 се изоморфни, тогаш постои биекција од M_1 во M_2, па $\mathrm{k}M_1 = \mathrm{k}M_2$. Ако пак M_1 е изоморфен со некој почетен сегмент од M_2, тогаш постои инјекција од M_1 во M_2, па $\mathrm{k}M_1 \leq \mathrm{k}M_2$; на крајот, ако M_2 е изоморфно со некој почетен сегмент на M_1, тогаш $\mathrm{k}M_2 \leq \mathrm{k}M_1$.

4.39. Да се покаже дека: лемата на Цорн, теоремата на Хаусдорф и аксиомата на Цермело се еквивалентни на аксиомата за избор. Притоа:

(i) (*Аксиома за избор*) Ако M е непразно множество, тогаш постои пресликување $f : \mathbb{P}(M) \to M$, такво што $f(A) \in A$, за секое непразно подмножество A од M.

(ii) (*Лема на Цорн*) Ако M е непразно подредено множество, со особината, секоја верига од M да има мајорант во M, тогаш во M постои барем еден максимален елемент.

(iii) (*Теорема на Хаусдорф*) Секоја верига од едно подредено множество M, се содржи во некоја максимална верига.

(iv) (*Аксиома на Цермело*) Секое непразно множество M може добро да се подреди.

Решение. Доказот ќе го извршиме, докажувајќи прво дека

(iv) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (iv), а потоа дека (iv) $\Rightarrow$ (i).

1) (iv) $\Rightarrow$ (iii) Нека A е произволна верига во подреденото множество M. Можеме да претпоставиме дека $A \neq M$, зашто, ако $A = M$, A би била максимална. Според (iv), множеството $B = M \setminus A$ може добро да се подреди. Да напомниме дека подредувањата на B и на M не мора да имаат никаква врска.

Множеството B да го разбиеме на две подмножества B_1 и B_2 на следниот начин. Множеството B, како добро подредено, има најмал елемент a. Ако a е споредлив со секој елемент од множеството A, тогаш нека $a \in B_1$; во спротивно нека $a \in B_2$. Ако b е произволен елемент од B, тогаш да претпоставиме дека сите елементи од B, коишто се помали од b, се внесени или во B_1 или во B_2. Ако b е споредлив со сите елементи од A и со сите елементи од B_1, тогаш нека $b \in B_1$; во спротивно нека $b \in B_2$.

Нека $C = A \cup B_1$; кои било два елементи од C се споредливи, па значи C е верига. Но таа верига е и максимална, бидејќи секој елемент од B_2 е неспоредлив со барем еден елемент од C.

2) (iii) $\Rightarrow$ (ii) Нека M е подредено множество во кое секоја верига има мајорант. Ќе покажеме дека во M има барем еден максимален елемент. Нека a е произволен елемент од M. Множеството $\{a\}$ е верига во M, па според (iii), таа се содржи во максимална верига C. Ако c е мајорант за веригата C, тогаш $a \leq c$. Ќе покажеме дека c е максимален елемент во M.

Навистина, ако постои $b \in M$, таков што $c < b$, тогаш за секој $x \in C$ ќе имаме $x < b$, па $C \cup \{b\}$ ќе биде верига во која се содржи C, спротивно на тоа што C е максимална верига. Значи, c е максимален елемент во M, т.е. во M постои барем еден максимален елемент.

3) (ii) $\Rightarrow$ (iv) Нека M е произволна множество, а U ги содржи оние подмножества од M, коишто се добро подредени. Јасно е дека $U \neq \emptyset$, зашто барем едноелементните подмножества од M му припаѓаат на U. Ако $X, Y \in U$ и ако $X \subseteq Y$, а подредувањето на X се

совпаѓа со подредувањето на Y, ќе ставиме $X \leq Y$. Лесно се проверува дека така дефинираната релација е подредување во U. Нека $\{C_i \mid i \in I\}$ е верига во U, а $D = \bigcup_i C_i$. Во D постои подредување, коешто на секое C_i го индуцира даденото подредување. Но, D е добро подредено. Навистина, нека $A \subseteq D$, $A \neq \emptyset$ и $x \in A$; тогаш $x \in C_i$ за некое $i \in I$, па значи $A \cap C_i \neq \emptyset$. Ако a е најмал елемент во $A \cap C_i$ (таков елемент постои, зошто C_i е добро подредено), тогаш a е најмал елемент и во A. Значи, $D \in U$ и е мајорант за веригата $\{C_i \mid i \in I\}$. Според (ii), во U постои макси-мален елемент B.

Ако $B \neq M$, нека $c \in M \setminus B$. Да го разгледаме множеството $B^* = B \cup \{c\}$, заедно со подредувањето од B и ставајќи $x < c$, за секој $x \in B$. На тој начин B^* е добро подредено и $B < B^*$, спротивно на претпоставката дека B е максимален елемент во U. Значи, имаме $B = M$, т.е. M може добро да се подреди.

(iv) $\Rightarrow$ (i) Нека M е дадено множество, коешто според (iv), можеме да го сметаме за добро подредено. Дефинираме $f : \mathbb{P}(M) \to M$, на следниов начин:

$f(A) = a \Leftrightarrow a$ е најмал елемент во A.

Јасно е дека f е пресликување и притоа $f(A) \in A$, т.е. точна е аксиомата за избор.

(За (i) $\Rightarrow$ (iv), види Г.Чупона, Б.Трпеновски: "Предавања по алгебра", кн.II, стр.32–33.)

4.40. Нека $a, b \in A$, $a \neq b$ и нека M е множеството од сите еквивалентности на A што ги раздвојуваат елементите a и b, т.е. $\alpha \in M \Leftrightarrow a \; \alpha' \; b$. Со помош на лемата на Цорн, а потоа и директно, да се покаже дека во M има барем еден максимален елемент. Во случај да е $A = \{a, b, c\}$, да се најде множеството M.

Решение. Релацијата $\beta = \{(a, a)\} \cup (B \times B), B = A \setminus \{a\}$, (1)
е еквивалентност на A што ги раздвојува елементите a и b, па значи M не е празно. За да покажеме дека во M има барем еден максимален елемент користејќи ја лемата на Цорн, треба да покажеме дека секоја верига во M е мајорирана. Нека $\{\alpha_i \mid i \in I\}$ е верига во M и $\alpha = \bigcup_i \alpha_i$.Бидејќи $\{\alpha_i \mid i \in I\}$ е верига, следува дека α е еквивалентност во A, а бидејќи $a \alpha_i' b$ за секој $i \in I$, следува дека $\alpha \in M$. Но α е мајорант за веригата $\{\alpha_i \mid i \in I\}$, па значи во M има барем еден максимален елемент.

Ова може да се покаже и директно. На пример, еквивалентноста β, дефинирана со (1), е максимален елемент во M. Во M максимален елемент е секоја еквивалентност α, таква што $M/_\alpha = \{a^\alpha, b^\alpha\}$ е двоелементно множество. Ако $A = \{a, b, c\}$, тогаш елементи на M се:

$\alpha_1 = \Delta_A$, $\alpha_2 = \Delta_A \cup \{(a, c), (c, a)\}$, $\alpha_3 = \Delta_A \cup \{(b, c), (c, b)\}$.

Еквивалентностите α_2 и α_3 се максимални елементи во M.

§ 5. ПОЛУГРУПИ

5.1. Дали $\mathbb{Z}(\circ)$ е групоид, ако операцијата "$\circ$" е дефинирана со:

а) $a \circ b = \sqrt{a+b}$; б) $a \circ b = (a+b)^2$; в) $a \circ b = a - b - ab$;

г) $a \circ b = 0$; д) $a \circ b = a$?

Одговор. а) Не. б) – д) Да.

5.2. Во $\mathbb{N}$ е дефинирана операција " $*$ " со: $a * n = a^n$.

а) Да се покаже дека $\mathbb{N}(*)$ не е полугрупа.

б) Да се најдат сите тројки (m, n, p) за кои важи

$m*(n * p) = (m * n)* p$.

Решение. а) $\mathbb{N}(*)$ не е полугрупа, бидејќи, на пример,

$2*(1 * 3) = 2 * 1^3 = 2 * 1 = 2^1 = 2$,

$(2 * 1)*3 = 2^1 * 3 = 2 * 3 = 2^3 = 8$.

б) $(1, n, p)$, $(m, n, 1)$ и $(m, 2, 2)$, каде што m, n и p се произволни елементи од $\mathbb{N}$.

5.3. Во множеството $\mathbb{Q}$ е дефинирана операција "$\circ$" со:

$a \circ b = a + b + ab$. Да се најде неутралниот елемент. Кои елементи се инверзибилни?

Решение. Неутрален елемент е 0, бидејќи

$a \circ 0 = a + 0 + a \cdot 0 = a$ и $0 \circ b = 0 + b + 0 \cdot b = b$.

За да видиме кои елементи од $\mathbb{Q}$ се инверзибилни, потребно е за $a \in \mathbb{Q}$, да најдеме $x \in \mathbb{Q}$, таков што $a \circ x = 0 = x \circ a$. Бидејќи $a \circ x = a + x + ax$, елементот x мора да ја задоволува равенката $a + x + ax = 0$, односно $(a + 1)x = -a$;

За $a = -1$ имаме $0 = -1$, па значи елементот -1 не е инверзибилен. Ако $a \neq -1$, тогаш $x = -\frac{a}{a+1} \in \mathbb{Q}$ и имаме

$a \circ (-\frac{a}{a+1}) = (-\frac{a}{a+1}) \circ a = 0$, т.е. секој $a \neq -1$ е инверзибилен во групоидот $\mathbb{Q}(\circ)$.

5.4. Во множеството $\mathbb{Z}$ дефинираме операција "$\circ$" со: $a \circ b = a + b - ab$. Да се покаже дека $\mathbb{Z}(\circ)$ е полугрупа со единица. Кои елементи се инверзибилни?

Решение. Ако $a, b \in \mathbb{Z}$, тогаш и $a + b - ab \in \mathbb{Z}$, па значи $\mathbb{Z}(\circ)$ е групоид. Ако сега $a, b, c \in \mathbb{Z}$, имаме:

$$(a \circ b) \circ c = (a + b - ab) \circ c = a + b - ab + c - (a + b - ab)c =$$
$$= a + b + c - ab - ac - bc + abc =$$
$$= a + (b + c - bc) - a(b + c - bc) = a \circ (b + c - bc) =$$
$$= a \circ (b \circ c),$$

т.е. $\mathbb{Z}(\circ)$ е полугрупа. Неутрален елемент во $\mathbb{Z}(\circ)$ е 0.

Ако a е инверзибилен елемент во $\mathbb{Z}(\circ)$, тогаш од равенството $a + x - ax = 0$ следува дека и $x = \frac{a}{a-1} \in \mathbb{Z}$. Значи, за да ги најдеме инверзибилните елементи, потребно е да видиме за кои $a \in \mathbb{Z}$, и бројот $\frac{a}{a-1} \in \mathbb{Z}$. Јасно е дека треба да биде $a \neq 1$ и дека 0 и 2 се инверзибилни. За секој друг a, броевите a и $a - 1$ се заемно прости, па значи 0 и 2 се единствените инверзибилни елементи во $\mathbb{Z}(\circ)$.

5.5. Во множеството $\mathbb{R}^+$ дефинираме операција "$\circ$" со:

$$a \circ b = \sqrt[n]{a^n + b^n}\ .$$

Да се најде неутралниот елемент во $\mathbb{R}^+(\circ)$. Кои елементи се инверзибилни?

5.6. Во $\mathbb{R}^*$ дефинираме операција "$\circ$" со: $a \circ b = |a|b$.

Да се покаже дека $\mathbb{R}^*(\circ)$ е некомутативна полугрупа со две леви единици.

5.7. Во множеството $G = \mathbb{R} \times \mathbb{R}$ дефинираме операција "$\circ$" со:
$(a, b) \circ (c, d) = (ac, bc + d)$.
Дали $G(\circ)$ е полугрупа? Дали е комутативна?

Одговор. Некомутативна полугрупа.

5.8. Во $\mathbb{R}$ е дефинирана операција "$\circ$" со: $a \circ b = |a - b|$. Да се покаже дека $\mathbb{R}(\circ)$ не е полугрупа.

5.9. Во множеството $G = \mathbb{R}^+ \cup \{0\}$ дефинираме операција"$\otimes$" со:

а) $a \otimes b = \max\{a, b\}$ б) $a \otimes b = \min\{a, b\}$

Да се покаже дека $G(\otimes)$ е полугрупа. Дали има единица, и ако има, кои елементи се инверзибилни?

Решение. а) Единица е 0, и тој е единствениот инверзибилен елемент.
б) Нема единица.

5.10. Во множеството $G = \mathbb{N}^0 \times \mathbb{N}^0$ дефинираме операција "$\otimes$" со:
$(i, j) \otimes (m, n) = (i + m, 2^m j + n)$.

Да се покаже дека $G(\otimes)$ е полугрупа со единица. Кои елементи се инверзибилни?

Ако наместо $\mathbb{N}^0$ се земе $\mathbb{Z}$, да се најдат инверзибилните елементи во полугрупата $\mathbb{Z} \times \mathbb{Z}(\otimes)$.

Решение. Лесно се покажува дека $G(\otimes)$ е полугрупа и дека $(0, 0)$ е единица.

Да видиме кои елементи се инверзибилни. Од равенството

$(x, y) \otimes (m, n) = (0, 0)$

следува $x + m = 0$ и $2^m y + n = 0$ т.е. $x = -m$ и $y = -2^{-m} + n$. Броевите $-m$ и $-2^{-m} + n$ му припаѓаат на $\mathbb{N}^0$ само за $m = n = 0$, што значи дека само $(0, 0)$ е инверзибилен.

Во полугрупата $\mathbb{Z} \times \mathbb{Z}$ $(\otimes)$ инверзибилни елементи се (m,n), $m \in \mathbb{Z}^-$, $n \in \mathbb{Z}$ и $(m, 2^m k)$, $k, m \in \mathbb{Z}$.

5.11. Да дефинираме операција "$\odot$" во $\mathbb{C}^2$ со:
$(z_1, z_2) \odot (w_1, w_2) = (z_1 w_1 - z_2 \overline{w}_2, z_1 w_2 + z_2 \overline{w}_1)$,
каде што $z_1, z_2, w_1, w_2 \in \mathbb{C}$. Да се покаже дека $\mathbb{C}^2(\odot)$ е некомутативна полугрупа со единица. Кои елементи се инверзибилни ?

Решение. Лесно се проверува дека $\mathbb{C}^2(\odot)$ е некомутативна полугрупа со единица, при што единица е елементот (1,0).

Елементот (a, b), $a = a_1 + a_2 i$, $b = b_1 + b_2 i$, е инверзибилен ако и само ако

$$\Delta = \begin{vmatrix} a_1 & -a_2 & -b_1 & -b_2 \\ a_2 & a_1 & -b_2 & b_1 \\ b_1 & b_2 & a_1 & -a_2 \\ b_2 & -b_1 & a_2 & a_1 \end{vmatrix} \neq 0.$$

Бидејќи $\Delta = (a_1^2 + a_2^2 + b_1^2 + b_2^2)^2$, добиваме дека секој елемент $(a, b) \neq (0, 0)$ е инверзибилен во $\mathbb{C}^2(\odot)$.

5.12. Во множеството $\mathcal{J}$ од сите трансформации во $\mathbb{R}$ дефинираме операција "+" со:

$f+g=h \Leftrightarrow (\forall a\in\mathbb{R})\ h(a)=f(a)+g(a)$.

Да се покаже дека $\mathcal{J}(+)$ е групоид со неутрален елемент и да се покаже дека секој елемент е инверзибилен.

Решение. Ако $f, g \in \mathcal{J}$, тогаш јасно е дека и $f+g \in \mathcal{J}$, па значи $\mathcal{J}(+)$ е групоид.

Ако $\omega : \mathbb{R} \to \mathbb{R}$ го дефинираме со: $(\forall r \in \mathbb{R})\ \omega(r)=0$,
тогаш имаме

$(f+\omega)(r)=f(r)+\omega(r)=f(r)+0=f(r)=0+f(r)=$
$=\omega(r)+f(r)=(\omega+f)(r)$,

што значи дека

$f+\omega=\omega+f=f$,

т.е. ω е неутрален елемент во $\mathcal{J}$.

Нека сега $f\in\mathcal{J}$ и нека f е инверзибилен во $\mathcal{J}$. Значи, постои $g\in\mathcal{J}$ така што $f+g=\omega$, т.е. $f(a)+g(a)=\omega(a)=0$. Одовде следува дека $g(a)=-f(a)$. Но, за секое $f\in\mathcal{J}$ можеме да го дефинираме пресликувањето $g:\mathbb{R}\to\mathbb{R}$ со

$(\forall a\in\mathbb{R})\ g(a)=-f(a)$,

и притоа имаме $f+g=g+f=\omega$, а тоа пак значи дека секој елемент од $\mathcal{J}$ е инверзибилен.

5.13. Нека $A=\{1, 2, 3, 4, 5\}$, $B=\{1, 2\}$, а $G=B^A$. Дали G во однос на операцијата множење на пресликувања е полугрупа со единица?

Решение. Не е, бидејќи не е групоид.

5.14. Ако X е непразно множество, тогаш $\mathcal{J}_X$ е полугрупа со единица, и притоа $f\in\mathcal{J}_X$ е инверзибилен, ако и само ако f е биекција.

Решение. Ако f и g се трансформации на X, тогаш и производот fg е трансформација на X, а ако $f, g, h\in\mathcal{J}_X$, тогаш и производите $f(gh)$, $(fg)h\in\mathcal{J}_X$, а бидејќи за произволни пресликувања важи асоцијативниот закон, имаме $f(gh)=(fg)h$, па значи $\mathcal{J}_X$ е полугрупа. Трансформацијата 1_X е единица во $\mathcal{J}_X$.

Да ги најдеме инверзибилните елементи во $\mathcal{J}_X$. Јасно е дека, ако f е биекција, тогаш f е инверзибилен. Обратно, нека f е инверзибилен. Тоа значи дека постои единствена трансформација g, така што $fg=gf=1_X$. Бидејќи 1_X е сурјекција и инјекција,

тогаш од $fg = 1_X$ следува дека f е сурјекција (види 2.19.), а од $gf = 1_X$ следува дека f е инјекција (види 2.19.). Значи f е биекција.

5.15. Дадено е множеството $X = \{1,2\}$. Да се најде полугрупата $\mathcal{J}_X$ и инверзибилните елементи во $\mathcal{J}_X$.

Решение. Елементите на $\mathcal{J}_X$ се 1_X; $f: 1 \to 1,\ 2 \to 1$; $g: 1 \to 2,\ 2 \to 2$; $h: 1 \to 2,\ 2 \to 1$. Инверзибилните елементи се 1_X и h.

5.16. Дадено е множеството $X = \{1, 2, 3\}$. Да се најдат инверзибилните елементи во полугрупата $\mathcal{J}_X$.

Одговор. 1_X; $f_1: 1 \to 2,\ 2 \to 3,\ 3 \to 1$; $f_2: 1 \to 3,\ 2 \to 1,\ 3 \to 2$;

$f_3: 1 \to 1,\ 2 \to 3,\ 3 \to 2$; $f_4: 1 \to 3,\ 2 \to 2,\ 3 \to 1$;

$f_5: 1 \to 2,\ 2 \to 1,\ 3 \to 3$.

5.17. Да се определат сите трансформации f на $A = \{a, b, c\}$, коишто ја имаат особината $ff = f$.

Решение. Такви трансформации ги има 10 и тоа се :

	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}
$a\to$	a	a	a	a	a	b	c	a	b	c
$b\to$	b	b	b	a	c	b	b	a	b	c
$c\to$	c	a	b	c	c	c	c	a	b	c

5.18. Ако A е конечно множество со n елементи, да се покаже дека множеството од сите трансформации f на A, со особината $ff = f$, има

$$\sigma(n) = \sum_{k=1}^{n} \binom{n}{k} k^{n-k}$$

елементи.

Решение. Нека B е подмножество од A со k елементи и нека $C = A \setminus B$. Ако $g: C \to B$ е произволно пресликување и ако пресликувањето $f: A \to A$ се дефинира со

$$f(x) = \begin{cases} x, & \text{ако } x \in B \\ g(x), & \text{ако } x \in C, \end{cases}$$

тогаш f е трансформација на A, со особината $ff = f$. Ако $g_1 \neq g_2$, тогаш и $f_1 \neq f_2$ па значи, при фиксирано B, постојат k^{n-k} различни трансформации. Понатаму јасно е дека, ако B_1 и B_2 се различни подмножества, не може да се добие иста трансформација f. Според тоа, постојат барем $\sigma(n)$ трансформации f на A со особината $ff = f$.

Нека, сега, f е произволна трансформација на A со особината $ff = f$. Ставајќи $B = f(A)$, добиваме $f_B = 1_B$, па f може да се добие, на погоре опишаниот начин, од подмножеството $B = f(A)$ и пресликувањето $g = f_{A\setminus B}$. Значи постојат точно $\sigma(n)$ трансформации f на A со особината $ff = f$.

5.19. Групоидот G $(\cdot)$ е полугрупа ако и само ако секоја лева транслација γ комутира со секоја десна транслација δ.

Решение. Ако групоидот G е полугрупа, тогаш имаме:

$$\gamma_a \delta_b(c) = \gamma_a(\delta_b(c)) = \gamma_a(cb) = a(cb) = (ac)b$$
$$= \delta_b(ac) = \delta_b(\gamma_a(c)) = \delta_b \gamma_a(c), \text{ т.е.}$$
$$(\forall a, b \in G)\ \gamma_a \delta_b = \delta_b \gamma_a. \qquad (1)$$

Обратно, нека е исполнет условот (1). Тогаш имаме:

$(c \in G)\ \gamma_a\delta_b(c) = \delta_b\gamma_a(c)$, т.е. $a(cb) = (ac)b$,

што значи дека G е полугрупа.

5.20. Да се покаже дека групоидот G е полугрупа ако и само ако е исполнет кој било од условите:

а) $(\forall a, b \in G)\ \gamma_a \gamma_b = \gamma_{ab}$;

б) $(\forall a, b \in G)\ \delta_a \delta_b = \delta_{ba}$.

Решение. а) Да препоставиме прво дека G е полугрупа. Тогаш имаме

$(\forall x \in G)\ \gamma_a \gamma_b(x) = \gamma_a(\gamma_b(x)) = \gamma_a(bx) = a(bx) = (ab)x = \gamma_{ab}(x)$, т.е.

$\gamma_a\gamma_b = \gamma_{ab}$.

Обратно, нека е $\gamma_a \gamma_b = \gamma_{ab}$ за секои $a, b \in G$. Тоа значи дека $\gamma_a \gamma_b(x) = \gamma_{ab}(x)\ \forall x \in G$, т.е. $a(bx) = (ab)x$, што значи дека G е полугрупа.

5.21. Ако G е полугрупа, тогаш множеството од сите леви (десни) транслации е полугрупа.

Решение. Да покажеме дека, ако G е полугрупа, тогаш и множеството $L = \{\gamma_a \mid a \in G\}$ од сите леви транслации е полугрупа.

Да забележиме прво дека

$$\gamma_a\gamma_b = \gamma_{a\,b}. \tag{1}$$

Навистина, имаме:

$\gamma_a\gamma_b(x) = \gamma_a(\gamma_b(x)) = \gamma_a(bx) = a(bx) = (ab)x = \gamma_{ab}(x)$.

Потоа според (1), имаме:

$\gamma_a(\gamma_b\gamma_c) = \gamma_a\gamma_{bc} = \gamma_{a\,(bc)} = \gamma_{(ab)c} = \gamma_{ab}\gamma_c = (\gamma_a\gamma_b)\gamma_c$,

т.е. L е полугрупа.

5.22. Елементот z од групоидот G велиме дека е *лев* (*десен*) *анулатор* во G, ако

$(\forall x \in G)\ zx = z\ \ (xz = z)$.

а) Да се даде пример на групоид со повеќе леви анулатори.

б) Да се покаже дека, ако во групоидот G, z_1 е лев, а z_2 десен анулатор, тогаш $z_1 = z_2$ и за него велиме дека е *анулатор* во G.

Решение. а) Нека S е непразно множество и нека дефинираме операција "$*$" со:

$(\forall x, y \in S)\ x * y = x$.

Јасно е дека $S(*)$ е групоид, при што секој елемент од S е лев анулатор во S.

б) Ако z_1 е лев, а z_2 десен анулатор, тогаш имаме $z_1 = z_1 z_2 = z_2$.

5.23. Да се определат левите анулатори на полугрупата $\mathcal{J}_A$ од трансформации на множеството A. Во кој случај $\mathcal{J}_A$ има и десен анулатор?

Решение. Нека A е дадено множество. Елементот $\omega \in \mathcal{J}_A$ ќе биде лев анулатор во $\mathcal{J}_A$, ако за секое $f \in \mathcal{J}_A$ е исполнето равенството

$$\omega f = \omega \tag{1}$$

Ако $a, b \in A$ се произволни елементи, а $g : A \to A$ е дефинирано со

$$g(x) = \begin{cases} a \text{ за } x = b \\ \text{произволно за } x \neq b. \end{cases}$$

тогаш (1) е исполнет и за g, па имаме

$\omega(b) = \omega g(b) = \omega(a)$ т.е. $\omega(a) = \omega(b)$.

Ако a и b се менуваат во A, тогаш и пресликувањето g се менува, па добиваме дека

$(\forall x, y \in A)\ \omega(x) = \omega(y)$,

т.е. ω е константно пресликување.

Бидејќи секое константно пресликување ω е и лев анулатор, заклучуваме дека трансформацијата $\omega \in \mathcal{J}_A$ е лев анулатор, ако и само ако ω е константно пресликување.

Да видиме во кој случај $\mathcal{J}_A$ има десни анулатори. Ако $A = \{a\}$ е едноелементно множество, тогаш и $\mathcal{J}_A = \{1_A\}$ е едноелементно множество и притоа имаме $1_A 1_A = 1_A$, т.е. $\mathcal{J}_A$ има десни анулатори.

Да претпоставиме сега дека A има барем два елемента a и b. Ако $\omega \in \mathcal{J}_A$ е десен анулатор, тогаш имаме

$$(\forall f \in \mathcal{J}_A)\ f\omega = \omega, \tag{2}$$

па ако f_1 е константно пресликување, од (2) добиваме:

$$\omega(x) = f_1\omega(x) = f_1\omega(y) = \omega(y),$$

т.е. и ω е константно пресликување. Значи, ако ω е десен анулатор во $\mathcal{J}_A$, тогаш ω мора да е константно пресликување. Затоа нека ω е константно пресликување, на пример дефинирано со:

$$(\forall x \in A)\ \omega(x) = a,$$

а f_2 нека е дефинирано со

$$(\forall x \in A)\ f_2(x) = b.$$

Тогаш имаме

$$\omega(a) = f_2\omega(a) = f_2(a) = b,$$

т.е. ω не е десен анулатор. Значи, ако A има барем два елемента, тогаш $\mathcal{J}_A$ нема десни анулатори.

5.24. Нека S е полугрупа со својството:

$(\forall a \in S)\ (\exists x, y \in S)\ (xa)a = a,\ a(ay) = a.$

Да се докаже дека:

а) $(\forall a \in S)\ (\exists e_a \in S)\ e_a a = a e_a = a$;

б) $(\forall a \in S)\ (\exists b_a \in S)\ a b_a = b_a a = e_a$.

Решение. а) Нека $a \in S$ и $xaa = a = aay$. Ако ставиме $e_a = xa = xaay = ay$, тогаш имаме $e_a a = xaa = a = aay = a e_a$.

б) Нека сега $b_a = xxa = xay = ayy$. Тогаш имаме:

$b_a a = xxaa = xa = e_a = ay = aayy = a b_a$.

5.25. Нека G е полугрупа, а a и b фиксни елементи од G, такви што

$(\forall x \in G)\ axb = x.$

Да се покаже дека во тој случај важи:

$(\forall x \in G)\ bxa = x,$

и дека $ab = ba$ е единица во G.

Решение. Имаме:

$ab = (aab)\,(abb) = a(abab)b = abab = a(ba)b = ba.$

Понатаму:

$abx = a(abx)b = (aab)xb = axb = x,$

$xab = a(xab)b = ax(abb) = axb = x.$

Значи, $ab = ba$ е единица во G. На крајот имаме:

$bxa = a(bxa)b = (ab)\,x\,(ab) = x.$

5.26. Ако S е непразно подмножество од полугрупата G, да се покаже дека постои најмала потполугрупа $[S]$ од G во која се содржи S.

Решение. Нека $\{G_i \mid i \in I\}$ е фамилија од сите потполугрупи што го содржат S. Оваа фамилија не е празна, зашто една таква потполугрупа е полугрупата G. Да ставиме:

$$[S] = \bigcap_i G_i$$

Јасно е дека $[S]$ е потполугрупа од G и дека $S \subseteq [S]$. Ако H е потполугрупа што го содржи S, тогаш $H = G_i$, за некој $i \in I$, па $[S] \subseteq H$, значи дека $[S]$ е најмалата потполугрупа што го содржи S.

5.27. Ако $A = \{1, 3, 5, \ldots\}$, да се најдат $[A]$ во:

а) $\mathbb{Z}(+)$; б) $\mathbb{Z}(\cdot)$.

Одговор. а) $[A] = \mathbb{N}$. б) $[A] = A$.

5.28. Подмножество S од полугрупата G се вика:

а) *лев идеал*, ако $(s \in S, g \in G) \Rightarrow gs \in S$;

б) *десен идеал*, ако: $(s \in S, g \in G) \Rightarrow sg \in S$;

в) *идеал*, ако S е и лев, и десен идеал.

Да се покаже дека секој лев, десен односно идеал во G е потполугрупа од G.

5.29. Нека G е полугрупа, а $\{S_i \mid i \in I\}$ е фамилија од леви, десни односно идеали во G. Да се покаже дека, ако $\bigcap_i S_i \neq \varnothing$, тогаш $S = \bigcap_i S_i$ е исто така лев, десен, односно идеал во G.

5.30. Ако R е непразно подмножество од полугрупата G, да се покаже дека постои:

а) најмал лев идеал $[R]_S$, таков што $R \subseteq [R]_S$.

б) најмал десен идеал $[R]_d$ таков што $R \subseteq [R]_d$.

в) најмал идеал $[R]$, таков што $R \subseteq [R]$.

Решение. а) Нека R е непразно множество од полугрупата G и нека $\{R_i \mid i \in I\}$ е фамилијата од сите леви идеали во G, такви што $R \subseteq R_i$, за секој $i \in I$. Јасно е дека оваа фамилија не е празна, зашто еден таков идеал е и самата полугрупа G. Да ставиме

$$[R]_S = \bigcap_i R_i \ .$$

Според претходната задача, $[R]_S$ е исто така лев идеал и притоа имаме $R \subseteq [R]_S$. Ако S е друг лев идеал во својството $R \subseteq S$, тогаш $S = R_i$ за некој $i \in I$, па значи имаме $[R]_S \subseteq S$, т.е. $[R]_S$ е најмалиот лев идеал со својството $R \subseteq [R]_S$.

5.31. При ознката од претходната задача, да се покаже дека:

а) $[R]_S = R \cup GR$;

б) $[R]_d = R \cup RG$;

в) $[R] = R \cup RG \cup GR \cup GRG$,

каде што, на пример, $GR = \{gr \mid g \in G, r \in R\}$.

Решение. а) Нека $S = R \cup GR$; да покажеме дека S е лев идеал во G.

Нека $s \in S$, $g \in G$; тогаш имаме: $s \in R$ или $s \in GR$. Ако $s \in R$, тогаш $gs \in GR$, па значи $gs \in S$. Ако пак $s \in GR$ тогаш $s = g_1 r$ за некој $g_1 \in G$ и $r \in R$, па имаме:

$$gs = g(g_1 r) = (gg_1)r \in GR,$$

т.е. $gs \in S$. Значи S е лев идеал во G и притоа $R \subseteq R \cup GR$.

Нека S_1 е друг лев идеал во G со својството $R \subseteq S_1$. Ако $r \in R$, $g \in G$, ќе имаме $r \in S_1$ и $g \in G$, па $gr \in S_1$, т.е. $GR \subseteq S_1$. Од тоа следува дека

$S = R \cup GR \subseteq S_1$, па $S = [R]_S$.

5.32. Нека G е полугрупа. За идеалот P велиме дека е *прост* ако $ab \in P \Rightarrow a \in P$ или $b \in P$.

Нека G го задоволува условот: за секои a, $b \in G$, такви што $b \notin [a]$, постои прост идеал P, таков што $a \in P$, $b \notin P$. Да се докаже дека:

$(\forall x \in G)\ x \in Gx^2G$.

Решение. Нека $x \in G$ и нека S е идеалот генериран од x^2. Според 5.31, имаме

$$S = \{x^2\} \cup x^2G \cup Gx^2 \cup Gx^2G. \qquad (1)$$

Ако $x \in S$, тогаш, според условот на задачата, постои прост идеал P, таков што $x^2 \in P$, $x \notin P$. Но, според дефиницијата на прост идеал, тоа не е можно, па значи $x \in S$. Од (1) имаме дека $x \in \{x^2\}$, или $x \in x^2G$, или $x \in Gx^2$ или $x \in Gx^2G$.

Ако $x \in \{x^2\}$, тогаш е $x = x^2$, па $x = x^4 \in Gx^2G$.
Ако $x \in x^2G$ тогаш постои $u \in G$, таков што
$x = x^2u = x(x^2u)u = x(x^2)u^2$, што значи $x \in Gx^2G$.
Слично, ако $x \in Gx^2$ добиваме дека $x \in Gx^2G$.
Значи, во секој случај, $x \in Gx^2G$.

5.33. Ако G е групоид, тогаш множеството End G од сите ендоморфизми на G е полугрупа со единица.

Решение. Бидејќи производ на хомоморфизми е хомоморфизам следува дека End G е групоид и притоа $1_G \in$ End G. Според 5.14, End G е полугрупа.

5.34. Нека G е полугрупа и $a, b \in G$ се дадени елементи. Пресликувањето $\tau : G \to G$ е дефинирано со: $(\forall x \in G)\ \tau(x) = axb$.
Да се докаже дека следниве услови се еквивалентни:
(i) τ е епиморфизам;
(ii) G има единица $e = ab = ba$;
(iii) τ е автоморфизам.

Решение. (i) $\Rightarrow$ (ii). Бидејќи τ е епиморфизам, тој како пресликување е сурјекција, па за секој $x \in G$, постои барем еден $y \in G$, таков што $x = \tau(y)$. Тогаш имаме:

$\tau(a)x = \tau(a) \cdot \tau(y) = \tau(ay) = aayb = a\tau(y) = ax$, па значи

$$aabx = ax \tag{1}$$

Слично добиваме:

$$xabb = xb. \tag{2}$$

Од (1) или (2) имаме $\tau(ab) = aabb = ab$; според (1) добиваме:
$(ab)x = \tau(ab)\ \tau(y) = \tau(aby) = aabyb = (aaby)b = ayb = \tau(y) = x$,
а според (2):

$x(ab) = \tau(y)\ \tau(ab) = \tau(yab) = ayabb = a(yabb) = ayb = \tau(y) = x$,
т.е ab е единица во G. Потоа имаме:
$ab = abab = \tau(ba) = \tau(b) \cdot \tau(a) = abbaab = (ab)ba(ab) = ba$.

(ii) $\Rightarrow$ (iii). Нека G има единица $ab = ba$. Треба да покажеме дека τ е автоморфизам. Имаме:
$\tau(xy) = axyb = ax(ba)yb = (axb)\ (ayb) = \tau(x) \cdot \tau(y)$,
т.е. τ е ендоморфизам. Ако x е даден елемент од G, да ставиме $y = bxa$. Тогаш
$ayb = a(bxa)b = (ab)x(ab) = x$,
т.е. $\tau(y) = x$, што значи τ е епиморфизам.

Ако $\tau(x_1) = \tau(x_2)$, тогаш по ред имаме

$ax_1b = ax_2b$,

$b(ax_1b)a = b(ax_2b)a$,

$(ba)x_1(ba) = (ba)x_2(ba)$,

т.е. $x_1 = x_2$, што значи τ е мономорфизам.

(iii) $\Rightarrow$ (i) очигледно.

5.35. Нека G е групоид и α е конгруенција во G. Ако G е:

а) комутативен; б) асоцијативен; в) со единица; г) со анулатор, тогаш истата особина ја има и фактор-групоидот $G/_\alpha$.

Решение. Нека групоидот G е, на пример, асоцијативен и нека a^α, b^α, c^α се произволни елементи од $G/_\alpha$. Имаме:

$$a^\alpha(b^\alpha c^\alpha) = a^\alpha(bc)^\alpha = (a(bc))^\alpha = ((ab)c)^\alpha = (ab)^\alpha c^\alpha = (a^\alpha b^\alpha)c^\alpha,$$

т.е. и $G/_\alpha$ е асоцијативен.

5.36. Да се определи множеството од сите конгруенции, како и соодветните фактор-групоиди, на следниве групоиди:

а)

	e	a
e	e	a
a	a	e

б)

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

в) S_3

Решение: а) Во множеството $G = \{e, a\}$ постојат две еквивалентности Δ_G и $\alpha = G \times G$, а бидејќи еквивалентностите Δ_S и $S \times S$ се конгруенции за секој групоид S, добиваме дека и двете еквивалентности Δ_G, α се конгруенции во G. Соодветните факторгрупоиди се:

$G/_\alpha = \{\{e, a\}\}$, $\quad G/_{\Delta G} = \{\{e\}, \{a\}\}$.

б) Еквивалентности во $G = \{a, e, b\}$ се: $\alpha = \Delta_G \cup \{(a, b), (b, a)\}$, $\beta = \Delta_G \cup \{(e, a), (a, e)\}$, $\gamma = \Delta_G \cup \{(e, b), (b, e)\}$, Δ_G и $G \times G$.

α не е конгруенција бидејќи $a\alpha b$ и $a\alpha a$, но $aa = b$ не е во релација α со $ba = e$. Слично се проверува дека β и γ не се конгруенции. Значи конгруенции се Δ_G и $G \times G$.

в) Елементите на S_3 се: $1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

$$\rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

а мултипликативната шема на S_3 е:

.	1	ρ_1	ρ_2	σ_1	σ_2	σ_3
1	1	ρ_1	ρ_2	σ_1	σ_2	σ_3
ρ_1	ρ_1	ρ_2	1	σ_3	σ_1	σ_2
ρ_2	ρ_2	1	ρ_1	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	1	ρ_1	ρ_2
σ_2	σ_2	σ_3	σ_1	ρ_2	1	ρ_1
σ_3	σ_3	σ_1	σ_2	ρ_1	ρ_2	1

Од сите 203 еквивалентности, колку што ги има во S_3, само три се конгруенции, и тоа двете тривијални, Δ_{S_3} и $S_3 \times S_3$ и една нетривијална,

$\alpha = \Delta_{S_3} \cup \{(1, \rho_1), (1, \rho_2), (\rho_1, 1), (\rho_2, 1), (\rho_1, \rho_2), (\rho_2, \rho_1)\}$.

5.37. Нека $G = G_1 \times G_2$ е директниот производ од групоидите G_1 и G_2, а α_i е конгруенција во групоидот G_i, $i = 1, 2$. Да се покаже дека релацијата α дефинирана со:

$(a_1, a_2)\ \alpha\ (b_1, b_2) \Leftrightarrow a_i \alpha_i b_i,\ \ i = 1, 2,$

е конгруенција во G. Да се обопшти овој резултат .

Решение. Лесно се проверува дека α е еквивалентност во G. Да покажеме дека α е и конгруенција во G.

Затоа нека $(a_1, a_2,)\ \alpha\ (b_1, b_2)$ и $(x_1, x_2)\ \alpha\ (y_1, y_2)$. Тоа значи дека

$a_1\ \alpha_1 b_1,\ a_2 \alpha_2 b_2,\ x_1 \alpha_1 y_1,\ x_2 \alpha_2 y_2.$ (1)

Бидејќи α_i, $i = 1, 2$ е конгруенција во G_i, од (1) следува дека

$a_i x_i \alpha_i b_i\ y_i,\ \ i = 1, 2,$

т.е. $(a_1 x_1, a_2 x_2)\ \alpha\ (b_1 y_1, b_2 y_2)$. Значи, α е конгруенција во G.

Обопштувањето на овој резултат е:

Ако $\{G_i \mid i \in I\}$ е фамилија групоиди, а α_i е конгруенција во G_i, за секој $i \in I$, тогаш релацијата α во директниот производ $G = \prod_i G_i$, дефинирана со

$(a_i)\ \alpha\ (b_i) \Leftrightarrow (\forall i \in I)\ a_i \alpha_i b_i,$ е конгруенција во G.

5.38. Нека групоидот G е определен со:
$(\forall x, y \in G)\ xy = x.$
Да се покаже дека :
а) Секоја трансформација $f \in \mathcal{J}_G$ е ендоморфизам на G.
б) Секоја еквивалентност во G е конгруенција на G.

Решение. а) Ако $f \in \mathcal{J}_G$, тогаш имаме :
$f(xy) = f(x) = f(x) f(y),$
т.е f е ендоморфизам.

б) Нека α е еквивалентност во G и нека $x_1 \alpha x_2$ и $y_1 \alpha y_2$. Бидејќи $x_1 y_1 = x_1$, $x_2 y_2 = x_2$, добиваме дека $x_1 y_1 \alpha x_2 y_2$, т.е. α е когруенција во G.

5.39. Нека G е групоид. Да се покаже дека, ако секоја трансформација на G е ендоморфизам во G, тогаш и секоја еквивалентност во G е конгруенција во G. Дали важи обратното?

Решение. Нека секоја трансформација $f: G \to G$ е ендоморфизам и нека α е еквивалентност во G. Да претпоставиме дека $x \alpha y$ и $u \alpha v$. Од секоја класа еквивалентни елементи по α да фиксираме по еден елемент; ако a е избран елемент од една класа, таа класа ќе ја означиме со a^{α}. Пресликувањето $f: G \to G$, дефинирано со
$(\forall x \in G)\ f(x) = a \Leftrightarrow x \in a^{\alpha},$
според претпоставката, е ендоморфизам. Бидејќи $\alpha = \ker f$, имаме:
$f(xu) = f(x) f(u) = f(y) f(v) = f(yv),$
т.е. $xu\ \alpha\ yv$, а тоа значи дека α е конгруенција.

Обратно, ако секоја еквивалентност во G е конгруенција, тогаш секоја трансформација на G не мора да биде ендоморфизам. За таа цел ќе дадеме два примера.

1) Нека $G = \{a, b\}$ е множество со два елемента. Во G постојат само две еквивалентности Δ_G и $G \times G$, коишто и двете се конгруенции. Но $\mathcal{J}_G$ има 4 елементи и, ако операцијата во G е дефинирана со шемата

	a	b
a	b	a
b	a	a

тогаш за трансформацијата $f: a \to b,\ b \to a$ имаме:
$f(ab) = f(a) = b,\ \ f(a) f(b) = ba = a,$

т.е. f не е ендоморфизам.

2) Ако $G = \{a, b, c\}$ е множество со три елементи и ако во G дефинираме операција со

$(\forall x, y \in G)\ xy = c,$

тогаш во $G(\cdot)$ секоја еквивалентност е и конгруенција, но пресликувањето $f: G \to G$, дефинирано со

$(\forall x \in G)\ f(x) = a,$

не е ендоморфизам, зашто е $f(ab) = f(c) = a,\ f(a)\,f(b) = aa = c.$

5.40. Да се даде карактеристика на класата групоиди, за кои секоја трансформација е ендоморфизам.

Решение. Нека $G(\cdot)$ е групоид за кој секоја трансформација $f \in \mathcal{J}_G$ е ендоморфизам. За секој $a \in G$, пресликувањето $f_a: G \to G$, дефинирано со

$(\forall x \in G)\ f_a(x) = a,$

треба да е ендоморфизам, па имаме:

$a = f_a(xy) = f_a(x)\,f_a(y) = aa.$

Според тоа, за секој $a \in G$ имаме $aa = a.$

Да претпоставиме дека постојат елементи $a, b \in G$, $a \neq b$, такви што $ab = ba = c.$ Пресликувањето $f: G \to G$ дефинирано со :

$$f(x) = \begin{cases} a, & \text{за} \quad x=b \\ b, & \text{за} \quad x=a \\ \neq c, & \text{за} \quad x=c \\ x, & \text{за} \quad x \neq a,b,c, \end{cases}$$

според претпоставката треба да е ендоморфизам, па имаме :

$c = ab = f(b)\,f(a) = f(ba) = f(c),$

спротивно на претпоставката $f(c) \neq c$. Значи, не постојат елементи $a, b \in G,\ a \neq b,$ такви што $ab = ba.$

За кои било елементи $a, b \in G$ избираме пресликување g такво што: $g(x) = g(y) = c$ само за $x = a,\ y = b$, каде што $c = ab$. Имаме

$g(ab) = g(a)\,g(b) = cc = c^2,$

$g(ba) = g(b)\,g(a) = cc = c^2,$

но $ab \neq ba$, па мора да е:

1) $ab = a,\ ba = b;$

2) $ab = b,\ ba = a.$

Значи, за кои било елементи $x, y \in G$ имаме:

$xy = x$ (1) или $xy = y$ (2)

Обратно, ако операцијата во G е дефинирана со (1) или (2), тогаш од 5.38. следува дека секоја трансформација на G е ендоморфизам.

5.41* Да се окарактеризира класата групоиди за кои секоја еквивалентност е конгруенција.

5.42. Да се докаже дека релацијата "изоморфизам" во класата групоиди е еквивалентност.

5.43. Ако операциите "$\circ$" и "$*$" во $\mathbb{Z}$ се дефинирани со:

$a \circ b = a + b + ab$,

$a * b = a + b - ab$,

да се докаже дека групоидите $\mathbb{Z}(\circ)$ и $\mathbb{Z}(*)$ се изоморфни.

Решение. Пресликувањето $f: \mathbb{Z} \to \mathbb{Z}$ дефинирано со

$(\forall a \in \mathbb{Z})\ f(a) = -a$,

е биекција и притоа имаме:

$$f(a \circ b) = f(a + b + ab) = -(a + b + ab) = -a + (-b) - (-a)(-b) =$$
$$= f(a) + f(b) - f(a)f(b) = f(a) * f(b).$$

Значи, f е изоморфизам од $\mathbb{Z}(\circ)$ на $\mathbb{Z}(*)$.

5.44. Секоја полугрупа $G(\cdot)$ може изоморфно да се вложи во полугрупата $\mathcal{J}_G$.

Решение. Да претпоставиме прво дека полугрупата G е со единица. Бидејќи важи равенството $\gamma_a\gamma_b = \gamma_{ab}$ (види 5.20.), преслукувањето $f: G \to \mathcal{J}_G$ дефинирано со

$f(a) = \gamma_a$

е хомоморфизам. Бидејќи f е и инјекција, тоа е мономорфизам, т.е. полугрупата $G(\cdot)$ изоморфно се вложува во полугрупата $\mathcal{J}_G$.

Ако пак полугрупата G е без единица, тогаш додавајќи му на G еден елемент e, и ставајќи

$(\forall a \in G)\ ea = ae = a$,

добиваме полугрупа $G' = G \cup \{e\}$ и притоа G е потполугрупа од G'. Ако $f': G' \to \mathcal{J}_{G'}$ е мономорфизам конструиран како f погоре, а $g: G \to G'$ дефиниран со $(\forall a \in G)\ g(a) = a$, кој што е исто така мономорфизам, добиваме мономорфизам

$f'g: G \to \mathcal{J}_{G'}$:

Значи, секоја полугрупа изоморфно се вложува во некоја полугрупа од трансформации.

5.46. Нека $G = \{e, a, b\}$, а операција во G е дефинирана со

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Да се покаже дека G е полугрупа со единица, и да се најде потполугрупата од $\mathcal{J}_G$ изоморфна со G.

Решение. Со директна проверка (од шемата) се покажува дека G е полугрупа со единица e.

Според претходната задача, G е изоморфна со потполугрупата $\{\gamma_e, \gamma_a, \gamma_b\}$ од $\mathcal{J}_G$, каде што e:

$\gamma_e = 1_G$; $\quad \gamma_a : e \to a,\ a \to b,\ b \to e$; $\quad \gamma_b : e \to b,\ a \to e,\ b \to a$.

5.47. Нека G е комутативна полугрупа во која секој елемент е *идемпотент*, т.е $(\forall x \in G)\ xx = x$.

Да се покаже дека G изоморфно се вложува во полугрупата $\mathbb{P}^*(G)(\cap)$, каде што $\mathbb{P}^*(G) = \mathbb{P}(G) \setminus \{\varnothing\}$.

Решение. За секој елемент $a \in G$, да ставиме

$A_a = \{b \mid (\exists x \in G)\ ax = b\}$.

Бидејќи G е комутативна, имаме:

$A_{ab} = \{c \mid (\exists x \in G)\ abx = c\} \subseteq A_a \cap A_b$.

Ако пак $d \in A_a \cap A_b$, тогаш постојат елементи $x, y \in G$, такви што $ax = d$ и $by = d$. Бидејќи G е комутативна, од $ax = by$ добиваме

$abx = bax = bby = by = d$, т.е. $d \in A_{ab}$. Значи

$A_{ab} = A_a \cap A_b$,

т.е. пресликувањето $f : G \to \mathbb{P}^*(G)$ дефинирано со $f(a) = A_a$ е хомоморфизам.

Нека $A_a = A_b$; бидејќи $bb = b$, имаме $b \in A_b = A_a$, т.е. постои $x \in G$, таков што $ax = b$. Аналогно, постои $y \in G$, таков што $by = a$.

Одовде добиваме $a = axy$, $b = bxy$, т.е.

$a = axy = by\ xy = bx\ yy = bxy = b$,

а тоа значи дека хомоморфизмот f е мономорфизам.

5.48. Нека во $M = \{0, 1\}$ е дефинирана операцијата "$\cdot$" со:

$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0,\ 1 \cdot 1 = 1$.

Да се покаже дека секоја комутативна полугрупа G во која секој елемент е идемпотент, изоморфно се вложува во некој директен степен од полугрупата M.

Решение. Според претходната задача можеме да сметаме дека G е потполугрупа од $\mathbb{P}^*(G)$ $(\cap)$. На секој елемент $x \in G$ да му придружиме примерок M_x од полугрупата M и да го формираме директниот производ

$$P = \prod_{x \in G} M_x .$$

Елементите на P се пресликувања f од G во M. На секое подмножество A од G му одговара карактеристичната функција

$$f_A : \begin{cases} f_A(x) = 0 & \text{ако } x \notin A \\ f_A(x) = 0 & \text{ако } x \in A \end{cases}$$

Со кореспонденцијата $A \to f_A(x)$ е определено пресликување f од G во P. Бидејќи на пресекот $A \cap B$ $(A, B \subseteq G)$ му одговара производ на соодветните карактеристични функции, $f_A(x)f_B(x)$ во P, добиваме дека f е хомоморфизам, а бидејќи од $f_A(x) = f_B(x)$ следува $A = B$, добиваме дека f е инјекција. Значи, G изоморфно е вложена во P.

5.49. Нека G_1, G_2 и G се три групоиди, такви што:

(i) постојат хомоморфизми $f_i : G \to G_i$ $(i = 1, 2)$;

(ii) ако S е групоид и $g_i : S \to G_i$ $(i = 1, 2)$

се хомоморфизми, тогаш постои еднозначно определен хомоморфизам $g : S \to G$, таков што $g_i = f_i g$.

Да се покаже дека G е изоморфен со директниот производ $G_1 \times G_2$. Да се обопшти овој резултат.

Решение. Нека $S = G_1 \times G_2$. Бидејќи проекциите $\pi_i : G_1 \times G_2 \to G_i$ $(i = 1,2)$ се хомоморфизми, според (ii), постои еднозначно определен хомоморфизам $f : G_1 \times G_2 \to G$ со особината $\pi_i = f_i f$. Но според 2.46. f е биекција, па значи f е изоморфизам.

Овој резултат се обоштува на следниот начин. Нека $\{G_i \mid i \in I\}$ е фамилија групоиди и G групоид, со својствата:

(i′) постојат хомоморфизми $f_i : G \to G_i$ $(i \in I)$

(ii′) за секој групоид S и фамилија хомоморфизми $g_i : S \to G_i$ $(i \in I)$ постои еднозначно определен хомоморфизам $g : S \to G$, таков што $g_i = f_i g$.

Тогаш G е изоморфен со директниот производ $\prod_i G_i$.

§ 6. ГРУПИ

6.1. Нека $n\in\mathbb{N}$ и $G_n = \{a + b\sqrt{n} \mid a, b\in\mathbb{Z}\}$. Да се покаже дека G_n е група во однос на собирањето на реални броеви. Кога $G_n = \mathbb{Z}$?

Одговор. Кога n е потполн квадрат од некој природен број.

6.2. Нека $n\in\mathbb{N}$ и нека $G_n = \{a + ib\sqrt{n} \mid a, b\in\mathbb{Z}\}$. Да се покаже дека G_n е група во однос на операцијата собирање на комплексни броеви. Дали G_n е група и во однос на множењето на комплексни броеви?

Одговор. Не.

6.3. Во множеството $D = \mathbb{Z}\times\mathbb{Z}$ е дефинирана операција "o" со:
(a, b) o $(c, d) = (a + c,\ (-1)^c b + d)$.
Да се покаже дека D(o) е група.

Решение. Да покажеме дека D(o) е полугрупа.

$((a, b)$ o $(c, d))$ o $(e, f) = (a + c,\ (-1)^c b + d)$ o $(e, f) =$
$= (a + c + e,\ (-1)^e((-1)^c b + d) + f) =$
$= (a + c + e,\ (-1)^{e+c} b + (-1)^e d + f) =$
$= (a, b)$ o $(c + e, (-1)^e d + f) =$
$= (a, b)$ o $((c, d)$ o $(e, f))$.

Лесно се проверува дека (0, 0) е единица во D и дека секој елемент во D е инверзибилен, при што $(a,\ b)^{-1} = (-a,\ (-1)^{a+1}b)$. Значи, D(o) е група.

Бидејќи (1,1) o (1,2) = (2,1) ≠ (2, −1) = (1,2) o (1,1), групата D(o) не е комутативна.

6.4. Во множеството $G = \mathbb{Z}\times\mathbb{Q}$ е дефинирана операција "$*$" со:
а) $(a, b) * (c, d) = (a + c,\ 2^c b + d)$;
б) $(a, b) * (c, d) = (a + c,\ 2^{-c} b + d)$;
в) $(a, b) * (c, d) = (a + c,\ 2^c b - d)$.

Решение. а) Лесно се проверува асоцијативноста на "$*$" и дека (0, 0) е единица на $G(*)$. Да покажеме дека секој елемент во $G(*)$ е инверзибилен. Затоа, нека (a, b) е даден елемент од G. Од равенството

$(a, b) * (x, y) = (0, 0)$, т.е.
$(a + x,\ 2^x b + y) = (0, 0)$,

добиваме $x = -a$ и $y = -2^{-a} b$. Бидејќи

$(-a, -2^{-a} b) * (a, b) = (0, 0)$,

следува дека $(a, b)^{-1} = (-a, -2^{-a}b)$. Според тоа, $G(*)$ е група. Групата не е комутативна.

б) $G(*)$ е група.

в) $G(*)$ не е група.

6.5. Нека $D_m = \{a_0, a_1, \ldots, a_{m-1}, b_0, b_1, \ldots, b_{m-1}\}$,

Дефинираме операција "$*$" во D_m со:

$a_i * a_j = a_{i+j}$, $a_i * b_j = b_{i+j}$, $b_i * b_j = a_{i-j}$, $b_i * a_j = b_{i-j}$,

каде што, ако $i + j \geq m$, се зема $i + j - m$, а ако $i - j < 0$, се зема $i - j + m$.

Да се покаже дека $D_m(*)$ е група. (Оваа група се вика *диедрална група*.)

6.6. Нека во множеството $K = \{1, -1, i, -i, j, -j, k, -k\}$ е дефинирана операција со шемата:

$\bullet$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Да се покаже дека $K(\bullet)$ е група. (Таа се вика *кватернионска група*.)

6.7. Нека G е множеството од сите реални триаголни матрици $A = [a_{ij}]$ со ред n, така што $a_{ii} \neq 0$, $i = 1, \ldots, n$ и $a_{ij} = 0$ за $i > j$. Да се покаже дека G е група во однос на множење на матрици.

6.8. Ако G е група и $a^{-1} b^2 a = ba$, тогаш $b = a$.

Решение. Множејќи го равенството $a^{-1} b^2 a = ba$ одлево со a, а оддесно со a^{-1}, добиваме $b^2 = ab$. Ако пак ова равенство го помножиме оддесно со b^{-1}, добиваме $b = a$.

6.9. Дадена е групата G. Ако $a, b \in G$ и ако $a^2 = 1$, $a^{-1} b^2 a = b^3$, тогаш $b^5 = 1$.

Решение. Од $a^2 = 1$ имаме $a = a^{-1}$.

Потоа, од $a^{-1} b^2 a = b^3$, добиваме $b^2 = ab^3a$. Од ова следува:

$b^5 = b^3b^2 = b^3ab^3a$,

$b^5 = b^2b^3 = b^2ab^2a$,

па од $b^3ab^3a = b^2ab^2a$ следува $bab = a$. Затоа имаме:

$b^5 = b^2ab^2a = b(bab)ba = baba = aa = 1$.

6.10.* Ако за елементите a и b од групата G се исполнети равенствата

$a^{-1} b^2 a = b^3$, $\quad b^{-1} a^2 b = a^3$,

тогаш $a = b = 1$.

6.11. Нека $S(\cdot)$ е конечна полугрупа со единица во која е точен условот

$ax = xb \Rightarrow a = b$.

Да се покаже дека $S(\cdot)$ е комутативна група.

Решение. Доволно е да покажеме дека во $S(\cdot)$ важи комутативниот закон. Од условот на задачата и од равенството $aba = aba$ следува дека $ab = ba$, т.е. во $S(\cdot)$ важи комутативниот закон.

6.12. Нека G е полугрупа со својството

$(\forall a \in G)\ (\exists b \in G)\ [(\forall x \in G)\ axb = x]$.

Да се покаже дека G е комутативна група.

Решение. Ако a, b се елементи од G со својството

$$(\forall x \in G) axb = x, \tag{1}$$

тогаш елементот $ab = ba$, според 5.25, е единица во G; да ја означиме со e.

Бидејќи за секој $a \in G$ постои $b \in G$ со својството $ab = ba = e$, имаме дека секој $a \in G$ е инверзибилен, па значи G е група. Да покажеме дека G е комутативна. Имаме:

$xy = x^{-1}(xy)x = (x^{-1}x)yx = yx$.

6.13. Ако G е полугрупа со единствена десна единица e и

$(\forall x \in G)(\exists\ \overline{x}\ \in G)\ \overline{x}\, x = e$,

тогаш G е група.

Решение. Треба да се докаже само дека $x\overline{x} = e$. Нека $x\overline{x}\ = b$. Тогаш

$b^2 = x\overline{x}\, x\overline{x} = (xe)\ \overline{x} = x\overline{x} = b$,

па $\overline{b}\, bb = \overline{b}\, b$, т.е. $eb = e$. Од тоа следува дека

$(\forall y \in G) yb = (ye)b = y(eb) = ye = y$.

Значи, b е десна единица, а бидејќи G има единствена десна единица, имаме $b = e$.

6.14. а) Нека $G(\cdot)$ е група и нека во G е определена операција ":" (делење) со $x : y = x^{-1}$.

Да се покаже дека:

(i) $(\forall x, y, z \in G)\ (x : z) : (y : z) = x : y$,

$x : (y : y) = x, \quad (x : x) : (y : z) = z : y.$

(ii) $(\forall x, y \in G)\ xy = x : ((y : y) : y)$.

(iii) $(\forall x \in G)\ x^{-1} = (x : x) : x, \quad x : x = e$.

б) Нека G е непразно множество и $G(:)$ групоид во кој се точни идентитетите во (i). Ако во G дефинираме операција "$\cdot$" со (ii), да се покаже дека $G(\cdot)$ е група.

Решение. а) Дека се исполнети (i) – (iii) се покажува со обична проверка.

б) Нека xy е определен со (ii), а x^{-1} со (iii); тогаш имаме

$$xy = x : ((y : y) : y) = x : y^{-1},$$

а потоа и

$$(x : y) : y^{-1} = (x : y) : ((y : y) : y) = x : (y : y) = x,$$
$$(x : y^{-1}) : y = (x : y^{-1} : ((y : y) : y^{-1}) = x : (y : y) = x,$$
$$(x : y)^{-1} = ((x : y) : (x : y)) : (x : y) = y : x.$$

Користејќи ги овие равенства, добиваме:

$$x(yz) = x : (yz)^{-1} = x : (y : z^{-1})^{-1} = x : (z^{-1} : y) =$$
$$= ((x : y^{-1}) : y) : (z^{-1} : y) = (x : y^{-1}) : z^{-1} = (xy)z,$$

т.е. $G(\cdot)$ е полугрупа. Понатаму имаме:

$$(x^{-1})^{-1} = ((x : x) : x) : ((x : x) : x) : ((x : x) : x) = x : (x : x) = x.$$

Ако a е фиксен елемент од G, да ставиме $a : a = e$. Тогаш имаме:

$$xe = x : e^{-1} = x : (a : a)^{-1} = x : (a : a) = x,$$

т.е. e е десна единица. На крајот имаме:

$$xx^{-1} = x : (x^{-1})^{-1} = x : x = e,$$

т.е. x^{-1} е десен инверзен елемент за x.

Од сето тоа следува дека $G(\cdot)$ е група.

6.15.* Групата G е абелова ако и само ако постои цел број s, таков што $(\forall x, y \in G)\ (xy)^2 = x^i y^i,\ i = s,\ s+1, s+2$.

Со противпример да се покаже дека горното тврдење не важи ако $i = s,\ s+1$.

6.16. Да се покаже дека за секој $n \in \mathbb{N}$, постои група со n елементи.

Решение. Нека G_n е множеството од сите корени на равенката

$$x^n - 1 = 0.$$

G_n има n елементи, кои се комплексни броеви, и во однос на операцијата множење на комплексните броеви, G_n е комутативна група. Значи, за секој $n\in\mathbb{N}$ постои група со n елементи.

6.17. Да се покаже дека секоја некомутативна група има барем 6 елементи и да се најде барем една некомутативна група со 6 елементи.

Решение. Ќе покажема дека секоја група со 1, 2, 3, 4 и 5 елементи е комутативна. Затоа ќе ги разгледаме сите посебни случаи и притоа еден од елементите ќе го означиме со e што ќе значи дека тој елемент е единица.

1. Ако $G = \{e\}$ има еден елемент, тогаш операцијата во G е дефинирана со $ee = e$, па $G(\cdot)$ е комутативна група.

2. Нека $G = \{e, a\}$ има два елемента. Бидејќи e треба да биде единица, ќе имаме $ee = e$, $ea = ae = e$, па за $G(\cdot)$ да биде група, операцијата мора да биде дефинирана со шемата 1.

Дека со така дефинираната операција G е група се гледа од тоа што пресликувањето $f : G_2 \to G$, каде што $G_2 = \{-1, 1\}$ е групата од вторите корени на единицата (види 6.16.), дефинирано со $f : 1\to e$, $-1\to a$, е *изоморфизам*. Според тоа, постои само една група со два елемента и таа е комутативна.

	e	a
e	e	a
a	a	e

Шема 1.

3. Нека $G = \{e, a, b\}$ е множество со три елементи. Јасно е дека мора да биде $ex = xe = x$, за секој $x\in G$. Елементот aa може да биде или e, или b. Ако $aa = e$, тогаш мора да биде $ab = b$, што не е можно, зашто $eb = b$. Значи имаме $aa = b$, а од ова следува дека $ab = ba = e$ и $bb = a$. Според тоа, шемата со која е дефинирана операцијата е:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Шема 2.

Дека $G(\cdot)$ е група се гледа од тоа што пресликувањето

$f : G_3 \to G$, $G_3 = \{1, \varepsilon, \varepsilon^2\}$ е групата од сите трети корени на единицата (види 6.16.), дефинирано со $f : 1 \to e$, $\varepsilon \to a$, $\varepsilon^2 \to b$, е изоморфизам. Од сето тоа следува дека постои само една група со три елементи и таа е комутативна.

4. Нека е $G = \{e, a, b, c\}$. И овде ќе ставиме $ex = xe = x$ за секој $x \in G$. Елементот aa може да биде еден од елементите e, b, c.

4.1) Нека $aa = e$. Тогаш мора да е $ab = ba = c$ и $ac = ca = b$. Елементот bb може да биде или e или a.

4.1.1) Нека $bb = e$ тогаш ќе биде $bc = cb = a$ и $cc = e$. Шемата 3 ја определува операцијата што ја дискутираме.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Шема 3.

Од шемата се гледа дека $G(\cdot)$ е комутативна лупа. За да се види дали е група, треба да се провери асоцијативниот закон.

Ако барем еден од три избрани елементи е единица, имаме:

$e(xy) = xy = (ex)y$,

а поради комутативноста, елементот e може да биде на кое било од трите места. Од шемата 3 гледаме дека производот на два различни елементи, од кои ниеден не е единицата, го дава третиот елемент што е различен од единицата, а производот на кој било елемент со себе самиот ја дава единицата. Затоа, ако сите три елементи x, y, z се различни од единица и меѓусебно, ќе имаме:

$x(yz) = xx = e$, $\qquad (xy)z = zz = e$,

а ако меѓу трите избрани елементи два се меѓусебно еднакви, ќе имаме, на пример,

$x(yy) = xe = x$, $\qquad (xy)y = zy = x$.

Значи, асоцијативниот закон важи, па G е група.

4.1.2) Нека $bb = a$. Тогаш мора да биде $bc = cb = e$ и $cc = a$, па шемата на операцијата е:

e	a	b	c	
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Шема 4.

Пресликувањето $f: G \to G$, дефинирано со: $e \to e$, $a \to a$, $b \to c$, $c \to b$ е изоморфизам од шемата 3 во шемата 4, па значи и со шемата 4 е определена комутативна група.

4.2) Нека $aa = b$. Тогаш мора да биде $ab = ba = c$ и $ac = ca = e$, а потоа и $bb = e$, $bc = cb = a$, $cc = b$, па шемата на операцијата е

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Шема 5.

Да забележиме дека $b = a^2$, $c = a^3$, $e = a^4$, па G е изоморфна со групата G_4 од четвртите корени на единицата (види 6.16.).

4.3) Нека $aa = c$. Тогаш мора да биде $ab = ba = e$ и $ac = ca = b$, а потоа и $bb = c$, $bc = cb = a$, $cc = e$. Шемата на операцијата е:

	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Шема 6.

Од неа се гледа дека $c = b^2$, $a = b^3$, $e = b^4$, па пресликувањето од шемата 5 во шемата 6, дефинирано со $a \to b$, е изоморфизам. Значи, групоидот $G(\cdot)$, дефиниран со шемата 6, е абелова група.

Со тоа се разгледани сите случаи, па значи постојат само две неизоморфни групи со четири елементи, а притоа и двете групи се комутативни.

5) Нека $G = \{e, a, b, c, d\}$. И овде ќе ставиме $ex = xe = x$ за секој $x \in G$. Елементот aa може да биде: e, b, c или d.

5.1) Нека $aa = e$; тогаш елементот ab може да биде c или d.

5.1.1) Нека $ab = c$; тогаш мора да биде $ac = d$ и $ad = b$, а елементот ba може да биде c или d.

5.1.1.1) Нека $ba = c$; тогаш имаме $bb = d$, а bc може да биде или e или a.

Ако $bc = e$, тогаш шемата со која е дефинирана операцијата е

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	c	d	e	a
c	c	d	a	b	e
d	d	b	e	a	c

Шема 7.

Но, тогаш имаме $a(bc) = ae = a$, $(ab)c = cc = b$, па $G(\cdot)$ не е група.

Ако е $bc = a$, тогаш шемата со која е дефинирана операцијата е:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	c	d	a	e
c	c	d	e	b	a
d	d	b	a	e	c

Шема 8.

Но, тогаш имаме $a(bc) = aa = e$, $(ab)c = cc = b$, па и овој групоид не е група.

Значи не може да биде $ba = c$.

5.1.1.2) Нека е $ba = d$; елементот bb може да биде e или a. Ако $bb = e$, тогаш шемата со која е дефинирана операцијата е:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Шема 9.

Бидејќи $b(cd) = ba = d$, $(bc)d = ad = b$, и овој групоид не е група. Ако $bb = a$, тогаш шемата со која е дефинирана операцијата е :

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	a	e	c
c	c	b	d	a	e
c	d	c	e	b	a

Шема 10.

Бидејќи $(bc)d = ed = d$, $b(cd) = be = b$, и овој групоид не е група. Значи, не може да биде $ba = d$.

Од 5.1.1.1) и 5.1.1.2) следува дека не може $ab = c$.

5.1.2) Ако $ab = d$, тогаш, пишувајќи c наместо d и d наместо c, имаме $ab = c$, што не е можно. Значи , не може да е $ab = d$.

Од 5.1.1) и 5.1.2) следува дека не може да биде $aa = e$.

5.2) Нека $aa = b$; тогаш ab може да биде или e, или c, или d.

Нека $ab = e$; тогаш $ac = d$, $ad = c$, $ba = e$, па и $bb = aab = ae = a$. Но, тогаш bc може да биде само d, а бидејќи $ac = d$, тоа не е можно. Значи, не може да биде $ab = e$.

Ако $ab = c$, тогаш $ac = d$, $ad = e$, т.е .

$b = a^2$, $c = ab = a^3$, $d = ac = a^4$, $e = ad = a^5$.

Значи, групоидот е генериран од a, па според тоа, тој е изоморфен со групата G_5 од сите петти корени на единицата, т.е. ако $ab = c$, се добива комутативна група.

Ако $ab = d$, тогаш $ac = e$, $ad = c$, т.е.

$b = a^2$, $d = ab = a^3$, $c = ad = a^4$, $e = ac = a^5$,

што значи дека и во овој случај се добива комутативна група, изоморфна со групата G_5 (види 6.16).

5.3) Нека $aa = c$; тогаш ab може да биде или e, или d.

Ако $ab = e$, тогаш имаме $ac = d$, $ad = b$, т.е.

$c = a^2$, $d = ac = a^3$, $b = ad = a^4$, $e = ab = a^5$,

па и во овој случај се добива комутативна група изоморфна со G_5.

Ако $ab = d$, тогаш имаме $ac = b$, $ad = e$, т.е.

$c = a^2$, $b = ac = a^3$, $d = ab = a^4$, $e = ad = a^5$,

па и во овој случај се добива комутативна група изоморфна со G_5.

5.4) Нека $aa = d$; тогаш ab може да биде или e или c.

Ако $ab = e$, тогаш имаме $ac = b$, $ad = c$, т.е.

$d = a^2$, $c = ad = a^3$, $b = ac = a^4$, $e = ab = a^5$,

па и во овој случај се добива комутативна група изоморфна со G_5.

Ако $ab = c$, тогаш имаме $ac = e$, $ad = b$, т.е.

$d = a^2$, $b = ad = a^3$, $c = ab = a^4$, $e = ac = a^5$,

па и во овој случај се добива комутативна група изоморфна со G_5.

Од сето тоа следува дека постои само една група со пет елементи при што таа е комутативна.

6) Групата S_3 (види 5.36.) има шест елементи и е некомутативна.

6.18. Да се најде бројот на неизоморфните групи со шест елементи.

Решение: Постојат само две неизоморфни групи со шест елементи.

Нивните шеми се:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	c	d	f	e
b	b	c	d	f	e	a
c	c	d	f	e	a	b
d	d	f	e	a	b	c
f	f	e	a	b	c	d

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	f	c	d
b	b	e	a	d	f	c
c	c	d	f	e	a	b
d	d	f	c	b	e	a
f	f	c	d	a	b	e

6.19. Да се определи полугрупата од сите ендоморфизми на адитивната група $\mathbb{Z}(+)$ од целите броеви и да се покаже дека таа е изоморфна со мултипликативната полугрупа $\mathbb{Z}(\cdot)$.

Решение. Нека f е ендоморфизам во $\mathbb{Z}(+)$, т.е. за кои било $x, y \in \mathbb{Z}$ е точно равенството

$$f(x + y) = f(x) + f(y).$$

Бидејќи f е ендоморфизам, имаме $f(0) = 0$.

Да претпоставиме дека $f(1) = a$. Тогаш имаме

$$x\in\mathbb{N} \Rightarrow f(x) = f(\underbrace{1+1+\ldots+1}_{x}) = f(\underbrace{(1)+f(1)+\ldots+f(1)}_{x}) =$$

$$= \underbrace{a+a+\ldots+a}_{x} = ax.$$

Ако $x\in\mathbb{N}$, тогаш $-x\in\mathbb{Z}^-$, па имаме

$f(0) = f(x-x) = f(x)+f(-x)$, т.е. $f(-x) = -f(x)$.

Значи, за секој ендоморфизам f, постои $a\in\mathbb{Z}$, т.ш. $f(x) = ax$. Затоа, ендоморфизмот што му одговара на $a\in\mathbb{Z}$ ќе го означиме со f_a.

Пресликувањето φ : End$\mathbb{Z}\to\mathbb{Z}$ дефинирано со $\varphi(f_a) = a$ е биекција и притоа имаме:

$\varphi(f_a f_b) = \varphi(f_{ab}) = ab = \varphi(f_a)\varphi(f_b)$,

т.е. φ е изоморфизам од End $\mathbb{Z}$ во $\mathbb{Z}$ $(\cdot)$.

6.20. Да се најдат сите епиморфизми од $\mathbb{Z}(+)$ во $\mathbb{Z}(+)$.

Решение. Нека $f:\mathbb{Z}\to\mathbb{Z}$ е епоморфизам и нека $f(1) = a$.

Од тоа што f е хомоморфизам имаме $f(0) = 0$, па

$0 = f(0) = f(1+(-1)) = f(1)+f(-1)$,

од каде што $f(-1) = -a$. Од тоа е јасно дека за кој било $z\in\mathbb{Z}$ ќе имаме $f(z) = az$.

Нека p е прост број, различен од a, и нека е слика на бројот k, т.е. $p = f(k) = ak$. Равенката $ak = p$ има решение во $\mathbb{Z}$ ако и само ако $a = \pm 1$. Според тоа, постојат само два епиморфизма од $\mathbb{Z}(+)$ во $\mathbb{Z}(+)$ и тоа $1_{\mathbb{Z}}$ и $f(z) = -z$, за секој $z\in\mathbb{Z}$.

6.21. Да се најдат сите хомоморфизми

а) од $\mathbb{Q}(+)$ во $\mathbb{Z}(+)$;

б) од $\mathbb{Z}(+)$ во $\mathbb{Q}(+)$.

Решение. Нека f : $\mathbb{Q}(+)\to\mathbb{Z}(+)$ е хомоморфизам. Тогаш, според 6.19, имаме

$(\forall z\in\mathbb{Z})\, f(z) = az$,

каде што $a = f(1)$. Нека $x\in\mathbb{Q}$; тогаш имаме:

$$f(x) = f\left(n\frac{x}{n}\right) = nf\left(\frac{x}{n}\right), \text{ т.е.}$$

$$f\left(\frac{x}{n}\right) = \frac{1}{n}f(x).$$

Од ова, за $x = 1$, добиваме $f\left(\frac{1}{n}\right) = \frac{1}{n} f(1) = \frac{a}{n}$. Но $\frac{a}{n}$ треба да биде цел број за секој $n \in \mathbb{N}$ а тоа е можно само за $a = 0$. Значи, постои само еден хомоморфизам од $\mathbb{Q}(+)$ во $\mathbb{Z}(+)$ и тоа е нултиот.

б) $f_a(z) = az$, за секој $a \in \mathbb{Q}$.

6.22. Да се најдат сите хомоморфизми од $\mathbb{Q}(+)$ во $\mathbb{Z}_m(+)$.

Решение. Нека $f : \mathbb{Q} \to \mathbb{Z}_m$ е хомоморфизам. Ако ставиме $f(1) = a$, тогаш ќе биде $f(n) = na$ за секој $n \in \mathbb{N}$. Нека x е кој било елемент од $\mathbb{Q}$. Бидејќи $m \neq 0$, можеме да ставиме $x = m\frac{x}{m}$. Имајќи предвид дека $mk = 0$ во $\mathbb{Z}_m$ за секој цел број k, добиваме :

$$f(x) = f(m\frac{x}{m}) = maf(\frac{x}{m}) = mk = 0,$$

што значи дека f е нултиот хомоморфизам. Според тоа, постои само еден хомоморфизам од $\mathbb{Q}(+)$ во $\mathbb{Z}_m(+)$.

6.23. Дали групите $\mathbb{Q}(+)$ и $\mathbb{Z}(+)$ се изоморфни?

Решение. Да препоставиме дека $f : \mathbb{Z}(+) \to \mathbb{Q}(+)$ е хомоморфизам. Тогаш имаме $f(0) = 0$, а нека $f(1) = q$. Ако $n \in \mathbb{N}$, тогаш имаме

$$f(n) = f(\underbrace{1 + \ldots + 1}_{n}) = \underbrace{f(1) + \ldots + f(1)}_{n} = nq,$$

$$f(-n) = -f(n) = -nq.$$

Значи, хомоморфизмот f мора да е дефиниран со: $f(z) = zq$. Ако $q \in \mathbb{Z}$, тогаш f не е епиморфизам. Ако пак $q = \frac{m}{n}$, $m, n \neq 0$, тогаш, на пример, бројот $\frac{1}{2n} \in \mathbb{Q}$ не е слика на ниеден цел број, па f пак не е епиморфизам. Значи, не постои изоморфизам од $\mathbb{Z}(+)$ во $\mathbb{Q}(+)$.

6.24. Да се покаже дека адитивната група $\mathbb{C}(+)$ од комплексните броеви е изоморфна со директниот производ $\mathbb{R} \times \mathbb{R}$ од адитивната група $\mathbb{R}(+)$ на реалните броеви. Дали истото важи за мултипликативните групоиди?

Решение. Пресликувањето $f : \mathbb{C} \to \mathbb{R} \times \mathbb{R}$, дефинирано со

$$f(a + bi) = (a, b),$$

е биекција. Бидејќи

$$f(z_1 + z_2) = f(a_1 + a_2 + (b_1 + b_2)i) = (a_1 + a_2, b_1 + b_2) =$$
$$= (a_1, b_1) + (a_2, b_2) = f(z_1) + f(z_2),$$

тоа е изоморфизам.

За мултипликативните групоиди тоа не важи, зашто ако би постоел изоморфизам, тогаш $\mathbb{R} \times \mathbb{R} \setminus \{(0, 0)\}$ во однос на множењето на парови реални броеви би требало да биде група. Меѓутоа, тоа не е група, бидејќи, на пример, $(1,0) \neq (0,0) \neq (0,1)$, но $(1,0) \cdot (0,1) = (0,0)$.

6.25. Нека матрицата A_α е формирана со помош на табелата на $\mathbb{Z}_5^*(\cdot)$ со ставање 1 на местата каде што стои α и нули на другите места, и нека $B = A_1 A_\alpha$.

Да се покаже дека множеството $G = \{B_\alpha \mid \alpha \in \mathbb{Z}_5^*\}$ е група во однос на операцијата множење на матрици, изоморфна со $\mathbb{Z}_5^*$

Да се покаже дека овој резултат важи ако наместо 5 се земе кој било прост број p.

Решение. Од табелата на $\mathbb{Z}_5^*(\cdot)$:

	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

ги добиваме матриците:

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \qquad A_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

а потоа и матриците

$$B_1 = A_1 A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B_2 = A_1 A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$B_3 = A_1 A_3 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad B_4 = A_1 A_4 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Мултипликативната таблица на $G(\cdot)$ е :

	B_1	B_2	B_3	B_4
B_1	B_1	B_2	B_3	B_4
B_2	B_2	B_4	B_1	B_3
B_3	B_3	B_1	B_4	B_2
B_4	B_4	B_3	B_2	B_1

Од таблицата се гледа дека $G(\cdot)$ е група со единица B_1. Пресликувањето

$f: \mathbb{Z}_5^* \to G$, дефинирано со $\alpha \to B_\alpha$ е изоморфизам.

6.26. Дадени се матриците

$$I = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix},$$

Да се покаже дека множеството $G = \{E, -E, I, -I, J, -J, K, -K\}$, каде што E е единичната матрица од четврти ред, образува група во однос на операцијата множење на матрици, изоморфна со кватернионската група (види 6.6).

6.27. Во множеството $G = \{e, a, b, c\}$ е дефинирана операцијата "$\cdot$" со:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Ако φ е пермутација во G, да дефинираме нова операција "$*$" со:
$x * y = \varphi^{-1}(\varphi(x)\,\varphi(y))$.

а) Да се покаже дека $G(*)$ е група изоморфна со групата $G(\cdot)$.

б) Дали постои пермутација $\varphi \neq 1_G$ таква што операциите "$\cdot$" и "$*$" се совпаѓаат?

в) Дали равенката $xb = c * x$ има решение, ако $\varphi = \begin{pmatrix} e & a & b & c \\ a & b & e & c \end{pmatrix}$?

6.28. Нека G е група, X произволно непразно множество, а Ga^X множеството на сите пресликувања од X во G. Во G^X определуваме операција $*$ со :

$f_1 * f_2 = f \Leftrightarrow (\forall x \in X)\, f(x) = f_1(x)\, f_2(x)$.

Да се покаже дека $G^X(*)$ е група и дека таа група е изоморфна со директниот производ $\prod_{x \in X} G_x$ каде што $\{G_x \mid x \in X\}$ е фамилија групи изоморфни со G.

Решение. Јасно е дека $G^X(*)$ е полугрупа со единица ω, каде што ω е определено со:

$(\forall x \in X)\ \omega(x) = e$,

при што e е единицата во G. Ако $f \in G^X$, тогаш за пресликувањето $g \in G^X$, определено со :

$g(x) = (f(x))^{-1}$

имаме $f * g = g * f = \omega$, па значи $G^X(*)$ е група.

Нека $\{G_x \mid x \in X\}$ е фамилија групи изоморфни со G, а $h_x : G_x \to G$ е изоморфизмот од G_x во G за секој $x \in X$. Нека φ е пресликување од

$P = \prod_{x \in X} G_x$ во G^X, дефинирано со $\varphi = h_x \pi_x$,

каде што π_x е проекцијата од P на G_x за секој $x \in X$. Бидејќи h_x и π_x се епиморфизми, следува дека и φ е епиморфизам. Од

$\varphi((a_x)) = \varphi((b_x))$ добиваме по ред

$h_x\pi_x((a_x)) = h_x\pi_x((b_x))$, $h_x(a_x) = h_x(b_x)$, $a_x = b_x$,

т.е φ е инјекција, па според тоа φ е изоморфизам.

6.29. Што претставува множеството од сите леви односно десни транслации на една група?

Решение. Нека G е дадена група, а G_l нека е множеството од сите леви транслации на групата G, т.е.

$G_l = \{\gamma_a \mid a \in G\}$.

Јасно дека G_l е полугрупа (види 5.21) Ако e е единицата во G, тогаш $\gamma_e = 1_G$, па значи полугрупата G_l е со единица. Нека сега γ_a е произволен елемент од G_l. Ако a^{-1} е инверзниот елемент на a во G, тогаш имаме

$$\gamma_a \gamma_{a^{-1}} = \gamma_{aa^{-1}} = \gamma_e,$$

$$\gamma_{a^{-1}} \gamma_a = \gamma_{a^{-1}a} = \gamma_e,$$

т.е. секој елемент γ_a е инверзибилен. Значи G_l е група.

Слично се докажува дека и множеството G_2 од сите десни транслации на групата G е група. Групите G_l и G_2 се изоморфни.

6.30. Во множеството $G = \mathbb{Z} \times \mathcal{J}_{\mathbb{Z}}$ дефинираме операција "o"

$(m, f) \circ (n, g) = (m + n, h)$,

каде што $(\forall z \in \mathbb{Z})\ h(z) = f(z - n) + g(z)$. Да се покаже дека $G\ (\circ)$ е група.

Решение. Јасно е дека $G(\circ)$ е групоид. Да покажеме дека операцијата "$\circ$" е асоцијативна. Имаме:

$$[(m, f_1) \circ (n, f_2)] \circ (k, f_3) = (m + n, g_1) \circ (k, f_3) = (m + n + k, g),$$

при што

$$(\forall z \in \mathbb{Z})\ \ g(z) = g_1(z - k) + f_3(z) = f_1(z - k - n) + f_2(z - k) + f_3(z);$$

$$(m, f_1) \circ [(n, f_2) \circ (k, f_3)] = (m, f_1) \circ (n + k, h_1) = (m + n + k, h)$$

при што

$(\forall z \in \mathbb{Z})\ h(z) = f_1(z - n - k) + h_1(z) = f_1(z - n - k) + f_2(z - k) + f_3(z)$, па значи $g = h$.

Ако пресликувањето $\omega : \mathbb{Z} \to \mathbb{Z}$ е дефинирано со $\omega(z) = 0$ за секој $z \in \mathbb{Z}$, тогаш елементот $(0, \omega)$ е единица во полугрупата $G(\circ)$.

Ако (m, f) е даден елемент од G, тогаш од равенството

$$(m, f) \circ (x, g) = (0, \omega)$$

добиваме $x = -m$ и $g(z) = -f(z + m)$ за секој $z \in \mathbb{Z}$, а бидејќи и

$(x, g) \circ (m, f) = (0, \omega)$, следува дека секој елемент (m, f) од G е инверзибилен и притоа имаме

$$(m, f)^{-1} = (-m, g),$$

каде што $(\forall z\in\mathbb{Z})\ g(z) = -f(z+m)$.
Од сето тоа следува дека $G\ (\circ)$ е група.

6.31. Ако G е група, тогаш и Aut G е група.

6.32. Ако G е група со барем три елементи, тогаш Aut G има барем два елемента.

Решение. За да покажеме дека Aut G има барем два елемента, доволно е да покажеме дека постои барем еден автоморфизам во G, различен од идентичниот. Ќе ги разгледаме двата случаја: G е некомутативна и G е комутативна.

Ако G е некомутативна, тогаш постои $a\in G\setminus C(G)$, па пресликувањето $f: G\to G$ дефинирано со

$(\forall x\in G)\ f(x) = a^{-1}xa$,

е автоморфизам, различен од 1_G.

Нека сега групата G е комутативна и нека го задоволува условот

$(\exists x\in G)\ x^2\neq e.$ (1)

Во овој случај пресликувањето $f: G\to G$ дефинирано со $f(x) = x^{-1}$, е автоморфизам во G, различен од 1_G. Ако пак G не го задоволува условот (1), т.е. го задоволува условот

$(\forall x\in G)\ x^2 = e$ (2)

нека $a,b\in G$, $e\neq a\neq b\neq e$. Тогаш пресликувањето $g: G\to G$ дефинирано со

$$f(x) = \begin{cases} b, & x = a \\ a, & x = b \\ x, & x\neq a,b \end{cases}$$

е автоморфизам во G, различен од 1_G.

6.33. Нека a е даден елемент од групата G. Да дефинираме пресликување $f_a: G\to G$ со:

$(\forall x\in G)\ f_a(x) = a^{-1}xa$.

Да се докаже дека f_a е автоморфизам и дека множеството

$H = \{f_a \mid a\in G\}$,

е подгрупа од групата Aut G.

Решение. Да покажеме дека f_a е биекција. Ако $f_a(x_1) = f_a(x_2)$, тогаш $a^{-1}x_1a = a^{-1}x_2a$, т.е. $x_1 = x_2$, што значи дека f_a е инјекција.

Ако y е произволен елемент од G, тогаш ставајќи $x = aya^{-1}$, имаме $f_a(x) = a^{-1}(aya^{-1})a = y$, т.е. f_a е сурјекција. Да покажеме уште дека f_a е хомоморфизам. Имаме:

$$f_a(xy) = a^{-1}(xy)a = a^{-1}x(aa^{-1})ya =$$
$$= (a^{-1}xa)\,(a^{-1}ya) = f_a(x)\,f_a(y).$$

Според тоа f_a е автоморфизам.

Ако $a,b \in G$, тогаш имаме:

$$f_a f_b(x) = f_a(b^{-1}xb) = a^{-1}(b^{-1}xb)a =$$
$$= (ba)^{-1}x(ba) = f_{ba}(x),$$

т.е. $f_a f_b = f_{ba}$. Бидејќи и $(f_a)^{-1} = f_{a^{-1}}$, добиваме дека H е подгрупа од групата Aut$G$.

6.34. Да се најдат групите автоморфизми од групата S_3 и A_3, каде што

$$A_3 = \left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}.$$

Решение. Елементите на S_3 ќе ги означиме со 1, ρ_1, ρ_2, σ_1, σ_2, σ_3, како во 5.36. Според претходната задача,

$f_1 = \varepsilon$, $f\rho_1 = \alpha_1$, $f\rho_2 = \alpha_2$, $f\sigma_i = \beta_i$ $(i = 1, 2, 3)$ се автоморфизми во S_3, при што:

$$\varepsilon = \begin{pmatrix}1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\\1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\end{pmatrix},\ \alpha_1 = \begin{pmatrix}1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\\1&\rho_1&\rho_2&\sigma_3&\sigma_1&\sigma_2\end{pmatrix},$$

$$\alpha_2 = \begin{pmatrix}1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\\1&\rho_1&\rho_2&\sigma_2&\sigma_3&\sigma_1\end{pmatrix},\ \beta_1 = \begin{pmatrix}1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\\1&\rho_2&\rho_1&\sigma_1&\sigma_3&\sigma_2\end{pmatrix},$$

$$\beta_2 = \begin{pmatrix}1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\\1&\rho_2&\rho_1&\sigma_3&\sigma_2&\sigma_1\end{pmatrix},\ \beta_3 = \begin{pmatrix}1&\rho_1&\rho_2&\sigma_1&\sigma_2&\sigma_3\\1&\rho_2&\rho_1&\sigma_2&\sigma_1&\sigma_3\end{pmatrix},$$

Ако f е друг автоморфизам, тогаш $f(1) = 1$. Да побараме што е $f(\rho_1)$. Ако $f(\rho_1)$ е σ_1, или σ_2, или σ_3, тогаш имаме :

$$f(\rho_2) = f(\rho_1\rho_1) = f(\rho_1)f(\rho_1) = \sigma_i\sigma_i = 1,$$

коешто не е можно, зашто $f(1) = 1$. Значи, $f(\rho_1)$ може да биде или ρ_1, или ρ_2. Слично, $f(\sigma_1)$ може да биде или σ_1, или σ_2, или σ_3, но ако $f(\rho_1)$ и $f(\sigma_1)$ се познати, тогаш од $\rho_1\rho_1 = \rho_2$, $\rho_1\sigma_1 = \sigma_3$, $\rho_2\,\sigma_1 = \sigma_2$, може да се најдат и $f(\rho_2)$, $f(\sigma_2)$ и $f(\sigma_3)$. Од ова следува дека секој автоморфизам на S_3 е еден од горните шест.

Користејќи го равенството $f_a f_b = f_{ab}$ (види 6.33), шемата на операцијата од Aut S_3 е:

	ε	α_1	α_2	β_1	β_2	β_3
ε	ε	α_1	α_2	β_1	β_2	β_3
α_1	α_1	α_2	ε	β_3	β_1	β_2
α_2	α_2	ε	α_1	β_2	β_3	β_1
β_1	β_1	β_2	β_3	ε	α_1	α_2
β_2	β_2	β_3	β_1	α_2	ε	α_1
β_3	β_3	β_1	β_2	α_1	α_2	ε

Споредувајќи ги шемите на S_3 и AutS_3, може да се заклучи дека тие се изоморфни, при што изоморфизмот е:

$1 \to \varepsilon$, $\rho_i \to \alpha_i$, $\sigma_j \to \beta_j$, $i = 1, 2$; $j = 1, 2, 3$.

Дека A_3 е група може да се види од шемата на S_3 (в.5.36.); елементите на A_3 се точно 1, ρ_1, ρ_2. Нека f е автоморфизам на A_3. Тогаш имаме $f(1) = 1$, а $f(\rho_1)$ може да биде ρ_1 или ρ_2. Значи, постојат само две биекции од A_3 во A_3 што можат да бидат автоморфизми. Тоа се ε и $f : 1 \to 1$, $\rho_1 \to \rho_2$. Лесно се проверува дека f е автоморфизам, па значи Aut A_3 има два елемента, ε и f.

6.35. Да се дадат неколку примери на квазигрупи што не се групи.

Решение. Јасно е дека секоја квазигрупа со 1 или со 2 елемента е група. Ако $G = \{a, b, c\}$ е множество со три елемнта, и ако дефинираме операција во G со шемата

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a,

тогаш G е квазигрупа што не е група.

Исто така, ако $G = \{a, b, c, d\}$, тогаш G во однос на операцијата дефинирана со шемата

	a	b	c	d
a	b	a	d	c
b	d	c	b	a
c	c	d	a	b
d	a	b	c	d

е квазигрупа што не е група.

Ако во $G = \mathbb{R} \times \mathbb{R}$ дефинираме операција "$\otimes$" со

$(x, y) \otimes (u, v) = (x + v, y + u)$,

тогаш $G(\otimes)$ е квазигрупа, но не и група.

6.36. Во множеството $\mathbb{N}^\circ$ е дефинирана операција "o" со:

$x \circ y = |x - y|$.

Да се покаже дека $\mathbb{N}^\circ$ е комутативен групоид, во кој, за секои $a,b \in \mathbb{N}^\circ$ равенката $a + x = b$ има решение во $\mathbb{N}^\circ$, но сепак не е квазигрупа.

Решение. Дека $\mathbb{N}^\circ(o)$ не е квазигрупа следува од тоа што во $\mathbb{N}^\circ(o)$ не важи законот за кратење. Имено: $|4 - 0| = |4 - 8|$, но $0 \neq 8$.

6.37. Дали групоид со кратење е квазигрупа?

Решение. Групоид со кратење не мора да е квазигрупа. На пример, таков е групоидот $\mathbb{N}(\cdot)$.

6.38. Да се покаже дека секој конечен групоид со кратење е квазигрупа. Дали истото важи и за бесконечните групоиди?

Решение. Нека $G = \{a_1, a_2, \ldots, a_n\}$ е конечен групоид со кратење. Треба да покажеме дека равенките

$ax = b$, $ya = b$,

се решливи во G. Нека a е фиксен елемент од G. Да го разгледаме множеството $G_1 = \{aa_1, aa_2, \ldots, aa_n\}$. Бидејќи G е групоид со кратење, следува дека $G = G_1$, т.е. за секој $a \in G$, постои $x = a_i \in G$, така што важи $aa_i = a_j$, а тоа значи дека равенката $ax = b$ е решлива во G. Слично за другата равенка.

За бесконечните групоиди тоа не важи. На пример, $\mathbb{N}(\cdot)$ е групоид со кратење што не е квазигрупа.

6.39. Да се определат сите квазигрупи што можат да се дефинират на множеството $G = \{a, b, c\}$. Кои од нив се групи?

Решение. Групоидот G, $G = \{a, b, c\}$, е *квазигрупа* ако и само ако важи законот за кратење. Според тоа, во шемата на квазигрупата, секој елемент ќе се појави само еднаш во секоја редица и во секоја колона. Квазигрупите ќе ги бараме користејќи го горното при формирањето на соодветните шеми.

Елементот aa може да биде или a, или b, или c.

1. Ако $aa = a$, можни се следниве шеми:

	a	b	c
a	a	b	c
b	b	c	a
b	c	a	b

1.1)

	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

1.2)

	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

1.3)

	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

1.4)

од кои 1.1) е група, а 1.2) и 1.3) се меѓусебно изоморфни квазигрупи.

2. Ако $aa = b$, тогаш шемите се:

	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

2.1)

	a	b	c
a	b	c	a
b	a	b	c
c	c	a	b

2.2)

	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

2.3)

	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

2.4)

од кои 2.1) е група, а 2.2) и 2.3) се маѓусебно изоморфни квазигрупи.

3. Ако $aa = c$, тогаш шемите се:

	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

3.1)

	a	b	c
a	c	a	b
b	b	c	a
c	a	b	c

3.2)

	a	b	c
a	c	b	a
b	a	c	b
c	b	a	c

3.3)

	a	b	c
a	c	b	a
b	b	a	c
c	a	c	b

3.4)

од кои 3.1) е група, а 3.2) и 3.3) се меѓусебно изоморфни.

Бидејќи постои само една група со три елемнти (види 6.17), групите 1.1), 2.1) и 3.1) се изоморфни.

Квазигрупите 1.2), 2.2) и 3.2) се изоморфни. На пример, пресликувањето $a \to b$, $b \to c$, $c \to a$, е изоморфизам од 1.2) во 2.2). Според тоа, сите квазигрупи 1.2), 1.3), 2.2), 2.3), 3.2), 3.3) се меѓусебно изоморфни.

Квазигрупите 1.4), 2.4) и 3.4) меѓусебно се изоморфни. На пример, пресликувањето $a \to b$, $b \to c$, $c \to a$ е изоморфизам од 1.4) во 2.4).

Значи, постојат три квазигрупи со по три елемнти, од кои едната е група, т.е. постојат две квазигрупи што не се групи, и тоа една комутативна и една некомутативна.

6.40. Нека G е квазигрупа и A е следното подмножество од G:
$A = \{a \mid a \in G, (\forall x, y \in G)\ (xa)y = x(ay)\}$.
Ако A е непразно подмножеството, да се покаже дека A е група во однос на операцијата во G.

Решение. Бидејќи во A, според условот на задачата, важи асоцијативниот закон, а G е квазигрупа, доволно е да покажеме дека A е групоид, т.е. дека $a, b \in A \Rightarrow ab \in A$.

Нека $A \neq \emptyset$, т.е. постои барем еден елемент a во A. Ако $a, b \in A$, тогаш

$(x(ab))y = ((xa)b)y = (xa)\ (by) = x(a(by)) = x((ab)y)$,

што значи дека $ab \in A$.

6.41. Нека $G(\cdot)$ е група и нека во G е дефинирана нова операција "$*$" со:
(1) $x * y = xy^{-1}$; (2) $x * y = x^{-1}y$.
Да се покаже дека:
а) $G(*)$ е квазгрупа.
б) $G(*)$ е група ако и само ако $(\forall x \in G)\ x^2 = e$.
в) α е конгруенција во $G(\cdot)$ ако и само ако α е конгруенција и во $G(*)$.

Решение. Задачата ќе ја решиме само за (1).

а) За да покажеме дека $G(*)$ е квазигрупа, треба да покажеме дека равенките

$x * a = b, \quad a * x = b$

се еднозначно решливи во $G(*)$. Равенката $x*a = b$ е еквивалентна со равенката $xa^{-1} = b$ во $G(\cdot)$. Но, равенката $xa^{-1} = b$ во $G(\cdot)$ има единствено решение $x = ba$. Значи, $x = ba$ е единствено решение на равенката $x * a = b$. Слично, $x = b^{-1}a$ е единствено решение на $a * x = b$.

б) Нека $G(*)$ е група, а e' нека е единицата во $G(*)$.

Од $x * e' = x$ имаме $x\ e'^{-1} = x\ e' = x$, т.е. $e' = e$, каде што e е единицата во $G(\cdot)$. Сега, од равенството $e'^{-1} * x = e * x = x$, следува $ex^{-1} = x$, т.е. $x^2 = e$.

Обратно, да претпоставиме дека во $G(\cdot)$ е исполнет условот $(\forall x \in G)x^2 = e$.

Тогаш имаме

$e * x = ex^{-1} = x^{-1} = x,\ x * e = xe^{-1} = xe = x,$

т.е. e е единица во $G(*)$. Понатаму имаме:

$x*(y * z) = x(y * z)^{-1} = x(yz^{-1})^{-1} =$

$= x(yz) = (xy)z = (xy^{-1})z^{-1} = (x * y) * z.$

Значи, $G(*)$ е група.

в) Нека α е конгруенција во $G(\cdot)$ и нека $a\ \alpha\ x$, $b\ \alpha\ y$. Од $b\ \alpha\ y$ следува дека $b^{-1}\ \alpha\ y^{-1}$, а од $a\ \alpha\ x$ и $b^{-1}\ \alpha\ y^{-1}$ следува $ab^{-1}\ \alpha\ xy^{-1}$, т.е. $a*b\ \alpha\ x*y$. Значи, α е когруенција и во $G(*)$.

Обратно, нека α е конгруенција во $G(*)$ и нека $a\alpha x$ и $b\alpha y$. Бидејќи $e\ \alpha\ e$, каде што e е единицата во $G(\cdot)$, од $e\ \alpha\ e$ и $b\ \alpha\ y$ следува $e*b\ \alpha\ e*y$, т.е. $b^{-1}\alpha\ y^{-1}$, а од $a\ \alpha\ x$ и $b^{-1}\ \alpha\ y^{-1}$ следува $a*b^{-1}\ \alpha\ x*y^{-1}$, т.е. $ab\alpha xy$. Значи, α е конгруенција и во $G(\cdot)$.

6.42. Секоја квазигрупа со единица се вика *лупа*. Да се покаже дека секоја лупа со 1, 2, 3 и 4 елементи е група и дека постои барем една лупа со 5 елементи што не е група .

Решение Според 1- 4 од 6.17 се гледа дека секоја лупа што има најмногу четири елементи е група, а шемата 7 покажува дека постои лупа со пет елементи што не е група.

6.43. Нека $G(\cdot)$ е групоид, а f, g, h се пермутации на G. Во G определуваме нова операција "$\circ$" со:

$a \circ b = h(f(a)\ g(b))$.

За групоидот $G(\circ)$ велиме дека е *изотопен* со гупоидот $G(\cdot)$. Да се покаже дека $G(\cdot)$ е квазигрупа ако и само ако $G(\circ)$ е квазигрупа.

Решение. Нека $G(\cdot)$ е квазигрупа. Да докажеме дека равенката

$a \circ x = b,$

има единствено решение во $G(\circ)$. Оваа равенка е еквивалентна со равенката

$f(a)\ g(x) = h^{-1}(b)$

во $G(\cdot)$, којашто има единствено решение $g(x) = c$, па и равенката $a \circ x = b$ има единствено решение $x = g^{-1}(c)$. Слично се покажува дека и равенката $x \circ a = b$ има единствено решение, па значи $G(\circ)$ е квазигрупа.

Обратно, нека $G(\circ)$ е квазигрупа. Равенката $ax = b$ е еквивалентна со равенката $f^{-1}(a) \circ g^{-1}(x) = h(b)$ во $G(\circ)$, којашто има единствено решение $g^{-1}(x) = d$, па и равенката $ax = b$ има единствено решение $x = g(d)$. Слично се покажува дека и равенката $xa = b$ има единствено решение, па значи $G(\cdot)$ е квазигрупа.

6.44. Ако $G(\circ)$ е изотопен со $G(\cdot)$, да се покаже дека едниот од нив може да биде:

а) комутативен; в) лупа;

б) полугрупа; г) група,

а другиот да го нема соодветното својство.

Решение. а) Нека $G(\cdot)$ е групоидот определен со шемата

$\cdot$	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

Ако $g = h = 1_G$, а f е дефинирано со $f(a) = a$, $f(b) = c$, $f(c) = b$ и ако дефинираме операција " $\circ$ " со:

$x \circ y = f(x)y$

тогаш шемата на групоидот $G(\circ)$ е:

o	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

Значи, групоидот G(o) е комутативен, но $G(\cdot)$ не е комутативен.

г) Нека $G(\cdot)$ е групоидот определен со шемата

$\cdot$	e	a	b	c
e	a	e	c	b
a	c	b	a	e
b	b	c	e	a
c	e	a	b	c

Јасно е дека $G(\cdot)$ не е група, но е квазигрупа.

Нека $f, g : G \to G$ се дефинирани со:

$y = f(x) \Leftrightarrow ya = x$,

$y = g(x) \Leftrightarrow ey = x$.

Тогаш имаме:

$f(e) = e$, $f(a) = c$, $f(b) = a$, $f(c) = b$,

$g(e) = a$, $g(a) = e$, $g(b) = c$, $g(c) = b$.

Ако во G определиме операција "o" со:

$$x \circ y = f(x) \cdot g(y),$$

тогаш шемата на групоидот $G(\circ)$ е:

o	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Дека $G(\circ)$ е група, види 6.17, шема 4. Значи, групата $G(\circ)$ е изотопна со квазигрупата $G(\cdot)$, при што $h = 1_G$.

Да забележиме дека овој пример ги потврдува б) и в).

6.45. Нека S е полугрупа со единица. Да се покаже дека множеството од сите инверзибилни елементи од S е подгрупа од S.

Решение. Нека G е множеството од сите инверзибилни елементи во полугрупата S, со единица e. Јасно е дека $e \in G$, а ако $a \in G$, т.е. ако a е инверзибилен, тогаш од $(a^{-1})^{-1} = a$ следува дека и a^{-1} е инверзибилен, т.е. $a^{-1} \in G$. Ако пак $a, b \in G$, тогаш од равенството $(ab)^{-1} = b^{-1}a^{-1}$ следува дека и $ab \in G$. Од сето тоа следува дека G е подгрупа од S.

6.46. Нека A, B и C се подгрупи од групата G и нека $A = B \cup C$. Да се покаже дека $A \subseteq B$ или $A \subseteq C$.

Решение. Ако за секој $x \in A$ имаме $x \in B$ или $x \in C$, тогаш е јасно дека $A \subseteq B$ или $A \subseteq C$. Затоа, да претпоставиме дека постојат два елемента $b, c \in A$, такви што $b \in B$, $c \in C$. Бидејќи A е подгрупа од G, имаме $bc \in A$, а од $A \subseteq B \cup C$, следува дека $bc \in B$ или $bc \in C$. Ако $bc \in B$, од тоа што $b \in B$ следува дека и $c \in B$, т.е. $A \subseteq B$. Ако пак $bc \in C$, тогаш од $c \in C$ следува дека и $b \in C$, т.е. $A \subseteq C$. Значи, во секој случај имаме $A \subseteq B$ или $A \subseteq C$.

6.47. Нека

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{bmatrix}, \begin{bmatrix} \varepsilon^2 & 0 \\ 0 & \varepsilon \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \varepsilon^2 \\ \varepsilon & 0 \end{bmatrix}, \begin{bmatrix} 0 & \varepsilon \\ \varepsilon^2 & 0 \end{bmatrix} \right\},$$

каде што ε е примитивен трети корен од единицата. Да се покаже дека G е група во однос на операцијата множење на матрици. Да се најдат сите подгупи од G.

6.48. Да се најде [1] во групата $\mathbb{Z}(+)$.

Решение. Бидејќи $n = \underbrace{1+1+\ldots+1}_{n}$, следува дека $n\in[1]$ за секој $n\in\mathbb{N}$, а бидејќи $-n = \underbrace{-1+(-1)+\ldots+(-1)}_{n}$, следува дека и $-n\in[1]$, за секој $n\in\mathbb{N}$. На крајот, од $0 = 1+(-1)$ следува дека и $0\in[1]$, па според тоа $[1] = \mathbb{Z}$.

6.49. Да се најде подгрупата [2] во $\mathbb{Q}^*(\cdot)$.

Решение. Бидејќи е $2^{-1} = \frac{1}{2}$, следува дека подгрупата [2] ги содржи сите рационални броеви со облик 2^n или 2^{-n} за секој $n\in\mathbb{N}$.

6.50. Да се најде подгрупата од S_3 генерирана од

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ и } \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Решение. Од шемата на S_3 (види 5.36) се гледа дека $\rho_1^{-1} = \rho_2$, па ако $H = [\{\rho_1, \sigma_1\}]$, тогаш $\rho_2\in H$. Бидејќи $\sigma_1\in H$, а $\sigma_2 = \rho_2\sigma_1$ и $\sigma_3 = \rho_1\sigma_1$, следува дека и $\sigma_2, \sigma_3\in H$. Значи, $H = S_3$.

6.51. Нека H е вистинска подгрупа од групата G, т.е. $\{e\}\subset H \subset G$. Да се покаже дека $[G \setminus H] = G$.

Решение. За да покажеме дека $[G \setminus H] = G$, треба да покажеме дека секој елемент $x\in G$ може да се претстави како конечен производ на елементи од $G \setminus H$. Ако $x\in G \setminus H$, тоа е јасно. Затоа, да претпоставиме дека $x\in H$. Од $\{e\} \subset H \subset G$ следува дека постои барем еден елемент $a\in G \setminus H$. Бидејќи G е група, за a и x постои единствен елемент $b\in G$, таков што

$$ab = x. \tag{1}$$

Ако $b\in H$, тогаш од (1) имаме $a = xb^{-1}$, па $a\in H$, спротивно на претпоставката дека $a\in G \setminus H$. Значи, $b\in G \setminus H$, т.е. x е претставен со (1) како производ на $a, b\in G \setminus H$; тоа значи дека $[G \setminus H] = G$.

6.52. Ако

$$P = \left\{ \frac{1}{p} \middle| \, p \in \mathbb{N},\ p - \text{прост} \right\}$$

го сметаме како подмножество од $\mathbb{Q}^+(\cdot)$, покажи дека $[P] = \mathbb{Q}^+$.

Решение. За да го покажеме тоа, треба да покажеме дека секој позитивен рационален број може да се претстави како конечен производ на елементи од P или нивни инверзии. Затоа, нека $x = \frac{a}{b} \in \mathbb{Q}^+$. Ако $a = p_1 p_2 \ldots p_r$ и $b = q_1 q_2 \ldots q_s$ се напишани како производи на прости броеви, не мора различни, тогаш имаме:

$$x = \frac{a}{b} = p_1 p_2 \ldots p_r \cdot \frac{1}{q_1} \cdot \frac{1}{q_2} \ldots \frac{1}{q_s} =$$

$$= \left(\frac{1}{p_1}\right)^{-1} \left(\frac{1}{p_2}\right)^{-1} \ldots \left(\frac{1}{p_r}\right)^{-1} \cdot \frac{1}{q_1} \frac{1}{q_2} \ldots \frac{1}{q_s},$$

што значи $[P] = \mathbb{Q}^+$.

§ 7. ПРСТЕНИ

7.1. Нека $R(+,\cdot)$ е асоцијативен прстен и нека во R определиме две нови операции "$\circ$" и "$\otimes$" со:

$a \circ b = ab - ba, \quad a \otimes b = ab + ba.$

Да се покаже дека $R(+, \circ)$ и $R(+, \otimes)$ се исто така прстени, при што $R(+,\circ)$ е лиев.

Решение. Треба да се покажат само дистрибутивните закони на операциите $\circ$ и $\otimes$ спрема $+$. Имаме:

$$a\circ(b+c) = a(b+c) - (b+c)a = ab + ac - ba - ca =$$
$$= (ab - ba) + (ac - ca) = a\circ b + a \circ c,$$
$$(b+c)\circ a = (b+c)a - a(b+c) = ba + ca - ab - ac =$$
$$= (ba - ab) + (ca - ac) = b\circ a + c\circ a,$$

што значи дека $R(+,\circ)$ е прстен. Слично за $R(+,\otimes)$.

Бидејќи

$a\circ a = aa - aa = 0$ и

$$(a \circ b) \circ c + (b \circ c) \circ a + (c \circ a) \circ b =$$
$$= (ab - ba) \circ c + (bc - cb) \circ a + (ca - ac) \circ b =$$
$$= (ab - ba)c - c(ab - ba) + (bc - cb)a - a(bc - cb) +$$
$$+ (ca - ac)b - b(ca - ac) =$$
$$= abc - bac - cab + cba + bca - cba - abc +$$
$$+ acb + cab - acb - bca + bac = 0,$$

добиваме дека прстенот $R(+,\circ)$ е *лиев.*

7.2. Нека $R(+,\cdot)$ е прстен и нека во R е определена нова операција "$\circ$" со:

$(\forall a, b \in R) \; a\circ b = a + b + ab.$

Да се покаже дека:

а) $R(\circ)$ е полугрупа ако и само ако прстенот е асоцијативен.

б) во алгебрата $R(+, \circ)$ се исполнети условите

$$(\forall a, b, c \in \mathbb{R}) \; a \circ (b + c) = a \circ b + a \circ c - a,$$
$$(a + b) \circ c = a \circ c + b \circ c - c. \qquad (1)$$

в) ако $R(+, \circ)$ е алгебра, таква што $R(+)$ е комутативна група и се исполнети условите (1) и ако во R определиме нова операција "$*$" со:

$(\forall a, b \in R) \; a * b = a \circ b - a - b.$

тогаш алгебрата $R(+, *)$ е прстен.

Решение. а) Нека прстенот $R(+,\cdot)$ е асоцијативен; тогаш имаме:

$$(a \circ b) \circ c = (a + b + ab) \circ c = a + b + ab + c + (a + b + ab)c =$$
$$= a + b + ab + c + ac + bc + (ab)\, c =$$

$= a + (b + c + bc) + ab + ac + a(bc) =$
$= a + (b + c + bc) + a(b + c + bc) =$
$= a \circ (b + c + bc) = a \circ (b \circ c),$

т.е. $R(\circ)$ е полугрупа.

Обратно, нека $R(\circ)$ е полугрупа. Од $a \circ b = a + b + ab$ добиваме $ab = a \circ b - a - b$, па имаме:

$$(ab)c = (a \circ b - a - b)c = (a \circ b)c - ac - b\,c =$$
$$= (a \circ b) \circ c - a \circ b - c - a \circ c + a + c - b \circ c + b + c =$$
$$= (a \circ b) \circ c - a \circ b - a \circ c - b \circ c + a + b + c =$$
$$= (a \circ (b \circ c) - b \circ c - a) - (a \circ b - a - b) - (a \circ c - a - c) =$$
$$= a(b \circ c) - ab - ac = a(b \circ c - b - c) = a(bc),$$

т.е. прстенот $R(+,\cdot)$ е асоцијативен.

б) Имаме:

$$a \circ (b + c) = a + b + c + a(b + c) = a + b + c + ab + ac =$$
$$= (a + b + ab) + (a + c + ac) - a =$$
$$= a \circ b + a \circ c - a;$$
$$(a + b) \circ c = a + b + c + (a + b)c = a + b + c + ac + bc =$$
$$= (a + c + ac) + (b + c + bc) - c =$$
$$= a \circ c + b \circ c - c.$$

в) За да покажеме дека алгебрата $R(+, *)$ е прстен, доволно е да покажеме дека се исполнети равенствата

$$a * (b + c) = a * b + a * c,$$
$$(a + b) * c = a * c + b * c.$$

Бидејќи операцијата $*$ е определена со

$$a * b = a \circ b - a - b,$$

ќе имаме:

$$a * (b + c) = a \circ (b + c) - a - b - c =$$
$$= a \circ b + a \circ c - a - a - b - c =$$
$$= (a \circ b - a - b) + (a \circ c - a - c) =$$
$$= a * b + a * c;$$
$$(a + b) * c = (a + b) \circ c - a - b - c =$$
$$= a \circ c + b \circ c - c - a - b - c =$$
$$= (a \circ c - a - c) + (b \circ c - b - c) =$$
$$= a * c + b * c.$$

7.3. Нека M е дадено непразно множество и $P = \mathbb{P}(M)$ е партитивното множество од M, а F фамилијата од сите конечни подмножества од M. Во P определуваме две операции "+" и "·" со:

$$A + B = A \,\Delta\, B; \quad AB = A \cap B\,.$$

Да се покаже дека:

а) P е асоцијативен и комутативен прстен, а F е потпрстен од P.

б) Ако M е бесконечно множество, тогаш во прстенот F нема единица.

7.4. Ако $M = \{1, 2, 3\}$, а $\mathbb{P}(M) = R$, да се напишат шемите на операциите на прстенот $R(\Delta, \cap)$. Потоа, да се најдат сите потпрстени на R.

Решение. Да ставиме $R = \{\varnothing, A_1, A_2, A_3, B_1, B_2, B_3, M\}$, каде што $A_i = \{i\}$, $i = 1, 2, 3$, а $B_i = \{j, k\}$, $j, k \neq i$. Имаме:

Δ	$\varnothing$	A_1	A_2	A_3	B_1	B_2	B_3	M
$\varnothing$	$\varnothing$	A_1	A_2	A_3	B_1	B_2	B_3	M
A_1	A_1	$\varnothing$	B_3	B_2	M	A_3	A_2	B_1
A_2	A_2	B_3	$\varnothing$	B_1	A_3	M	A_1	B_2
A_3	A_3	B_2	B_1	$\varnothing$	A_2	A_1	M	B_3
B_1	B_1	M	A_3	A_2	$\varnothing$	B_3	B_2	A_1
B_2	B_2	A_3	M	A_1	B_3	$\varnothing$	B_1	A_2
B_3	B_3	A_2	A_1	M	B_2	B_1	$\varnothing$	A_3
M	M	B_1	B_2	B_3	A_1	A_2	A_3	$\varnothing$

Шема 1.

$\cap$	$\varnothing$	A_1	A_2	A_3	B_1	B_2	B_3	M
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
A_1	$\varnothing$	A_1	$\varnothing$	$\varnothing$	$\varnothing$	A_1	A_1	A_1
A_2	$\varnothing$	$\varnothing$	A_2	$\varnothing$	A_2	$\varnothing$	A_2	A_2
A_3	$\varnothing$	$\varnothing$	$\varnothing$	A_3	A_3	A_3	$\varnothing$	A_3
B_1	$\varnothing$	$\varnothing$	A_2	A_3	B_1	A_3	A_2	B_1
B_2	$\varnothing$	A_1	$\varnothing$	A_3	A_3	B_2	A_1	B_2
B_3	$\varnothing$	A_1	A_2	$\varnothing$	A_2	A_1	B_3	B_3
M	$\varnothing$	A_1	A_2	A_3	B_1	B_2	B_3	M

Шема 2.

Нетривијални потпрстени од R се:
$R_i = \{\varnothing, A_i, B_i, M\}$, $i = 1, 2, 3$.

7.5. Да се покаже дека во секој комутативен и асоцијативен прстен R е точна биномната формула, т.е.

$$(\forall a, b \in R, n \in \mathbb{N})\ (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i ,$$

каде што $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.

Упатство. Со индукција по n.

7.6. Нека $R(+,\cdot)$ е алгебра со две операции што ги задоволува следниве услови:

(i) $R(+)$ е група;

(ii) $R(\cdot)$ е групоид;

(iii) $x(y+z) = xy + xz, \quad (y+z)x = yx + zx.$

Ако $\mathbb{R}(\cdot)$ има десна единица, тогаш $R(+,\cdot)$ е прстен.

Решение. За да покажеме дека $R(+,\cdot)$ е прстен, доволно е да покажеме дека групата $R(+)$ е комутативна. Нека e е десна единица во $\mathrm{R}(\cdot)$. Тогаш имаме:

$0 = b(e + (-e)) = be + b(-e) = b + b(-e),$ т.е.

$b(-e) = -b;$

$0 = (-b) + (-a) + a + b = b(-e) + a(-e) + a + b =$

$= (b+a)(-e) + a + b,$ т.е.

$a + b = -((b+a)(-e))$ (1)

$(b+a)+(b+a)(-e) = (b+a)e + (b+a)(-e) = (b+a)(e+(-e)) = 0$ т.е.

$b + a = -((b+a)(-e)).$ (2)

Од (1) и (2) следува $a + b = b + a$, т.е. групата $R(+)$ е комутативна.

7.7. Нека $R(+,\cdot)$ е алгебра со две операции што ги задоволува условите (i), (ii) и (iii) од 7.6, како и условот:

(iv) $(\exists a \in R)\ (\forall x, y \in R) \quad ax = ay \Rightarrow x = y.$

Да се покаже дека $R(+,\cdot)$ е прстен.

Решение: Нека x, y се произволни елементи од R. Според (iii) имаме:

$(a+a)(x+y) = a(x+y) + a(x+y) = ax + ay + ax + ay,$

$(a+a)(x+y) = (a+a)x + (a+a)y = ax + ax + ay + ay,$ т.е.

$ax + ay + ax + ay = ax + ax + ay + ay,$

од каде што добиваме

$ay + ax = ax + ay,$ т.е. $a(y+x) = a(x+y).$

Од ова, според условот (iv), следува $y + x = x + y$, т.е. групата $R(+)$ е комутативна, па значи, алгебрата $R(+,\cdot)$ е прстен.

7.8. Нека R е прстен со единица и го задоволува условот

$(\forall x, y \in R)\ (xy)^2 = x^2y^2$. (*)

Да се покаже дека R е комутативен. Дали важи истото ако прстенот R нема единица? Дали условот (*) може да се замени со условот

$(xy)^k = x^k y^k,\ k > 2$?

***Решение*:** Нека $x, y \in R$; тогаш имаме

$[x(y + 1)]^2 = x^2(y + 1)^2 = x^2y^2 + 2x^2y + x^2$,

$[x(y + 1)]^2 = [xy + x]^2 = (xy)^2 + (xy)x + x(xy) + x^2$, па значи

$(xy)x + x(xy) = 2x^2y$. (1)

Ако во (1) наместо x ставиме $x + 1$ добиваме

$[(x + 1)y]\ (x + 1) + (x + 1)\ [(x + 1)y] = 2(x + 1)^2y$,

коешто се сведува на

$(xy)x + yx + x(xy) = 2x^2y + xy$,

од каде што, користејќи го (1), добиваме $xy = yx$, т.е. прстенот R е комутативен.

Ако прстенот R нема единица, тогаш тој не мора да биде комутативен. На пример , ако

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\}$$

тогаш важи равенството $(xy)^2 = x^2y^2$, но R не е комутативен.

Условот $(xy)^2 = x^2y^2$ не може да се замени со $(xy)^k = x^k y^k$ за $k > 2$. На пример, нека $k \geq 3$ е зададен, а p нека е прост број што го задоволува условот :

1) ако k е непарен, тогаш $p \mid k$;

2) ако k е парен, тогаш $p \mid \frac{k}{2}$

$$\text{Ако } R = \left\{ \begin{bmatrix} a & b & c \\ 0 & a & d \\ 0 & 0 & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{Z}_p \right\}$$

тогаш R е прстен со единица, во кој е точно равенството $(xy)^k = x^k y^k$, но R не е комутативен.

7.9 *Лева единица* на еден прстен R е секоја лева единица на неговиот мултипликативен групоид. Да се покаже дека, ако еден асоци-

јативен прстен има само една лева единица, тогаш тој прстен има и единица. Да се покаже дека подмножеството S од матрици со обликот $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ $(a,\ b\in\mathbb{Z})$ е потпрстен од прстенот M_2 од сите матрици со елементи цели броеви и дека во S има безброј многу леви единици

Решение. Нека e е лева единица во прстенот R, т.е.

$(\forall x\in R)\ \ ex = x.$

Тогаш имаме:

$(xe - x + e)y = (xe)y - xy + ey = x(ey) - xy + y = xy - xy + y = y,$

па значи елементот $xe - x + e$ е исто така лева единица. Бидејќи R има единствена лева единица e следува дека

$xe - x + e = e,$ т.е. $\quad xe = x, \quad x\in R$

Значи, e е и десна единица, т.е. прстенот R е со единица.

Лесно се покажува дека S е потпрстен од M_2, а секој елемент $\begin{bmatrix} 1 & c \\ 0 & 0 \end{bmatrix}$, $c\in\mathbb{Z}$ е лева единица во S.

7.10. Елементот a од еден асоцијативен прстен R се вика *нилпотент* ако $a^n = 0$ за некој $n\in\mathbb{N}$. Да се најде бројот на нилпотентите кај секој од прстените $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_{20}$ и $\mathbb{Z}_{1000}$. Каков треба да биде природниот број n, во $\mathbb{Z}_n$ да нема ненулти нилпотенти?

Решение. Ненулти нилпотенти во $\mathbb{Z}_6$, и $\mathbb{Z}_7$ нема; во $\mathbb{Z}_4$, и $\mathbb{Z}_{20}$ има само по еден и тоа нилпотент во $\mathbb{Z}_4$ е 2, а во $\mathbb{Z}_{20}$ е 10; во $\mathbb{Z}_{1000}$ постојат 99 и тоа се сите оние броеви помали од 1000 што завршуваат со нула.

Да видиме сега за кои n во прстенот $\mathbb{Z}_n$ нема ненулти нилпотенти. Да го напишеме n во обликот

$$n = p_1^{\alpha_1} p_2^{\alpha_i} \dots p_r^{\alpha_r},$$

каде што $p_1, p_2, \dots, p_r$ се различни прости броеви.

Ако барем еден од α_i, $i = 1, 2, \dots, r$, е поголем од единица, да го означиме со α најголемиот од нив. За $m = p_1 p_2 \dots p_r$ имаме:

$$m^\alpha = (p_1 p_2 \dots p_r)^\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \dots p_1^{\alpha-\alpha_1} \dots p_r^{\alpha-\alpha_r} =$$

$$= n \cdot p_1^{\alpha-\alpha_1} \dots p_r^{\alpha-\alpha_r}$$

што значи дека $m^\alpha \equiv 0 \pmod n$, т.е. m е нилпотент.

Затоа, нека $n = p_1 p_2 \dots p_r$, каде што $p_1 p_2 \dots p_r$, се различни прости броеви. Ако m е нилпотент во $\mathbb{Z}_n$, тогаш од $m^k \equiv 0 \pmod n$

следува дека $p_1 p_2 \dots p_r \mid m^k$, од каде што пак следува дека $p_i \mid m^k$, за $i = 1, 2, \dots, r$, т.е. $p_i \mid m$ за $i = 1, 2, \dots, r$. Меѓутоа $m < n$, па следува дека $m = 0$.

Значи, во $\mathbb{Z}_n$ нема ненулти нилпотенти ако и само ако n не се дели со квадратот на ниеден прост број.

7.11. Нека R е асоцијативен ненулти прстен, таков што
$(\forall a \in R\,;\ a \neq 0)\ (\exists!\ a' \in R)\ \ aa'a = a.$
Да се докаже дека R е тело.

Решение. Да покажеме прво дека во R нема вистински делител на нулата. Затоа нека $a \neq 0$ и $ac = 0$. Тогаш имаме:

$a = a'a + aca = a(a' + c)a$, т.е.

$a' + c = a'$,

од што следува дека $c = 0$. Слично, од $ba = 0$ и $a \neq 0$, следува $b = 0$. Понатаму имаме $aa'a = a$, $a'aa'aa' = a'aa'$, $a'aa' = a'$. Нека $xaa' = y$; тогаш $xaa'a = ya$, $xa = ya$, $x = y$, т.е. aa' е десна единица. Слично, добиваме дека $a'a$ е лева единица, па $aa' = a'a = 1$, т.е. прстенот R има единица и притоа a' е инверзен елемент на a. Значи прстенот R е тело.

7.12. Да се покаже дека секој конечен асоцијативен прстен без делители на нулата е тело.

Решение. Нека R е конечен асоцијативен прстен без делители на нулата. Во секој прстен без делители на нулата исполнет е законот за кратење.

Навистина, нека $ax = bx$; тогаш имаме $(a - b)x = 0$, па ако $x \neq 0$, тогаш $a - b = 0$, т.е. $a = b$. Слично, од $xa = xb$, при $x \neq 0$ следува $a = b$.

Значи $R^*(\cdot)$ е конечен групоид со кратење, а според 6.38, $R^*(\cdot)$ е квазигрупа. (Притоа $R^* = R \setminus \{0\}$). Од друга страна $R^*(\cdot)$ е полугрупа, па следува дека $R^*(\cdot)$ е група. Според тоа, прстенот R е тело.

7.13. Да се даде пример на тело што не е поле.

Решение. 1) * Нека K е множеството од сите "броеви" $a + bi + cj + dk$, каде што a, b, c, d се реални броеви. Ако во K дефинираме операција собирање и множење со :

$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) =$
$= (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k,$

$(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) =$
$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + a_2 b_1 + c_1 d_2 - c_2 d_1) i +$
$+ (a_1 c_2 + a_2 c_1 + b_2 d_1 - b_1 d_2) j + (a_1 d_2 + a_2 d_1 + b_1 c_2 - b_2 c_1) k,$

добиваме тело што не е поле. Ова тело се вика тело на *кватерниони.*

2) Множеството M од сите реални матрици од четврти ред со облик

$$\begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}$$

во однос на операцијата собирање и множење на матрици е тело што не е поле.

Да забележиме дека $M(+,\cdot)$ е изоморфно со $K(+,\cdot)$ при изоморфизмот

$$\varphi(a + bi + cj + dk) = \begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix}$$

7.14. Нека R е асоцијативен прстен и e фиксен елемент од R т.ш.

$e + y + ey \neq 0 \quad \forall y \in R.$

Да се покаже дека важи

$(\forall x \in R;\ x \neq e)(\exists y \in R) \quad x + y + xy = 0$ (1)

ако и само ако R е тело.

Решение. Бидејќи за $x = 0$ е исполнет условот (1), зашто, на пример, за $y = 0$ имаме $x + y + xy = 0$, следува дека елементот e е различен од 0, $e \neq 0$.

Нека во прстенот R е исполнет условот (1). Бидејќи

$e + y + ey \neq 0 \quad \forall y \in R,$

ставајќи $y = -e + z - ez$, добиваме

$0 \neq e + (-e + z - ez) + e(-e + z - ez) = -e^2 + z - e^2 z,$

што значи условот (1) не е исполнет и за $-e^2$. Според тоа, имаме $-e^2 = e$, т.е.

$e^2 + e = 0.$ (2)

Ако постои $x \in R$, таков што $x + ex \neq 0$, тогаш и $e + x + ex \neq e$, а од тоа следува дека постои $y \in R$, таков што

$e + x + ex + y + (e + x + ex)y = 0.$

Множејќи го ова равенство одлево со e, добиваме

$e^2 + ex + e(ex) + ey + e(ey) + e(xy) + e((ex)y) = 0,$

$e^2 + (e + e^2)x + (e + e^2)y + (e + e^2)xy = 0,$

од каде што, според (2), добиваме $e^2 = 0$, т.е. $e = 0$ што е невозможно. Значи имаме:

$(\forall x \in R) \quad x + ex = 0.$

Слично добиваме дека важи и

$(\forall x \in R) \quad x + xe = 0,$

т.е. $-e$ е единица во R.

Нека $x \neq e$ е кој било елемент од R. Според (1), постои $y \in R$, така што $x + y + xy = 0$, коешто може да се напише во обликот

$(x - e)(y - e) = -e,$

т.е. секој елемент $u = x - e \neq 0$, е инверзибилен, при што $u^{-1} = v = y - e$. Значи R е тело.

Обратно, нека R е тело и $x \neq -1$ е кој било елемент од R. Тогаш $x + 1 \neq 0$, па постои $(x + 1)^{-1}$, којшто може да се напише во обликот $y + 1$. Од $(x + 1)(y + 1) = 1$ следува $x + y + xy = 0$, т.е. исполнет е условот (1).

7.15. Дадена е реалната матрица A од ред n.

а) Ако K_n е множеството од сите реални матрици со ред n што комутираат со A, тогаш $K_n(+,\cdot)$ е потпрстен од прстенот $M_n(+,\cdot)$ од сите матрици со ред n.

б) Ако матрицата A е дијагонална, чии елементи по дијагоналата се меѓусебно различни, да се најде соодветниот потпрстен $K_n(+,\cdot)$.

Решение. а) Нека $B, C \in K_n$, т.е.

$AB = BA, \quad AC = CA;$

Поради асоцијативноста на множењето на матрици, имаме:

$A(BC) = (AB)C = (BA)C = B(AC) =$

$= B(CA) = (BC)A,$

т.е. $BC \in K_n$. Понатаму, поради дистрибутивноста, имаме:

$A(B - C) = AB - AC = BA - CA = (B - C)A,$

па и $B - C \in K_n$. Значи, K_n е потпрстен од M_n.

б) $K_n = \{X \mid X \in M_n, X \text{ е дијагонална}\}$.

7.16. Нека p е прост број. Да се покаже дека:

а) Множеството $\mathbb{Q}_p = \left\{ \frac{a}{b} \;\middle|\; \frac{a}{b} \in \mathbb{Q}, (b,p)=1 \right\}$

е потпрстен од $\mathbb{Q}$. Дали е потполе?

б) Множеството $G = \mathbb{Q}_p \cap \mathbb{Q}_p^{-1}$ е група во однос на операцијата множење на рационални броеви.

7.17. Нека $I = \{1, 2, \ldots, n\}$, $\alpha \subseteq I \times I$, а M_α е множеството на сите матрици $A = [a_{ij}]$ со ред n, над едно поле F, такви што

$(i,j) \in (I \times I) \setminus \alpha \Rightarrow a_{ij} = 0$.

Да се даде карактеристика на сите релации α, такви што M_α е потпрстен од прстенот R на сите матрици со ред n над F.

Решение. Да забележиме прво дека

$$M_\alpha = \{A = [a_{ij}] \mid a_{ij} \neq 0 \Rightarrow (i,j) \in \alpha\}$$

и дека $M_\alpha(+)$ е комутативна група. Значи, M_α е потпрстен од R ако и само ако $M_\alpha(\cdot)$ е подгрупоид од групоидот $R(\cdot)$.

За $(i, j) \in \alpha$, да ставиме E_{ij} да биде матрицата за која $a_{ij} = 1$, $a_{\nu\lambda} = 0$, за $\nu \neq i$ и $\lambda \neq j$. Јасно е дека $E_{ij} \in M_\alpha$. Ако E_{ir} и E_{rj} се две такви матрици, тогаш од равенството

$$E_{ir}E_{rj} = E_{ij},$$

следува дека $E_{ir}E_{rj} \in M_\alpha$, т.е.

$$(i, r), (r, j) \in \alpha \Rightarrow (i, j) \in \alpha.$$

Значи, ако M_α е потпрстен од R тогаш релацијата α е транзитивна.

Да претпоставиме сега дека α е транзитивна релација. Нека $A, B \in M_\alpha$ и $AB \neq 0$ (зашто ако $AB = 0$, тогаш $AB \in M_\alpha$). Ако $AB = [c_{ij}]$, нека ν, λ се такви што $c_{\nu\lambda} \neq 0$. Имаме

$$c_{\nu\lambda} = \sum_{\mu \in I} a_{\nu\mu} b_{\mu\lambda} = \sum_{\mu \in J} a_{\nu\mu} b_{\mu\lambda},$$

каде што

$$J = \{\mu \mid \mu \in I, a_{\nu\mu} \neq 0, b_{\mu\lambda} \neq 0\} = \{\mu \mid \mu \in I, (\nu, \mu) \in \alpha, (\mu, \lambda) \in \alpha\}.$$

Бидејќи α е транзитивна релација, следува дека и $(\nu, \lambda) \in \alpha$ т.е. $AB \in M_\alpha$.

Значи, M_α е потпрстен на R ако и само ако релацијата α е транзитивна.

7.18. Нека R е прстен со единица и нека

$A = \{x \mid x \in R, x$ не е инверзибилен$\}$,

$B = \{x \mid x \in R, x$ не е лево инверзибилен$\}$,

$C = \{x \mid x \in R, x$ не е десно инверзибилен$\}$.

Да се покаже дека множествата A, B и C се еднакви ако и само ако едното од нив е групоид во однос на собирањето во R.

Решение. Нека $a \in A$. Ако $a \notin B \cap C$, тогаш $a \notin B$, или $a \notin C$. Да претпоставиме дека $a \notin B$. Тоа значи дека a е лево инверзибилен, т.е. постои елемент $x \in R$, таков што $xa = 1$, од каде што следува $a = axa \neq 0$. Од $a \in A$, следува дека $1 - ax \neq 0$, а бидејќи $ax = axax$ следува дека $ax(1-ax) = 0$ и $(1-ax)ax = 0$. Значи, ax, $-ax \in A \cap B \cap C$. Од ова следува дека, ако едно од множествата A, B или C е групоид во однос на собирањето, тогаш и $1 = ax + (1 - ax)$ припаѓа на тоа множество, коешто не е можно, зашто 1 е инверзибилен елемент. Значи, $a \in B$. Слично добиваме дека $a \in C$, т.е. $A \subseteq B \cap C$. Од друга страна, јасно дека е $B \cap C \subseteq A$, па $A = B \cap C$. Равенството $A = B \cap C$ повлекува $A = B = C$.

7.19. Да се определи бројот на меѓусебно неизоморфни прстени со два и три елементи.

Решение. За кој било природен број постои барем една група (6.16), па следствено постои барем еден прстен–нултиот. Бидејќи со два односно со три елементи постои само една група, којашто е комутативна, постои само еден нулти прстен со два односно со три елементи. Понатаму ќе ги бараме само ненултите меѓусебно неизоморфни прстени. Еден од елементите ќе го означиме со 0 и ќе го сметаме за неутрален елемент на $R(+)$.

Нека $R = \{0, a\}$. Соодветната група е дадена со шемата 1,

$+$	0	a
0	0	a
a	a	0

Шема 1

$\cdot$	0	a
0	0	0
a	0	a

Шема 2

па за да не биде $R(+,\cdot)$ нулти прстен, множењето може да се дефинира само со шемата 2. Очигледно е дека дистрибутивните закони се исполнети. Значи, со два елемента постојат само два неизоморфни прстени, еден е нултиот, а другиот е поле.

Нека $R = \{0, a, b\}$. Соодветната група $R(+)$ е дадена со шемата 3. Да дефинираме множење во R. Ако

+	0	a	b
0	0	a	b
a	a	b	0
b	b	0	a

шема 3

·	0	a	b
0	0	0	0
a	0	a	b
b	0	b	a

шема 4

·	0	a	b
0	0	0	0
a	0	b	a
b	0	a	b

шема 5

$xx = 0$ за $x = a$ или за $x = b$, тогаш мора да е:

$xy = x(x + x) = xx + xx = 0$,

$yy = (x + x)y = xy + xy = 0$,

т.е. $R(+, .)$ е нулти прстен. Значи, треба да земеме $aa \neq 0$, па aa може да биде или a, или b. Ако $aa = a$, тогаш мора да е:

$ab = a(a + a) = aa + aa = a + a = b$,

$ba = (a + a)a = aa + aa = a + a = b$,

$bb = b(a + a) = ba + ba = b + b = a$,

па $R(\cdot)$ ќе биде зададен со шемата 4. Ако пак $aa = b$, тогаш мора да е:

$ab = a(a + a) = aa + aa = b + b = a$,

$ba = (a + a)a = aa + aa = b + b = a$,

$bb = (a + a)b = ab + ab = a + a = b$,

па $R(\cdot)$ ќе биде зададен со шемата 5. На тој начин добиваме два прстени коишто се изоморфни, па значи со три елементи постојат само два неизоморфни прстени, еден е нултиот, а другиот е поле.

7.20. Да се најде бројот на меѓусебно неизоморфните прстени со четири елементи, ако адитивната група на прстенот е цикличната група со четири елементи.

Решение. Ако $R = \{0, a, b, c\}$, тогаш групата $R(+)$ е дадена со шемата 1.

	0	a	b	c
0	0	a	b	c
a	a	b	c	0
b	b	c	0	a
c	c	0	a	b

Шема 1

Да дефинираме множење, така што $R(+,\cdot)$ е прстен.

Елементот aa може да биде 0, a, b, или c. Ако $aa = 0$, тогаш се добива нултиот прстен.

Ако $aa = a$, тогаш мора да е:

$ab = a(a + a) = a + a = b$, $\qquad ba = (a + a)a = a + a = b$,

$ac = a(a+b) = aa + ab = a + b = c$, $\quad ca = (a+b)a = aa + ba = c$,
$bc = (a+a)c = ac + ac = c + c = b$, $\quad cb = c(a+a) = b$,
$bb = (a+a)b = ab + ab = b + b = 0$, $\quad cc = (a+b)c = c + b = a$,

па $R(\cdot)$ е дефиниран со шемата 2.

$\cdot$	0	a	b	c
a	0	0	0	0
a	0	a	b	c
b	0	b	0	b
c	0	c	b	a

Шема 2

$\cdot$	0	a	b	c
0	0	0	0	0
a	0	b	0	b
b	0	0	0	0
c	0	b	0	b

Шема 3

Алгебрата $R(+,\cdot)$, при што " +" и "$\cdot$" се определени со шемите 1 и 2, е изоморфна со прстенот $\mathbb{Z}_4$, па и $R(+,\cdot)$ е прстен.

Ако $aa = b$, тогаш мора да е

$ab = a(a+a) = b + b = 0$, $\quad ba = (a+a)b = 0 + 0 = 0$,
$ac = a(a+b) = aa + ab = b$, $\quad ca = (a+b)a = aa + ba = b$,
$bc = (a+a)c = ac + ac = b + b = 0$, $\quad cb = c(a+a) = 0$,
$bb = (a+a)b = ab + ab = 0$, $\quad cc = (a+b)c = ac + bc = b$,

па $R(\cdot)$ е зададено со шемата 3. Бидејќи $R(\cdot)$ е комутативен, за проверка дали алгебрата $R(+,\cdot)$ е прстен, доволно е да се провери само едниот дистрибутивен закон, на пример левиот:

$x(y+z) = xy + xz$.

Јасно е дека ова равенство е исполнето за $x = 0$ и $x = b$. Имајќи ги предвид равенствата од горната дискусија, останува да се извршат следните проверки (од шемите 1 и 3):

$a(a+c) = a0 = 0$, $\quad aa + ac = b + b = 0$,
$a(b+c) = aa = b$, $\quad ab + ac = 0 + b = b$,
$a(b+b) = a0 = 0$, $\quad ab + ab = 0 + 0 = 0$,
$a(c+c) = ab = 0$, $\quad ac + ac = b + b = 0$,
$c(b+b) = c0 = 0$, $\quad cb + cb = 0 + 0 = 0$
$c(b+c) = ca = b$, $\quad cb + cc = 0 + b = b$,
$c(a+c) = c0 = 0$, $\quad ca + cc = b + b = 0$,
$c(c+c) = cb = 0$, $\quad cc + cc = b + b = 0$.

Според тоа, $R(+,\cdot)$ е прстен, којшто не е изоморфен со прстенот дефиниран со шемите 1 и 2.

Ако $aa = c$, слично како и за претходните случаи, за $R(\cdot)$ ја добиваме шемата 4.

·	0	*a*	*b*	*c*
0	0	0	0	0
a	0	*c*	*b*	*a*
b	0	*b*	0	*b*
c	0	*a*	*b*	c

Шема 4

Алгебрата $R(+,\cdot)$, каде што " + " и "·" се дефинирани со шемите 1 и 4, е изоморфна со прстенот $R(+,\cdot)$ определен со шемите 1 и 2 при изоморфизмот $a \to c,\ b \to b,\ c \to a$.

Значи, постојат три меѓусебно неизоморфни прстени со четири елементи, при што адитивната група е циклична, и тоа нултиот прстен, прстенот определен со шемите 1 и 2 односно 1 и 4, и прстенот определен со шемите 1 и 3.

7.21. а) Колку прстени можат да се конструираат на множеството $R = \{0, a, b, c\}$ ако адитивната група е зададена со шемата

+	0	*a*	*b*	*c*
0	0	*a*	*b*	*c*
a	*a*	0	*c*	*b*
b	*b*	*c*	0	*a*
c	*c*	*b*	*a*	0

б)* Колку од овие прстени се неизоморфни ?

Решение. а) Да дефинираме множење во R, така што алгебрата $R(+,\cdot)$ да биде прстен. Да ставиме $aa = \alpha$, $ab = \beta$; тогаш имаме

$ac = a(a + b) = \alpha + \beta$.

Слично, ако ставиме $ba = \gamma$, $bb = \delta$, добиваме

$bc = \gamma + \delta$, $ca = \alpha + \gamma$, $cb = \beta + \gamma$ и $cc = \alpha + \beta + \gamma + \delta$.

Според тоа, множењето е определено со следнава шема

·	0	*a*	*b*	*c*
0	0	0	0	0
a	0	α	β	$\alpha + \beta$
b	0	γ	β	$\gamma + \delta$
c	0	$\alpha + \gamma$	$\beta + \delta$	$\alpha + \beta + \gamma + \delta$

каде што α, β, γ и δ се произволни елементи од R. Лесно се проверува дека за кој било избор на α, β, γ и δ се исполнети дистрибутивните закони, па значи, со секој избор на α, β, γ и δ се добива прстен. Според тоа, на множеството $R = \{0, a, b, c\}$ можат да се конструираат $4^4 = 256$ прстени.

7.22. Нека $G(+)$ е комутативна група. Во множеството $R = \mathrm{End}G$ определуваме операции собирање и множење со:

$f_1 + f_2 = g \Leftrightarrow (\forall x \in G)\ g(x) = f_1(x) + f_2(x)$,

$f_1 f_2 = h \Leftrightarrow (\forall x \in G)\ h(x) = f_1(f_2(x))$.

Да се покаже дека $R(+,\cdot)$ е асоцијативен прстен со единица.

Решение. Јасно дека $R(+)$ е комутативна група, при што нула е ендоморфизмот ω дефиниран со $(\forall x \in G)\ \omega(x) = 0$, а ако $f \in R$, тогаш спротивен на f е пресликувањето g, дефинирано со $(\forall x \in G)$ $g(x) = -f(x)$. Лесно се проверува дека $R(\cdot)$ е полугрупа со единица. Значи, за да покажеме дека $R(+,\cdot)$ е прстен, треба да ги докажеме дистрибутивните закони. Имаме:

$$(f_1 (f_2 + f_3))(x) = f_1((f_2 + f_3)(x)) = f_1(f_2(x) + f_3(x)) =$$
$$= f_1(f_2(x)) + f_1(f_3(x)) = f_1 f_2(x) + f_1 f_3(x) = (f_1 f_2 + f_1 f_3)(x),$$

т.е. $f_1(f_2 + f_3) = f_1 f_2 + f_1 f_3$.

Слично се докажува и другиот дистрибутивен закон.

7.23. Ако $G(+)$ е групата определена со шемата

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

да се определи и множеството $\mathrm{End}G$, а потоа и шемите на операциите од прстенот $\mathrm{End}G$.

Решение. За да биде φ ендоморфизам, треба да е $\varphi(0) = 0$. Од шемата на операцијата гледаме дека за кои било ненулти и меѓусебно различни елементи, $x, y \in G$ имаме $x + y = z$, каде што z е ненулти елемент, различен и од x, и од y. Според тоа, ако φ е биекција, таква што $\varphi(0) = 0$, ќе имаме:

$\varphi(x + y) = \varphi(z) = \varphi(x) + \varphi(y)$.

Значи, секоја таква биекција е автоморфизам, а такви постојат шест:

$$1,\quad \rho_1=\begin{pmatrix}0 & a & b & c\\ 0 & b & c & a\end{pmatrix},\quad \rho_2=\begin{pmatrix}0 & a & b & c\\ 0 & c & a & b\end{pmatrix},$$

$$\sigma_1=\begin{pmatrix}0 & a & b & c\\ 0 & a & c & b\end{pmatrix},\quad \sigma_2=\begin{pmatrix}0 & a & b & c\\ 0 & c & b & a\end{pmatrix},\quad \sigma_3=\begin{pmatrix}0 & a & b & c\\ 0 & b & a & c\end{pmatrix}.$$

Да забележиме дека, за секој φ од овие ендоморфизми, $\mathrm{Ker}\varphi=\{0\}$. За да најдеме други ендоморфизми, ако такви постојат, ќе го разгледуваме јадрото на секој таков ендоморфизам, при што ќе го користиме равенството

$\varphi(z)=\varphi(x)+\varphi(y)$

ако x,y,z се меѓусебно различни (ненулти) елементи.

Ако $\mathrm{Ker}\varphi=\{0,a\}$ можни се следниве случаи:

$b\to a,\ b\to b,\ b\to c$; но, тогаш:

$c\to a,\ c\to b,\ c\to c$ соодветно. Така ги добиваме ендоморфизмите:

$$\alpha_1=\begin{pmatrix}0 & a & b & c\\ 0 & 0 & a & a\end{pmatrix},\quad \alpha_2=\begin{pmatrix}0 & a & b & c\\ 0 & 0 & b & b\end{pmatrix},\quad \alpha_3=\begin{pmatrix}0 & a & b & c\\ 0 & 0 & c & c\end{pmatrix},$$

Ако пак $\mathrm{Ker}\varphi=\{0,b\}$ или $\mathrm{Ker}\varphi=\{0,c\}$, како и погоре, ги добиваме ендоморфизмите:

$$\beta_1=\begin{pmatrix}0 & a & b & c\\ 0 & a & 0 & a\end{pmatrix},\quad \beta_2=\begin{pmatrix}0 & a & b & c\\ 0 & b & 0 & b\end{pmatrix},\quad \beta_3=\begin{pmatrix}0 & a & b & c\\ 0 & c & 0 & c\end{pmatrix},$$

$$\gamma_1=\begin{pmatrix}0 & a & b & c\\ 0 & a & a & 0\end{pmatrix},\quad \gamma_2=\begin{pmatrix}0 & a & b & c\\ 0 & b & b & 0\end{pmatrix},\quad \gamma_3=\begin{pmatrix}0 & a & b & c\\ 0 & c & c & 0\end{pmatrix},$$

Ако $\{0,x,y\}\subseteq\mathrm{Ker}\varphi$, тогаш

$\varphi(z)=\varphi(x+y)=\varphi(x)+\varphi(y)=0$, што значи и третиот ненулти елемент z е во јадрото на φ, т.е. $\mathrm{Ker}\varphi=G$, па пресликувањето ω, дефинирано со $\omega(x)=0,\ \forall x\in G$, е ендоморфизам.

Од сето ова следува дека $|\mathrm{End}G|=16$.

Составувањето на шемите на операциите "+" и "·" во End G се остава на читателот.

7.24. Да се покаже дека прстенот End$\mathbb{Z}$ од адитивната група $\mathbb{Z}(+)$ е изоморфен со прстенот $\mathbb{Z}(+,\cdot)$

Решение. Според 6.19., секој ендоморфизам во $\mathbb{Z}(+)$ е од облик f_a, каде што f_i е определено со

$(\forall x\in\mathbb{Z})\ f_a(x) = ax.$

Значи, End$\mathbb{Z} = \{f_a \mid a\in\mathbb{Z}\}$. Бидејќи

$f_a f_b = f_{ab},\quad f_a + f_b = f_{a+b},$

пресликувањето $\varphi : \text{End}\,\mathbb{Z} \to \mathbb{Z}$ дефинирано со

$\varphi(f_a) = a,$ е биекција и притоа имаме :

$\varphi(f_a f_b) = \varphi(f_{ab}) = ab = \varphi(f_a)\varphi(f_b),$

$\varphi(f_a + f_b) = \varphi(f_{a+b}) = a + b = \varphi(f_a) + \varphi(f_b)$. Значи φ е изоморфизам.

7.25. Да се покаже дека множеството од ендоморфизми на еден прстен е пак прстен, каде што операциите се определени, како во задачата 7.22.

7.26. Нека R е прстен и нека во $\mathcal{J}_R$ се определени операции " +" и "$\cdot$" како во 7.22. Да се провери дали добиената алгебра $\mathcal{J}_R(+,\cdot)$ е прстен.

Решение. Алгебрата $\mathcal{J}_R(+,\cdot)$, во општ случај, не е прстен зашто левиот дистрибутивен закон не мора да важи. Имено, ако $f\in\mathcal{J}_R$ не е ендоморфизам на R, тогаш

$$[f(g + h)](x) = f(g(x) + h(x)) \neq f(g(x)) + f(h(x)),$$

т.е. $f(g + h) \neq fg + fh.$

7.27. Нека P е прстен, а S произволно непразно множество, и нека во $R = P^S = \{f \mid f : S \to P\}$ се дефинирани операции "+" и "$\cdot$" со:

$f_1 + f_2 = g \iff (\forall s\in S)\ f_1(s) + f_2(s) = g(s),$

$f_1 f_2 = h \iff (\forall s\in S)\ f_1(s)\cdot f_2(s) = h(s).$

Да се покаже дека $R(+,\cdot)$ е прстен со делители на нулата.

7.28. Нека R е прстен и нека во $S = \mathbb{Z}\times R$ се определени операции "+" и "$\cdot$" со:

$(m, x) + (n, y) = (m + n, x + y)$

$(m, x)(n, y) = (mn, my + nx + xy)$

Да се покаже дека:

а) $S(+,\cdot)$ е прстен со единица и дека тој прстен е комутативен, односно асоцијативен ако и само ако истото својство го има и прстенот R;

б) Пресликувањето $f : R \to S$, определено со $f(x) = (0, x)$, е мономорфизам.

Решение. а) Јасно е дека $S(+)$ е комутативна група. Понатаму имаме:

$$(m, x)[(n, y) + (p, z)] = (m, x)(n + p, y + z) =$$
$$= (m(n + p), m(y + z) + (n + p)x + x(y + z)) =$$
$$= (mn + mp, my + mz + nx + px + xy + xz) =$$
$$= (mn + mp, (my + nx + xy) + (mz + px + xz)) =$$
$$= (mn, my + nx + xy) + (mp, mz + px + xz) = (m, x)(n, y) + (m, x)(p, z),$$

а слично и другиот дистрибутивен закон.

За елементот (1,0) имаме $(1,0)(n, y) = (n, y)$ и $(n, y)(1,0) = (n, y)$, па $S(+,\cdot)$ е прстен со единица.

Да покажеме сега дека $S(+,\cdot)$ е комутативен, односно асоцијативен ако и само ако истото својство го има и R. Ако R е комутативен, односно асоцијативен, тогаш имаме:

$(m, x)(n, y) = (mn, my + nx + xy) = (nm, nx + my + yx) = (n,y)(m, x)$, и

$$(m, x)[(n, y)(p, z)] = (m, x)(np, nz + py + yz) =$$
$$= (m(np), m(nz + py + yz) + (np)x + x(nz + py + yz)) =$$
$$= ((mn)p, mnz + mpy + myz + npx + nxz + pxy + x(yz)) =$$
$$= ((mn)p, mnz + p(my + nx + xy) + (my + nx + xy)z) =$$
$$= (mn, my + nx + xy)(p,z) = [(m, x)(n, y)](p, z),$$

т.е. и $S(+,\cdot)$ е комутативен, односно асоцијативен.

Обратно, нека $S(+,\cdot)$ е комутативен. Тогаш имаме:

$(m, x)(n, y) = (n, y)(m, x)$,

$(mn, my + nx + xy) = (nm, nx + my + yx)$,

$my + nx + xy = nx + my + yx$,

т.е. $xy = yx$. Значи, и R е комутативен, а слично се покажува дека ако S е асоцијативен, тогаш и R е асоцијативен.

б) Јасно е дека пресликувањето $f : R \to S$, дефинирано со $f(x) = (0, x)$, е инјекција, а бидејќи

$f(x + y) = (0, x + y) = (0, x) + (0, y) = f(x) + f(y)$,

$f(xy) = (0, xy) = (0, x)(0, y) = f(x)f(y)$,

следува дека f е мономорфизам.

7.29. Да се покаже дека секој прстен R е потпрстен од некој прстен со единица.

Решение. Прстенот S од претходната задача е прстен со единица и пресликувањето $f : R \to S$, определено со $f(x) = (0, x)$ е мономорфизам. Значи, множеството $S_1 = \{(0, x) \mid x \in R\}$ е потпрстен од S, изоморфен со R. Според тоа, ставајќи $x = (0, x)$, можеме да сметаме дека R е потпрстен од прстенот S.

7.30. Во множеството $R = \mathbb{Q}^4$ се дефинирани операции "+" и "·" со:
$(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$,
$(a, b, c, d)\,(a', b', c', d') = (aa' + bc', ab' + bd', ca' + dc', cb' + dd')$
Да се покаже (за а) – ѓ)) дека:
а) $R(+,\cdot)$ е некомутативен прстен со единица;
б) елементот (a, b, c, d) е инверзибилен ако и само ако $ad - bc \neq 0$;
в) подмножеството $P = \{(a, b, -b, a) \mid a, b \in \mathbb{Z}\}$ е комутативен потпрстен од R, изоморфен со прстенот од гаусовите цели броеви, $G = \{a + ib \mid a, b \in \mathbb{Z}\}$;
г) подмножеството $S = \{(a, b - b, a) \mid a, b \in \mathbb{Q}\}$ е поттело од R. Дали е потполе?
д) подмножествата
$T_1 = \{(a, 0, c, d) \mid a, c, d \in \mathbb{Q}\}$ и $T_2 = \{(a, 0, 0, d) \mid a, d \in \mathbb{Q}\}$ се потпрстени од R.
ѓ) пресликувањето $f: T_1 \to T_2$, дефинирано со
$f((a, 0, c, d)) = (a, 0, 0, d)$ е хоморфизам
е) Да се најде хомоморфизам g од T_1 во S, а потоа и $\mathrm{Ker}g$.
ж) Дали пресликувањето $h : P \to \mathbb{Z}$, дефинирано со:
$h((a, b, -b, a)) = a$ е хомоморфизам ?

7.31. Во множеството $P = \{(a, b, -b, a) \mid a, b \in \mathbb{R}\}$ се дефинирани операции "+" и "·" како во 7.30. Да се покаже дека P е поле изоморфно со полето на комплексните броеви.

7.32. Во множеството $R = \mathbb{C}^4$ се дефинирани операции "+" и "·" како во 7.30. Да се покаже дека:
а) $R(+, \cdot)$ е некомутативен прстен со единица $(1, 0, 0, 1)$;
б) множеството $S = \{(z, w, -w, z) \mid z, w \in \mathbb{C}\}$ е потпрстен од R;
в) множеството $T = \{(z, w, -\overline{w}, \overline{z}) \mid z, w \in \mathbb{C}\}$ е поттело од R, но не и поле. Притоа,

$$(z, w, -\overline{w}, \overline{z})^{-1} = \left(\frac{\overline{z}}{\Delta}, -\frac{w}{\Delta}, \frac{\overline{w}}{\Delta}, \frac{z}{\Delta}\right) \quad \Delta = |z|^2 + |w|^2.$$

7.33. Нека f е епиморфизам од прстенот $\mathbb{Z}$ на целите броеви на ненултиот прстен R. Да се докаже дека f е изоморфизам или пак R е прстен изоморфен со прстенот $\mathbb{Z}_n$, за некој $n \in \mathbb{N}$, $n > 1$.

Решение. Да препоставиме дека f не е изоморфизам, т.е. f не е инјекција. Тогаш $\{0\} \subset \mathrm{Ker}f$, па $\mathrm{Ker}f$ е конгруенција во $\mathbb{Z}$, различна од еднаквоста. Бидејќи секоја конгруенција во $\mathbb{Z}$ е $\equiv (\mathrm{mod}\ n)$, следува дека

постои $n\in\mathbb{N}$, $n > 1$, такашто $\mathrm{Ker}f$ е $\equiv (\mathrm{mod}\ n)$. Фактор-прстенот $\mathbb{Z}/_{\mathrm{Ker}f}$ е прстенот $\mathbb{Z}_n$ и притоа епиморфизмот f индуцира епиморфизам $f^*: \mathbb{Z}_n \to R$, којшто е изоморфизам.

Значи, ако f не е изоморфизам, тогаш R е изоморфен со $\mathbb{Z}_n$ за некое $n\in\mathbb{N}$.

7.34. Да се покаже дека прстенот $\mathbb{Z}_{12}$ е изоморфен со прстенот $\mathbb{Z}_3\times\mathbb{Z}_4$. Поопшто, ако $n = n_1 n_2 \ldots n_k$, кадешто $(n_i, n_j) = 1$, за $i \neq j$, тогаш $\mathbb{Z}_n$ е изоморфен со директниот производ $\prod_1^k \mathbb{Z}_{n_i}$

Решение. Дека прстенот $\mathbb{Z}_{12}$ е изоморфен со прстенот $\mathbb{Z}_3\times\mathbb{Z}_4$ се гледа од тоа што пресликувањето $f: \mathbb{Z}_{12} \to \mathbb{Z}_3\times\mathbb{Z}_4$ дефинирано со:

$0 \to (0, 0)$, $1 \to (1, 1)$, $2 \to (2, 2)$, $3 \to (0, 3)$, $4 \to (1, 0)$, $5 \to (2, 1)$,

$6 \to (0, 2)$, $7 \to (1, 3)$, $8 \to (2, 0)$, $9 \to (0, 1)$, $10 \to (1, 2)$, $11 \to (2, 3)$,

е изоморфизам.

Нека сега n е претставен во обликот $n = n_1 n_2 \ldots n_k$, каде што $(n_i, n_j) = 1$ за $i \neq j$. Пресликувањето $f: \mathbb{Z}_n \to \prod_1^k \mathbb{Z}_{n_i}$ да го дефинираме со:

$f(0) = (0, 0,\ldots, 0)$, $f(1) = (1, 1,\ldots,1)$, $f(m) = mf(1)$,

каде што со $mf(1)$ означуваме:

$mf(1) = (m_1, m_2,\ldots, m_k) \Leftrightarrow m \equiv m_i(\mathrm{mod}n_i)$, $m_i < n_i$.

Бидејќи $r_i + s_i \equiv (r + s)_i\ (\mathrm{mod}n_i)$ и $r_i s_i = (rs)_i\ (\mathrm{mod}n_i)$ имаме:

$f(r + s) = (r + s)f(1) = rf(1) + sf(1) = f(r) + f(s)$

$f(rs) = (rs)f(1) = rsf(1)f(1) = (rf(1))\,(sf(1)) = f(r)f(s)$,

т.е. f е хомоморфизам. За да покажеме дека f е изоморфизам, доволно е да покажеме дека f е инјекција, зашто $\mathbb{Z}_n$ и $\prod_1^k \mathbb{Z}_{n_i}$ имаат ист број елементи. Нека $f(r) = f(s)$. Тоа значи дека

$r \equiv r_i\ (\mathrm{mod}n_i)$, $s \equiv r_i\ (\mathrm{mod}n_i)$,

од каде што $r \equiv s_i\ (\mathrm{mod}n_i)$ за $i = 1, 2,\ldots k$, а пак од овие конгруенции и следува

$r \equiv s\ (\mathrm{mod}\ [n_1, n_2,\ldots, n_k])$.

Бидејќи $(n_i, n_j) = 1$ за $i \neq j$, имаме $[n_1, n_2,\ldots, n_k] = n_1 n_2 \ldots n_k = n$, т.е.

$r \equiv s(\mathrm{mod}n)$, а поради $r, s < n$, следува $r = s$, што значи дека f е инјекција.

7.35. Да се најде групата автоморфизми од полето:

а) $\mathbb{Q}$; б) $\mathbb{Q}(\sqrt{2})$; в) $(\mathbb{Q}\sqrt[3]{2})$.

Одговор. а) $1_{\mathbb{Q}}$. б) $1_{\mathbb{Q}}$; и $\varphi : a + b\sqrt{2} \to a - b\sqrt{2}$. в) $1_{\mathbb{Q}}$.

7.36. Да се најдат сите епиморфизми од $\mathbb{Z}(+,\cdot)$ во $\mathbb{Z}_m(+,\cdot)$, $m \neq 1$.

7.37. Ако R и R' се прстени, а $f : R \to R'$ хомоморфизам, тогаш постои конгруенција α во R, епиморфизам, $g : R \to R/_\alpha$ и мономорфизам $h : R/_\alpha \to R'$ такви што $f = hg$.

Упатство. Да се земе $r_1 \alpha\, r_2 \Leftrightarrow f(r_1) = f(r_2)$.

7.38. Ако R е прстен со единица, и ако $f : \mathbb{Z} \to R$ е дефинирано со: $f(m) = ma$, $a \in R$, дали f е хомоморфизам?

7.39. Нека R и S се асоцијативни прстени со единица и α кореспонденција од R во S што ги задоволува условите:

$$0\alpha 0, \qquad 1\alpha 1; \tag{1}$$

$$r_1 \alpha s_1,\ r_2 \alpha s_2 \Rightarrow (-r_1)\alpha(-r_2),\ (r_1 + r_2)\ \alpha\ (s_1 + s_2),\ (r_1 r_2)\ \alpha\ (s_1 s_2) \tag{2}$$

Ако B е потпрстен од S, да се покаже дека
$A = \{a \mid a \in R,, (\exists b \in B)\ a \alpha b\}$ е потпрстен од R.

7.40. Нека R, S и T се асоцијативни прстени со единици и кореспонденциите $\alpha \subseteq R \times S$, $\beta \subseteq S \times T$ ги задоволуваат условите (1) и (2) од 7.39. Да се покаже дека тие услови ги задоволува и кореспонденцијата $\beta\alpha \subseteq R \times T$.

7.41. Во прстенот R, α е рефлексивна релација што ги задоволува условите (1) и (2) од задача 7.39. Да се покаже дека α е конгруенција во R.

Решение. Доволно е да покажеме дека релацијата α е симетрична и транзитивна.

Нека $a\ \alpha\ b$. Бидејќи $a\ \alpha\ a$ и $b\ \alpha\ b$, имаме
$b = (a - a + b)\ \alpha\ (a - b + b) = a$, што значи дека α е симетрична.
Нека $a\ \alpha\ b$ и $b\ \alpha\ c$. Бидејќи $b\ \alpha\ b$ имаме
$a = (a - b + b)\ \alpha\ (b - b + c) = c$, што значи дека α е транзитивна.

7.42. Нека P е поле и нека секој елемент $(x, y) \in P \times P$ го сметаме за точка. Ако $a, b \in P$, тогаш множествата точки

$$[a, b] = \{(x, ax + b) \mid x \in P\},\ [b] = \{(b, y) \mid y \in P\}$$

ги сметаме за прави. Да се покаже дека така дефинираните множества од точки и прави формираат афина рамнина.

Решение. Нека (a, b) и (c, d) се две различни точки. Ако $a \neq c$, тогаш правата $[(d - b)(c - a)^{-1}, b - a(d - b)(c - a)^{-1}]$ е единствена што минува низ точките (a, b) и (c, d).

Нека $[a, b]$ е произволна права, а (c, d) произволна точка, така што правата $[a, b]$ не минува низ (c, d), т.е. $ac + b \neq d$. Правата $[a, d - ac]$ е единствена што минува низ точката (c, d) и е паралелна права со $[a, b]$.

На крајот, точките (0, 0), (1, 0) и (0, 1) не лежат на иста права.

Значи, множествата точки и прави, дефинирани во условот на задачата, формираат афина рамнина.

7.43. Нека а) $P = \mathbb{Z}$, б) $P = \mathbb{Z}_4$ и нека се дефинирани множества прави како во 7.42. Дали и во овие случаи имаме афина рамнина?

Решение. Не. За $P = \mathbb{Z}$ и $P = \mathbb{Z}_4$, на пример, точките (1, 1) и (3, 2) се различни, но низ нив не минува права.

§ 8. БУЛОВИ АЛГЕБРИ

8.1. Нека M е дадено множество, а $\mathbb{B}$ е непразно подмножество од $\mathbb{P}(M)$ што ги задоволува условите:

(i) $A, B \in \mathbb{B} \Rightarrow A \cup B \in \mathbb{B}$

(ii) $A \in \mathbb{B} \Rightarrow M \setminus A = A' \in \mathbb{B}$.

Да се покаже дека $\mathbb{B}(\cup, \cap)$ е булова алгебра и дека условот (i) може да се замени со условот

(i') $A, B \in \mathbb{B} \Rightarrow A \cap B \in \mathbb{B}$.

Решение. Нека $A \in \mathbb{B}$; според (ii) следува дека $A' \in \mathbb{B}$; според (i) следува дека $M = A \cup A' \in \mathbb{B}$, а потоа и $\varnothing \in \mathbb{B}$. За да покажеме дека $\mathbb{B}(\cup, \cap)$ е булова алгебра, доволно е да покажеме уште дека $A \cap B \in \mathbb{B}$ кога $A, B \in \mathbb{B}$. Затоа, нека $A, B \in \mathbb{B}$. Бидејќи

$$A \cap B = M \setminus (A \cap B)' = M \setminus (A' \cup B'),$$

од (i) и (ii) следува дека и $A \cap B \in \mathbb{B}$. Значи $\mathbb{B}$ е булова алгебра.

Дека условот (i) може да се замени со (i'), следува од тоа што $A \cup B = M \setminus (A \cup B)' = M \setminus (A' \cap B')$.

8.2. Нека M е множество со барем три елементи, а A нека е подмножество од M со барем два елемнта. Ако

$$\mathbb{B} = \{X \mid X \subseteq M,\ (X \cap A = \varnothing \text{ или } X \cap A = A)\},$$

да се покаже дека $\mathbb{B}(\cup, \cap)$ е булова алгебра.

Решение. Според 8.1, за да покажеме дека $\mathbb{B}(\cup, \cap)$ е булова алгебра, доволно е да покажеме дека $B \cup C, M \setminus B \in \mathbb{B}$, кога $B, C \in \mathbb{B}$. Имаме

$$(M \setminus B) \cap A = B' \cap A,$$

па ако $B \cap A = \varnothing$, тогаш $B' \cap A = A$, а ако $B \cap A = A$, тогаш $B' \cap A = \varnothing$.

Значи, $B \in \mathbb{B} \Rightarrow M \setminus B \in \mathbb{B}$. Ако $B, C \in \mathbb{B}$, тогаш

$$(B \cup C) \cap A = (B \cap A) \cup (C \cap A) = \begin{cases} \varnothing & \text{за} \quad B \cap A = C \cap A = \varnothing \\ A & \text{инаку} \end{cases}$$

т.е. $B \cup C \in \mathbb{B}$.

Да забележиме дека, ако A е едноелементно множество или празно, тогаш $\mathbb{B} = \mathbb{P}(M)$.

8.3. Нека $\mathbb{B}$ е множеството од сите конечни подмножества од некое бесконечно множество M. Дали $\mathbb{B}(\cup, \cap)$ е булова алгебра ?

Одговор. Не.

8.4. За дадено множество M, да го означиме со K_M множеството од сите карактеристични функции на сите подмножества од M. Ако во K_M дефинираме подредување со:

$\chi_A \leq \chi_B \Leftrightarrow A \subseteq B$,

тогаш K_M е булова алгебра изоморфна со буловата алгебра $\mathbb{P}(M)$.

Притоа: $\chi_A(x) = \begin{cases} 1 & \text{за } x \in A, \\ 0 & \text{за } x \notin A. \end{cases}$

8.5. Да се покаже дека буловите алгебри $\mathbb{B}_1 = \mathbb{P}(M_1)$ и $\mathbb{B}_2 = \mathbb{P}(M_2)$ се изоморфни ако и само ако $\mathrm{k}M_1 = \mathrm{k}M_2$.

Решение. Ако $\mathrm{k}M_1 = \mathrm{k}M_2$, тогаш постои биекција $f : M_1 \to M_2$, којашто индуцира пресликување $g : \mathbb{B}_1 \to \mathbb{B}_2$, определено со

$(\forall A \in \mathbb{B}_1)\ g(A) = f(A)$.

Лесно се проверува дека g е изоморфизам меѓу $\mathbb{B}_1$ и $\mathbb{B}_2$ Обратно, нека $\mathbb{B}_1$ и $\mathbb{B}_2$ се изоморфни, при изоморфизмот g.

Да дефинираме пресликување $f : M_1 \to M_2$ со:

$(\forall x \in M_1)\ f(x) = g(\{x\})$.

Јасно е дека f е биекција, т.е. $\mathrm{k}M_1 = \mathrm{k}M_2$.

8.6. Ако во множеството $B = \{0, a, b, 1\}$ дефинираме две операции "$\cup$" и "$\cap$" со шемите

$\cup$	0	a	b	1
0	0	a	b	1
a	a	a	1	1
b	b	1	b	1
1	1	1	1	1

$\cap$	0	a	b	1
0	0	0	0	0
a	0	a	0	a
b	0	0	b	b
1	0	a	b	1

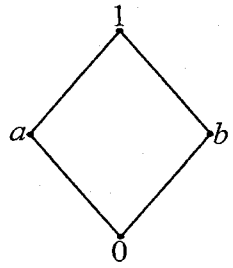
тогаш $B(\cup, \cap)$ е булова алгебра.

Решение. Дијаграмот на мрежата $B(\cup, \cap)$ е даден на цртеж 1 од каде што се гледа дека 0 е најмал елемент, 1 е најголем елемент и мрежата е комплементарна. Значи, за да покажеме дека $B(\cup, \cap)$ е булова алгебра, доволно е да покажеме дека е дистрибутивна.

Да го покажеме, на пример, дистрибутивниот закон

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z), \qquad (1)$$

а другиот се докажува слично.



Црт.1

Ако $x = 0$ или $x = 1$, тогаш точноста на (1) е јасна. Нека $x = a$; тогаш:

$$a \cap (0 \cup z) = a \cap z,$$
$$(a \cap 0) \cup (a \cap z) = 0 \cup (a \cap z) = a \cap z, \qquad (2)$$
$$a \cap (1 \cup z) = a,$$
$$(a \cap 1) \cup (a \cap z) = a \cup (a \cap z) = a, \qquad (3)$$
$$a \cap (a \cup b) = a, (a \cap a) \cup (a \cap b) = a \cup (a \cap b) = a. \qquad (4)$$

Ако пак $x = b$, пишувајќи b наместо a, и a наместо b во (2), (3) и (4) се добиваат соодветни равенства.

Значи, точно е равенството (1).

8.7. Да се покаже дека буловата алгебра $B(\cup, \cap)$ од 8.6 е изоморфна со алгебрата $\mathbb{P}(P)(\cup, \cap)$ каде што $P = \{0,1\}$.

Решение. Пресликувањето $f: B \to \mathbb{P}(P)$ дефинирано со:

$f(0) = \varnothing, f(a) = \{0\}, f(b) = \{1\}, f(1) = P$ е изоморфизам.

8.8. Нека S е подмножество од $\mathbb{N}$, а

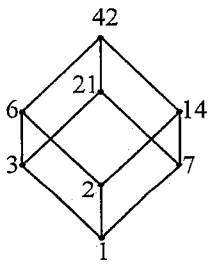
$a \cap b = (a, b)$, $a \cup b = [a, b]$,

каде што (a, b) е НЗД, а $[a, b]$ е НЗС на a, b. Да се покаже дека:

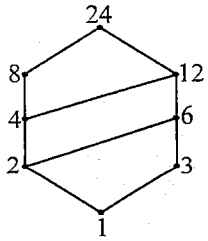
а) ако $S = \{1, 2, 3, 6, 7, 14, 21, 42\}$, тогаш $S(\cup, \cap)$ е булова алгебра;

б) ако $S = \{1, 2, 3, 4, 6, 8, 12, 24\}$, тогаш $S(\cup, \cap)$ не е булова алгебра.

Решение. Од својствата на НЗС и НЗД следува дека мрежата $S(\cup, \cap)$ е дистрибутивна, а од дијаграмите на црт.2. и црт.3 се гледа



Црт.2



Црт.3

дека мрежата $S(\cup, \cap)$ под а) е комплементарна, при што $2' = 21$, $3' = 14$, $6' = 7$, а под б) не е комплементарна, зашто на пример, $2'$ не постои. Значи мрежата $S(\cup, \cap)$ под а) е булова алгебра, а под б) не е.

8.9. Дали една булова алгебра, може да биде потполно подредена?

Решение. Нека B е булова алгебра, при што B е потполно подредено множество. Ако a е произволен елемент од B, тогаш постои a', така што

$$a \cap a' = 0 \quad \text{и} \quad a \cup a' = 1. \tag{1}$$

Бидејќи B е потполно подредено множество, можеме да претпоставиме дека $a \leq a'$. Но, тогаш

$$a \cap a' = a, \text{ и } a \cup a' = a' \tag{2}$$

Од (1) и (2) следува дека $a = 0$, $a' = 1$, т.е. B се состои само од два елемента.

Значи, една булова алгебра B е потполно подредена ако и само ако $B = \{0, 1\}$.

8.10. Дали постои булова алгебра $B(\cup, \cap)$, ако B содржи три елементи?

Решение. Нека $B = \{0, a, 1\}$. За да биде 0 најмал елемент, а 1 најголем елемент, подредувањето во B може да се дефинира со $0 \leq a \leq 1$, кое е потполно, па според претходната задача, B не е булова алгебра.

Во наредните задачи 8.11. – 8.15. се работи за булови алгебри.

8.11. Ако $a \cup x = b \cup x$, $a \cup x' = b \cup x'$, тогаш $a = b$.

Решение. Од $a \cup x = b \cup x$ и $a \cup x' = b \cup x'$ следува дека

$$(a \cup x) \cap (a \cup x') = (b \cup x) \cap (b \cup x').$$

Од друга страна имаме:

$$(a \cup x) \cap (a \cup x') = a \cup (x \cap x') = a \cup 0 = a,$$

а слично и $(b \cup x) \cap (b \cup x') = b$.

8.12. Ако $a \cap b = a \cap c$, $a \cup b = a \cup c$, тогаш $b = c$.

Решение. Имаме:

$$b = b \cap (b \cup a) = b \cap (c \cup a) = (b \cap c) \cup (b \cap a) = (b \cap c) \cup (c \cap a) =$$
$$= c \cap (b \cup a) = c \cap (c \cup a) = c.$$

8.13. Да се покаже дека :

а) $(x \cap y) \cup [(x \cup y') \cap y]' = 1$.

б) $\{[(x' \cap y')' \cup z] \cap (x \cup z)\}' = x' \cap z'$

в) $[x \cup (x' \cup y)'] \cap [x \cup (y' \cap z')']' = x$.

Решение. а) $(x \cap y) \cup [(x \cup y') \cap y]' = (x \cap y) \cup [(x \cup y')' \cup y']' =$

$= (x \cap y) \cup [(x' \cap y) \cup y'] = (x \cap y) \cup [(x' \cup y') \cap (y \cup y')] =$

$= (x \cap y) \cup [(x' \cup y') \cap 1] = (x \cap y) \cup (x' \cup y') =$

$= (x \cap y) \cup (x \cap y)' = 1$

8.14. Да се упростат изразите:

а) $(a \cup b) \cap a' \cap b'$;

б) $(a \cap b \cap c) \cup a' \cup b' \cup c'$;

в) $[a \cup (a' \cap b)] \cap [b \cup (b \cap c)]$

г) $[(a' \cap b')' \cup c] \cap (a \cup b')'$;

д) $(a \cup b') \cap (a' \cup b) \cap (a' \cup b')$;

ѓ) $[(a \cup b) \cap (c \cup b')] \cup [b \cap (a' \cup c')]$.

Одговор. а) 0; б) 1; в) b; г) $a' \cap b$; д) $a' \cap b'$; ѓ) $a \cup b$

8.15. Да се реши системот равенки :

а) $x = y \cap z,\ y = x \cup z',\ z = x' \cap y'$;

б) $x = y \cap z,\ y = x \cup z,\ z = x' \cap y'$.

Решение. а) Имаме:

$z = x' \cap y' = (y \cap z)' \cap y' = (y' \cup z') \cap y' = y'$, а потоа и

$x = y \cap z = y \cap y' = 0$.

Од ова следува дека секоја тројка $(0,\ y,\ y')$ е решение на системот.

б) Како и во а) добиваме $z = y'$ и $x = 0$.

Од $y = x \cup z$ следува $y = y'$ што не е можно, па значи системот нема решение.

8.16. Нека $B = \{0, 1\} = \mathbb{Z}_2$ е буловиот прстен со два елемента. Да се провери дали прстенот M_n од сите матрици со ред n над B, е булов.

Решение. Не е булов. На пример, ако $A = [a_{ij}]$, $a_{12} = 1$, $a_{ij} = 0$ за $i \neq 1, j \neq 2$, тогаш $A^2 = 0 \neq A$.

8.17. Да се покаже дека:

а) хомоморфни слики; б) фактор–прстени; в) потпрстени;

г) директни производи од булови прстени се булови прстени.

Решение. а) Нека B_1 и B_2 се прстени, при што B_1 е булов, а $f: B_1 \to B_2$ е хомоморфизам. Ништо не се губи од општоста ако се претпостави дека f е епиморфизам. Јасно е дека B_2, како хомоморфна слика од B_1, е асоцијативен. Ако y е произволен елемент од B_2, тогаш постои $x \in B_1$, така што $y = f(x)$ и притоа имаме:

$y^2 = f(x)f(x) = f(xx) = f(x) = y$, т.е. B_2 е булов прстен.

б) Нека B е булов прстен, а α конгруенција во B. Тогаш $B/_\alpha$ е исто така асоцијативен прстен, и притоа имаме:

$(a^\alpha)^2 = (a^2)^\alpha = a^\alpha$, т.е. прстенот $B/_\alpha$ е булов.

8.18. Нека $R(+,\cdot)$ е булов прстен и нека во R дефинираме нови операции "$\oplus$" и "$\odot$" со

$x \oplus y = 1 + x + y, \quad x \odot y = x + y + xy.$

Да се покаже дека $R(\oplus,\odot)$ е исто така булов прстен, изоморфен со $R(+,\cdot)$.

Решение. Комутативноста и асоцијативноста на операцијата $\oplus$ се проверува непосредно. Бидејќи $x \oplus 1 = 1 + x + 1$, $x \oplus x = 1 + x + x = 1$, следува дека $R(\oplus)$ е комутативна група со нула 1. Понатаму имаме:

$x \odot (y \oplus z) = x + (1 + y + z) + x(1 + y + z) = 1 + y + z + xy + xz,$

$(x \odot y) \oplus (x \odot z) = 1 + (x + y + xy) + (x + z + xz) = 1 + y + z + xy + xz,$

а бидејќи операцијата $\odot$ е комутативна, следува дека $R(\oplus,\odot)$ е прстен. Бидејќи

$0 \odot x = 0 + x + 0 \cdot x = x,$

следува дека 0 е единица во прстенот $R(\oplus, \odot)$, а дека тој прстен е и асоцијативен се проверува непосредно. На крајот имаме

$x \odot x = x + x + xx = x,$

т.е. прстенот $R(\oplus, \odot)$ е булов.

Пресликувањето $f: R(\oplus, \odot) \to R(+,\cdot)$, дефинирано со:

$(\forall x \in R)\ f(x) = x + 1$ е биекција, а покрај тоа, имаме

$f(x \oplus y) = f(x + y + 1) = x + y + 1 + 1 = f(x) + f(y),$

$f(x \odot y) = f(x + y + xy) = x + y + xy + 1 = (x + 1)(y + 1) = f(x) \cdot f(y)$

што значи дека f е изоморфизам на разгледуваните прстени.

8.19. Нека $R(+,\cdot)$ е асоцијативен прстен со единица 1, а $R(\circ)$ нека е групоид со единица e, при што се исполнети условите:

$(x + y) \circ z = x \circ z + y \circ z,$

$x \circ (yz) = (x \circ y)(x \circ z).$

Да се покаже дека R е булов прстен, при што $e = 1$ и $x \circ y = xy$.

Решение. Доказот ќе го спроведеме во неколку етапи.

Прво имаме:

$(1 \circ 1)\,(1 \circ y) + (x \circ 1)\,(x \circ y) = 1 \circ (1 \cdot y) + x \circ (1 \cdot y) =$

$= (1 + x) \circ (1 \cdot y) = ((1 + x) \circ 1))\,((1 + x) \circ y) =$

$= ((1 \circ 1) + (x \circ 1))\,((1 \circ y) + (x \circ y)) =$

$= (1 \circ 1)\,(1 \circ y) + (x \circ 1)\,(1 \circ y) + (1 \circ 1)\,(x \circ y) + (x \circ 1)\,(x \circ y),$

од каде што добиваме

$$(1 \circ 1)\,(x \circ y) + (x \circ 1)\,(1 \circ y) = 0. \qquad (1)$$

Понатаму имаме:

$1 \circ 1 = 1 \cdot (1 \circ 1) = (1 \circ e)\,(1 \circ 1) = 1 \circ (e \cdot 1) = 1 \circ e = 1.$

Ставајќи $x = y = 1$ во (1) добиваме $1 + 1 = 0$, т.е. прстенот R има карактеристика 2.

Од (1) имаме:

$0 = (1 \circ 1)\,(e \circ e) + (e \circ 1)\,(1 \circ e) = 1 \cdot e + 1 \cdot 1 = e + 1,$

а бидејќи $e + e = 0$, добиваме $e = 1$.

Понатаму имаме:

$x^2 = xx = (x \circ 1)\,(x \circ 1) = x \circ (1 \cdot 1) = x \circ 1 = x,$

т.е. R е булов прстен. На крајот имаме:

$0 = (1 \circ 1)\,(x \circ y) + (x \circ 1)\,(1 \circ y) = 1(x \circ y) + xy = x \circ y + xy,$

од каде што следува $x \circ y = xy$.

8.20. Нека $B(\cup, \cap)$ е булова алгебра, а $B(+,\cdot)$ соодветниот булов прстен. Да се претстави изразот $a \cup (b \cap c) \cup d$ со помош на операциите во прстенот, а изразот $a + b(b - c(a + b))$ со помош на операциите во алгебрата.

Решение. $a \cup (b \cap c) \cup d = a \cup (bc) \cup d = (a + bc + abc) \cup d =$

$= a + bc + abc + d + ad + bcd + abcd =$

$= a + bc(1 + a) + d(1 + a) + bcd(1 + a) =$

$= a + (1 + a)[bc + (1 + bc)d];$

$a + b(b - c(a + b)) = a + b(b + ca + cb) = a + b + abc + bc =$

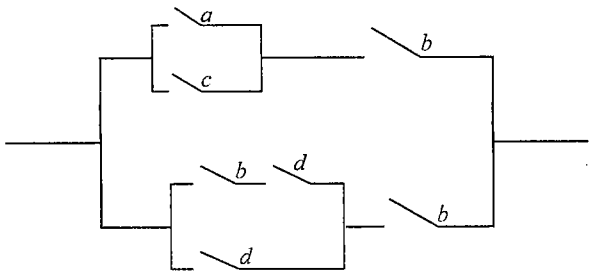
$= a + b + a'bc = a + b(a'c)' = a + [b \cap (a \cup c')] =$

$= \{a' \cap [(b \cap a) \cup (b \cap c')]\} \cup \{a \cap [b' \cup (a' \cap c)]\} =$

$= (a' \cap b \cap a) \cup (a' \cap b \cap c') \cup (a \cap b') \cup (a \cap a' \cap c) =$

$= (a' \cap b \cap c') \cup (a \cap b').$

8.21. Да се најде попроста контактна шема, еквивалентна со шемата



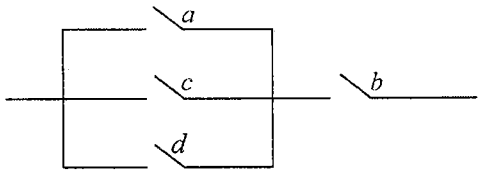
Решение. Имаме:

$((a \cup c) \cap b) \cup (((b \cap d) \cup d) \cap b) = ((a \cup c) \cap b) \cup (b \cap d) =$

$= (((a \cup c) \cap b) \cup b) \cap (((a \cup c) \cap b) \cup d) =$

$= b \cap ((a \cup c \cup d) \cap (b \cup d)) = (a \cup c \cup d) \cap b,$

па ја добиваме следната еквивалентна, попроста контакна шема.



8.22. Во еден одбор од три члена, на секој член му стои на располагање еден прекинувач. При гласањето, секој што вели "да" го вклучува својот прекинувач, а тој што вели "не", не го вклучува. Да се состави шема на електрично коло кое ќе има вредност 1, т.е. ќе биде вклучено, ако барем двајца од одборот го дадат својот глас за определен предлог.

Решение. Прекинувачите да ги означиме со a, b и c. Ако прекинувачот е вклучен, ќе велиме дека има вредност 1, ако не е вклучен дека има вредност 0. Колото ќе биде вклучено (т.е. предлогот ќе биде прифатен) ако барем два од прекинувачите се вклучени, т.е ако е исполнет еден (и само еден) од случаите:

$a = b = c = 1;\ \ a = b = 1,\ \ c = 0;\ \ a = c = 1, b = 0;\ \ b = c = 1,\ \ a = 0,$

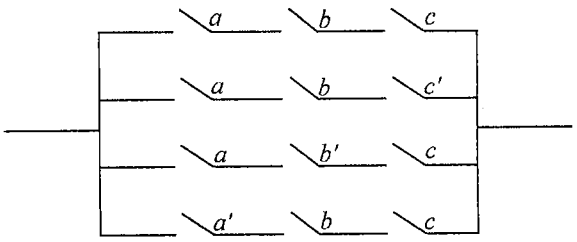
т.е. ако

$$a \cap b \cap c = 1;\ \ a \cap b \cap c' = 1;\ \ a \cap b' \cap c = 1; a' \cap b \cap c = 1. \qquad (1)$$

Според тоа, предлогот ќе биде прифатен ако и само ако

$(a \cap b \cap c) \cup (a \cap b \cap c') \cup (a \cap b' \cap c) \cup (a' \cap b \cap c) = 1.$

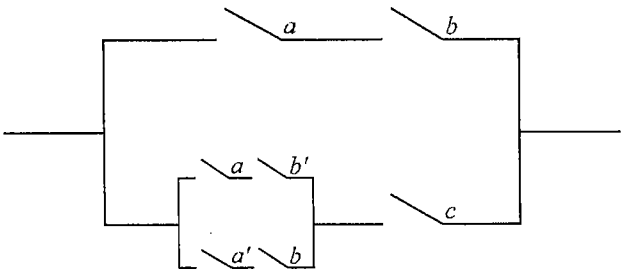
Така, ја добиваме следнава шема:



Бидејќи $(a \cap b \cap c) \cup (a \cap b \cap c') = (a \cap b) \cap (c \cup c') = a \cap b$, а
$(a \cap b' \cap c) \cup (a' \cap b \cap c) = ((a \cap b') \cup (a' \cap b)) \cap c$,
равенството (1) станува:

$$(a \cap b) \cup (((a \cap b') \cup (a' \cap b)) \cap c) = 1, \qquad (2)$$

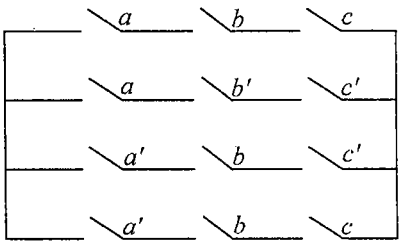
за кое соодветната шема е



која е еквивалентна со претходната.

8.23. Во една просторија има една светилка и три прекинувачи. Како да се реализира електричното коло за да се менува состојбата на светилката со промена на само еден од прекинувачите?

Решение. Шемата на колото е



8.24. Еден од учениците Андон, Борис, Цветан, Драган скршил прозорец во училницата. На прашањето кој го сторил тоа, секој од нив го дал следниов одговор:

A: " Цветан го стори тоа!";

B: "Јас не го направив тоа!";

C: "Тврдењето на Андон е лажно!";

D:" Андон го направи тоа!".

Да се најде виновникот ако се знае дека :

а) само еден од одговорите е точен.

б) само еден од одговорите не е точен.

Решение. а) Борис го скршил прозорецот. (Точен е одговорот на Цветан). До овој заклучок може да се дојде со обична дискусија, а и со помош на алгебрата на исказите на следниов начин: Имаме: $A : c$, $B : b'$, $C : c'$, $D : a$, па:

$$1 = (c \cap b'' \cap c'' \cap a') \cup (c' \cap b' \cap c \cap a') \cup (c' \cap b'' \cap c' \cap a') \cup (c' \cap b' \cap c'' \cap a) =$$
$$= (c \cap b \cap a') \cup 0 \cup (c' \cap b \cap a') \cup 0 = (c \cup c') \cap b \cap a' = 1 \cap b \cap a' = b \cap a'.$$

Од ова следува дека $b = 1$, $a = 0$, т.е. Борис го скршил прозорецот.

б) Имаме:

$$1 = (c' \cap b' \cap c' \cap a) \cup (c \cap b \cap c' \cap a) \cup (c \cap b' \cap c \cap a) \cup (c \cap b' \cap c' \cap a') =$$
$$= (c' \cap b' \cap a) \cup 0 \cup (c \cap b' \cap a) \cup 0 = (c' \cup c) \cap b' \cap a = b' \cap a,$$

од каде што добиваме $b = 0$ и $a = 1$. Значи, Андон го скршил прозорецот, при што одговорот на Андон е погрешен.

§ 9. МОДУЛИ И ВЕКТОРСКИ ПРОСТОРИ

9.1. Нека R а асоцијатавен прстен со единица. Да се покаже дека:

а) K може да се смета за модул над себе;

б) подмножеството $A \subseteq R$ е подмодул од R ако и само ако A е потпрстен од R со својството

$$(\forall x \in R,\ a \in A)\ \ xa \in A. \tag{1}$$

Решение. а) Тврдењето следува од тоа што $R(+)$ е комутативна група, а поради: $1 \cdot x = x$ за $\forall x \in R$, асоцијативноста на множењето и дистрибутивноста на множењето спрема собирањето, исполнети се условите за модул.

б) Нека A е подмодул од R-модулот R и $a,\ b \in A$. Тогаш $a - b,\ ab \in A$, па значи A е потпрстен од R. Ако x е кој било елемент од R, тогаш од дефиницијата за подмодул следува дека $xa \in A$, т.е важи (1).

Обратно, ако A е потпрстен од R со својството (1), тогаш од дефиницијата за подмодул е очигледно дека A е подмодул од R.

9.2. Нека R е асоцијативен прстен со единица и нека

$M = \{(x, x^2) \mid x \in R\}$.

Во M определуваме операција + (собирање) со:

$(x, x^2) + (y, y^2) = (x + y, (x + y)^2)$

и операција "множење" на елементите од R со елементите од M:

$r(x, x^2) = (rx, (rx)^2)$.

Да се провери дали M е R–модул.

Решение. Од комутативноста и асоцијативноста на операцијата + во прстенот R се добива дека $M(+)$ е комутативна полугрупа. Потоа, $(0, 0^2)$ е неутрален елемент во $M(+)$, а $(-x, (-x)^2)$ е инверзен елемент за (x, x^2). Значи, $M(+)$ е комутативна група.

Ако 1 е единица на R, а (x, x^2) е кој било елемент од M, ќе имаме:

$1(x, x^2) = (1x, (1x)^2) = (x, x^2)$.

Бидејќи прстенот R е асоцијативен, за секој пар $r,\ s \in R$ имаме:

$(rs)\ (x, x^2) = ((rs)x, ((rs)x)^2) = (r(sx), (r(sx))^2) = r(sx, (sx)^2)$,

Применувајќи го дистрибутивниот закон во R, ќе имаме:

$(\forall r,\ s \in R)\ (r + s)(x, x^2) = ((r + s)x, ((r + s)x)^2) = (rx + sx, (rx + sx)^2) =$

$= (rx, (rx)^2) + (sx, (sx)^2) = r(x, x^2) + s(x, x^2)$.

На крајот, за кој било $r \in R$ и $(x, x^2), (y, y^2) \in M$ имаме:

$r[(x, x^2) + (y, y^2)] = r(x + y, (x + y)^2) = (r(x + y), (r(x + y))^2) =$

$= (rx + ry, (rx + ry)^2) = (rx, (rx)^2) + (ry, (ry)^2) =$

$= r(x, x^2) + r(y, y^2)$.

Од сето тоа следува дека M е R–модул.

9.3. Секоја комутативна група е $\mathbb{Z}$–модул.

Решение. Ако G е адитивно означена комутативна група, тогаш со:

$(\forall x \in G)\ 0x = 0,\ 1x = x,$

$(\forall n \in \mathbb{N},\ x \in G)\ nx = \underbrace{x + \ldots + x}_{n},\ (-n)x = -nx$

е определено пресликување од $\mathbb{Z} \times G$ во G. Од својствата на комутативните групи е јасно дека G станува $\mathbb{Z}$–модул во однос на така дефинираната операција множење на "скалар" со вектор.

9.4. Нека $A(+)$ е група, R асоцијативен прстен со единица и нека е дефинирано множење на елементите од R со елементите од A што ги задоволува условите:

(i) $r(a + b) = ra + rb$,

(ii) $(r + s)a = ra + sa$,

(iii) $(rs)a = r(sa)$,

(iv) $1 \cdot a = a$,

за кои било $a, b \in A$ и $r, s \in R$. Да се покаже дека A е R–модул.

Решение. Доволно е да се покаже дека групата $A(+)$ е комутативна. Нека 1 е единица на прстенот R и a, b се кои било елементи од A. Според (ii), а потоа, имајќи го предвид (iv), имаме:

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b, \qquad (1)$$

а според (i), применувајќи ги потоа (ii) и (iv), имаме:

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b. \qquad (2)$$

Од (1) и (2) добиваме

$a + b + a + b = a + a + b + b$,

па кратејќи одлево со a и оддесно со b, добиваме $b + a = a + b$.

9.5. Нека A е R модул и нека во множеството $M = R \times A$ дефинираме операции "+" и "*" со:

$$(r_1, a_1) + (r_2, a_2) = (r_1 + r_2, a_1 + a_2) \qquad (1)$$

$$(r_1, a_1) * (r_2, a_2) = (r_1 r_2, r_1 a_2 + a_1). \qquad (2)$$

Да се испитаат својствата на алгебрата $M(+,*)$.

Решение. Групоидот $M(+)$ може да се смета како директен производ од $R(+)$ и $A(+)$, па според тоа, $M(+)$ е комутативна група.

Да ги испитаме својствата на групоидот $M(*)$. Користејќи ја дефиницијата (2) и асоцијативноста на $R(\cdot)$, добиваме дека

$[(r_1, a_1) * (r_2, a_2)] * (r_3, a_3) = (r_1, a_1) * [(r_2, a_2) * (r_3, a_3)]$,

т.е. $M(*)$ е полугрупа. Понатаму, имаме

$(1, 0) * (r, a) = (1r, 1a + 0) = (r, a)$,

$(r, a) * (1, 0) = (r1, r \cdot 0 + a) = (r, a)$,

т.е. полугрупата $M(*)$ е со единица.

Да видиме дали "$*$" е дистрибутивна спрема " + ". Имаме:

$[(r_1,a_1) + (r_2, a_2)] * (r_3, a_3) = (r_1 + r_2, a_1 + a_2) * (r_3, a_3) =$

$=((r_1 + r_2) r_3, (r_1 + r_2) a_3 + a_1 + a_2) = (r_1 r_3 + r_2 r_3, r_1a_3 + r_2 r_3 + a_1 + a_2) =$

$= (r_1r_3, r_1 a_3 + a_1) + (r_2 r_3, r_2 a_3 + a_2) =$

$= (r_1, a_1) * (r_3, a_3) + (r_2, a_2) * (r_3, a_3)$

т.е. важи десниот дистрибутивен закон. Бидејќи

$(0, a_1) * [(r, a) + (r, a)] = (0, a_1)$

$(0, a_1) * (r, a) + (0, a_1) * (r, a) = (0, a_1 + a_1)$,

следува дека левиот дистрибутивен закон не важи.

Значи, алгебрата $M(+, *)$ не е прстен. (Алгебрата $M(+, *)$ се вика *скоро–прстен*.)

9.6. Нека A и B се два R–модула. За пресликувањето $f : A \to B$ велиме дека е *модулен хомоморфизам* (или накусо, *R–хомоморфизам*) ако се исполнети следниве услови:

$(\forall x, y \in A)\ f(x + y) = f(x) + f(y)$, (1)

$(\forall r \in R, x \in A)\ f(rx) = rf(x)$. (2)

Ако R–хомоморфизмот f е инјекција, сурјекција, биекција, тогаш f го викаме *R–мономорфизам*, *R–епиморфизам*, *R–изоморфизам*, соодветно.

Да се покаже дека производот на R–хомоморфизми (R–мономорфизми, R–епиморфизми, R–изоморфизми) е R–хомоморфизам (R–мономорфизам, R–епиморфизам, R–изоморфизам, соодветно).

Решение. Нека $f : A \to B$ и $g : B \to C$ се R–хомоморфизми. Тогаш, за пресликувањето $gf : A \to C$, дефинирано со: $(\forall x \in A)\ (gf)(x) = g(f(x))$, имаме:

$(gf)(x + y) = g(f(x + y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y))$,

$(gf)(rx) = g(f(rx)) = g(rf(x)) = rg(f(x))$,

што значи дека gf е R–хомоморфизам.

Ако f, g се R–мономорфизми, тогаш тие се инјекции, па според 2.17., gf е инјекција, што значи дека gf е R–мономорфизам. Слично ако f и g се R–епиморфизми или R–изоморфизми.

9.7. Да се покаже дека R–хомоморфизмот $f : A \to B$ е R–мономорфизам ако и само ако за кој било R-модул M и кои било R–хомоморфизми $g_1, g_2 : M \to A$ е исполнет условот

$fg_1 = fg_2 \Rightarrow g_1 = g_2$

(т.е. f може да се "крати" одлево).

Упатство. Види 2.23.

9.8. Да се покаже дека R–хомоморфизмот $f : A \to B$ е R–епиморфизам ако и само ако за кој било R–модул N и кои било R–хомоморфизми $h_1, h_2 : B \to N$ е исполнет условот

$h_1 f = h_2 f \Rightarrow h_1 = h_2$

(т.е. f може да се "крати" оддесно).

Упатство. Види 2.24.

9.9. Да се покаже дека:

а) ако gf е мономорфизам, тогаш f е мономорфизам.

б) ако gf е епиморфизам, тогаш g е епиморфизам.

9.10. Пресек на произволна фамилија R–подмодули е R–подмодул. Докажи!

9.11. Нека $f : A \to B$ е модулен хомоморфизам. Да се покаже дека множествата

$\mathrm{Ker} f = \{a \mid a \in A, f(a) = 0\}$,

$\mathrm{Im} f = \{b \mid b \in B, (\exists a \in A) f(a) = b\}$

се подмодули од A и B соодветно.

Дали множеството $\mathrm{Ker} f$ може да биде празно ?

$\mathrm{Ker} f$ се вика *јадро* на f.

Одговор. $\mathrm{Ker} f$ содржи барем еден елемент; имено, $0 \in \mathrm{Ker} f$ бидејќи секогаш $f(0) = \{0\}$, па $\mathrm{Ker} f$ не е празно.

9.12. Да се покаже дека R–хомоморфизмот $f : A \to B$ е R–мономорфизам ако и само ако $\mathrm{Ker} f = \{0\}$.

Решение. Нека $f : A \to B$ е R–мономорфизам и нека x е кој било елемент од $\mathrm{Ker} f$. Тогаш имаме $f(x) = 0 = f(0)$, па бидејќи f е инјекција, добиваме $x = 0$, што значи дека $\mathrm{Ker} f = \{0\}$.

Обратно, нека $\mathrm{Ker} f = \{0\}$.

Ако x_1, x_2 се произволни елементи од A, такви што $f(x_1) = f(x_2)$, тогаш од $f(x_1) - f(x_2) = 0$ добиваме $f(x_1 - x_2) = 0$, т.е. $x_1 - x_2 \in \mathrm{Ker} f$.

Бидејќи $\mathrm{Ker} f = \{0\}$, имаме $x_1 - x_2 = 0$, т.е. $x_1 = x_2$, што значи R–хомоморфизмот f е инјекција, па според тоа f е R– мономорфизам.

9.13. Нека C е непразно подмножество од R-модулот A. Ако
$[RC] = \{r_1c_1 + r_2c_2 + \ldots + r_n c_n \mid r_i \in R,\ c_i \in C,\ n \in \mathbb{N}\}$,
да се покаже дека $[RC]$ е подмодул од A.

За подмодулот $[RC]$ велиме дека е *генериран* од множеството C.

9.14. Ако $f : A \to B$ е R–хомоморфизам, а $g : B \to M$ е R–мономорфизам, тогаш $\mathrm{Ker}\,(gf) = \mathrm{Ker} f$.

Решение. Нека $x \in \mathrm{Ker}(gf)$; тоа значи дека $(gf)(x) = g(f(x)) = 0$, а бидејќи g е R–мономорфизам, според 9.7, добиваме $f(x) = 0$, т.е. $x \in \mathrm{Ker} f$. Значи имаме $\mathrm{Ker}(gf) \subseteq \mathrm{Ker} f$. Слично добиваме и $\mathrm{Ker} f \subseteq \mathrm{Ker}(gf)$, т.е.
$\mathrm{Ker}(gf) = \mathrm{Ker} f$.

9.15. Нека A и B се дадени R–модули. Во множеството $\mathrm{Hom}_R(A,B)$ од сите R–хомоморфизми од A во B дефинираме операција собирање на R–хомоморфизми $f, g \in \mathrm{Hom}_R(A,B)$ со :

$$(\forall x \in A)\ (f + g)(x) = f(x) + g(x) \qquad (1)$$

и операцијата множење на R–хомоморфизам f со елемент $s \in R$ со :

$$(\forall x \in A)\ (sf)(x) = sf(x). \qquad (2)$$

Да се покаже дека:

а) $\mathrm{Hom}_R(A,B)(+)$ е комутативна група.

б) ако прстенот R е комутативен, тогаш $\mathrm{Hom}_R(A,B)$ е R–модул.

Решение. а) Нека f и g се R–хомоморфизми од A во B и нека $h = f + g$. Тогаш, за кои било $a, a' \in A$ и $r \in R$ имаме:

$$h(a + a') = (f + g)(a + a') = f(a + a') + g(a + a') =$$
$$= f(a) + f(a') + g(a) + g(a') =$$
$$= f(a) + g(a) + f(a') + g(a') = (f + g)(a) + (f + g)(a') = h(a) + h(a'),$$
$$h(ra) = (f + g)(ra) = f(ra) + g(ra) = rf(a) + rg(a) = r[f(a) + g(a)] =$$
$$= r(f + g)(a) = rh(a),$$

што значи $f + g$ е исто така R–хомоморфизам, т.е. операцијата "+" со (1) е добро дефинирана.

Од комутативноста на операцијата "+" во B следува дека
$f + g = g + f$.

Ако f, g и h се R–хомоморфизми од A во B, тогаш

$$[f + (g + h)](x) = f(x) + (g + h)(x) = f(x) + g(x) + h(x) =$$
$$= (f + g)(x) + h(x) = [(f + g) + h](x),$$
$$f + (g + h) = (f + g) + h.$$

R–хомоморфизмот $\omega : A \to B$, дефинирано со: $(\forall a \in A)\ \omega(a) = 0$, е нула во групоидот $\mathrm{Hom}_R(A, B)$, а за кој било R–хомоморфизам f, R–хомоморфизмот дефиниран со : $(\forall a \in A)\ (-f)(a) = -f(a)$, е спротивен на f.

Од сето тоа следува дека $\mathrm{Hom}_R(A, B)$ е комутативна група.

б) Да покажеме прво дека sf, дефинирано со (2), е R–хомоморфизам кога прстенот R е комутативен. Затоа, нека $a, a' \in A$ и $r \in R$ се произволни. Имаме:

$(sf)(a + a') = sf(a + a') = s(f(a) + f(a')) = sf(a) + sf(a') = (sf)(a) + (sf)(a')$,

$(sf)(ra) = sf(ra) = s[rf(a)] = (sr)f(a) = (rs)f(a) = r[sf(a)] = r[(sf)(a)]$,

што значи дека sf е R–хомоморфизам.

Да покажеме уште дека се исполнети условите (i) – (iv) од 9.4.

Нека f, g се хоморфизми од A во B, r, s произволни елементи од R и

$f_1 = r(f + g)$, $f_2 = (r + s)f$, $f_3 = (rs)f$.

Имаме:

$f_1(a) = [r(f + g)](a) = r[(f + g)(a)] = r[f(a) + g(a)] = rf(a) + rg(a) =$
$= (rf)(a) + (rg)(a) = (rf + rg)(a)$, т.е.

$r(f + g) = rf + rg$;

$f_2(a) = [(r + s)f](a) = (r + s)f(a) = rf(a) + sf(a) = (rf + sf)(a)$, т.е.

$(r + s)f = rf + sf$;

$f_3(a) = [(rs)f]((r + s)f = rf + sf$;

$f_3(a) = [(rs)f](a) = (rs)f(a) = r[sf(a)] = r[(sf)(a)] = [r(sf)](a)$, т.е.

$(rs)f = r(sf)$;

$1f(a) = f(a)$, т.е. $1f = f$.

Од сето тоа следува дека $\mathrm{Hom}_R(A, B)$ кога прстенот R е комутативен, е R–модул.

9.16. Да се воведе поим за конгруенција во R–модул, а потоа да се воведе поим за фактор–модул.

Решение. Нека е α еквивалентност во R–модулот A. Ако α е согласна со операцијата во A, т.е.

$$a_1 \alpha b_1 \text{ и } a_2 \alpha b_2 \Rightarrow (a_1 + a_2)\ \alpha\ (b_1 + b_2), \tag{1}$$

и со операцијата множење на елементите од R со елементите од A, т.е.

$$(\forall r \in R)\ a\ \alpha\ b \Rightarrow (ra)\ \alpha\ (rb) \tag{2}$$

тогаш велиме дека α е *конгруенција* во R–модулот A.

Нека α е конгруенција во A и нека е означено со $A/_\alpha$ множеството од сите класи еквивалентни елементи при конгруенцијата α, т.е. $A/_\alpha = \{a^\alpha \mid a \in A\}$. Дефинирајќи операција "+" во $A/_\alpha$ со

$$a^{\alpha} + b^{\alpha} = (a+b)^{\alpha} \qquad (3)$$

добиваме дека $A/_{\alpha}(+)$ е комутативна група, а дефинирајќи множење на елементите од R со елементите од $A/_{\alpha}$ со :

$$r\imath^{\alpha} = (ra)^{\alpha}, \qquad (4)$$

добиваме дека $A/_{\alpha}$ е R–модул; $A/_{\alpha}$ се вика *фактор–модул по конгруенцијата* α, а пресликувањето $\pi : A \to A/_{\alpha}$, дефинирано со: $\pi(a) = a^{\alpha}$ се вика *природен епиморфизам.*

9.17. Да се покаже дека на кој било подмодул L од R–модулот A одговара конгруенција α во A, а и обратно, на која било конгруенција α во A одговара подмодул L од A.

Решение. Нека L е подмодул од R–модулот A и нека дефинираме релација α во A со:

$a\alpha b \Leftrightarrow a - b \in L$.

Бидејќи $a - a = 0 \in L$, имаме $a\alpha a$, за кој било $a \in A$, т.е. релацијата α е рефлексивна. Потоа, ако $a\ \alpha\ b$, тогаш $a - b \in L$, а бидејќи L е подмодул, имаме $(b - a) = -(a - b) \in L$, што значи дека $b\alpha a$, т.е. рела-цијата α е симетрична. На крајот, ако $a\alpha b$ и $b\alpha c$, тогаш $a - b$, $b - c \in L$, па и $(a - b) + (b - c) = a - c \in L$, што значи дека релацијата α е еквивалентност во A.

Понатаму имаме:

$a_1\alpha b_1,\ a_2\alpha b_1 \Rightarrow a_1 - b_1,\ a_2 - b_2 \in L \Rightarrow (a_1 + a_2) - (b_1 + b_2) \in L \Rightarrow$

$\Rightarrow (a_1 + a_2)\ \alpha\ (b_1 + b_2)$;

$a\alpha b \Rightarrow a - b \in L \Rightarrow (\forall r \in R)\ r(a - b) = ra - rb \in L \Rightarrow (\forall r \in R)\ ra\ \alpha\ rb$,

т.е. α е конгруенција во A.

Обратно, нека α е конгруенција во R–модулот A и нека

$L = \{a \mid a \in A,\ a\ \alpha\ 0\}$

Тогаш имеме:

$a, b \in L \Rightarrow a\ \alpha\ 0,\ b\ \alpha\ 0 \Rightarrow (\forall r, s \in R)\ (ra)\ \alpha\ 0, (sb)\ \alpha\ 0 \Rightarrow$

$\Rightarrow (\forall r, s \in R)\ (ra + sb)\ \alpha\ 0 \Rightarrow (\forall r, s \in R)\ ra + sb \in L$,

т.е. L е подмодул од R–модулот A.

Од изнесеното (и од задачата 9.16.) следува дека има смисла да се зборува за фактор–модул на R–модулот A над подмодулот L. Имено, множеството

$A/L = \{a + L \mid a \in A\}$

во однос на собирањето: $(a + L) + (a' + L) = (a + a') + L$ и множењето со елементи од R : $r(a + L) = ra + L$, *е фактор–модул на A над L.*

9.18. Нека $f : A \to B$ е R–хомоморфизам и L подмодул од $\mathrm{Ker} f$.

Покажи дека:

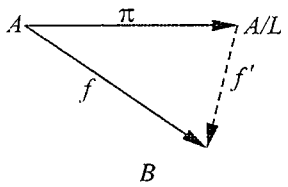
а) f може на единствен начин да се престави како производ $f'\pi$, каде што $\pi : A \to A/L$ е природниот епиморфизам $(\forall a \in A)\ \pi(a) = a + L$ (види дијаграм).

Во овој случај велиме дека f *еднозначно поминува низ* π.

б) Ако f е епиморфизам со јадро L, тогаш $A/L \cong B$ при f'.

Решение. а) Да ставиме

$$(\forall\, a + L \in A/L)\ f'(a + L) = f(a).$$



Бидејќи $L \subseteq \mathrm{Ker} f$, f' е добро дефинирано, а бидејќи

$$(f'\pi)(a) = f'(\pi(a)) = f'(a + L) = f(a)$$

за секој $a \in A$, добиваме $f = f'\pi$.

Ако f'' е R–хомоморфизам со својството $f = f''\pi$, тогаш од $f''\pi = f'\pi$, бидејќи π е епиморфизам, добиваме $f'' = f'$.

б) Бидејќи f е епиморфизам, тогаш $f'\pi$ е епиморфизам, а според 9.9. следува дека f' е епиморфизам. Да покажеме уште дека f' е и мономорфизам.

Ако $f'(a_1 + L) = f'(a_2 + L)$, т.е. $f(a_1) = f(a_2)$, тогаш имаме $f(a_1 - a_2) = 0$, т.е. $a_1 - a_2 \in L$, што значи дека $a_1 + L = a_2 + L$.

Од ова следува дека f' е изоморфизам.

9.19. Ако L е подмодул од A и $h : A \to B$ е R–хомоморфизам, таков што $h(L) = 0$ и секој хомоморфизам $f : A \to A'$ еднозначно поминува низ h (види 9.18.), тогаш постои изоморфизам $h' : A/L \to B$, при што $h = h'\pi$ ($\pi : A \to A/L$ е природниот епиморфизам).

Решение. Од условот на оваа задача имаме дека $\pi : A \to A/L$ еднозначно поминува низ h, па $\pi = \pi' h$. Но, според 9.18, имаме $h = h'\pi$, па значи $h = h'\pi = (h'\pi')h = 1h$, од каде што, поради еднозначноста на разложувањето на h, имаме $h'\pi' = 1$. Од причини на симетрија имаме $\pi' h' = 1$. Значи, $\pi' = (h')^{-1}$ и h' е бараниот изоморфизам.

9.20. Нека $\{A_i \mid i \in I\}$ е фамилија R–модули и во директниот производ од множествата A_i, означен со $P = \prod_{i \in I} A_i$, нека се определени операции собирање на елементи од P и множење на елемент од R со елемент од P на следниов начин:

$$(a_i) + (a_i') = (a_i + a_i'),\quad r(a_i) = (ra_i), \tag{1}$$

$r \in R$, $(a_i), (a_i') \in P$. Да се покаже дека:

а) P во однос на операциите (1) е R–модул.

б) Пресликувањата $\pi_i : P \to A_i,\ i \in I,$ дефинирано со:

$$\pi_i((a_i)) = a_i \tag{2}$$

се R-епиморфизми.

$P = \prod_i A_i$ се вика *директен производ* на дадената фамилија R-модули, а π_i се викаат *проекции на директниот производ*.

Решение. Јасно е дека $P(+)$ е абелова група, а лесно се проверува дека се исполнети и условите (i)–(iv) од 9.4. Значи, P е R-модул.

б) Нека (a_i), (a_i') се кои било елементи од P, а r е кој било елемент од R. Имаме:

$$\pi_i((a_i) + (a_i')) = \pi_i((a_i + a_i')) = a_i + a_i' = \pi_i((a_i)) + \pi_i((a_i'));$$

$$\pi_i(r(a_i)) = \pi_i((ra_i)) = ra_i = r\pi_i((a_i)),$$

што значи π_i е R-хомоморфизам. Но, јасно е дека π_i е сурјекција, па значи π_i е R-епиморфизам.

9.21. Нека $\{A_i \mid i \in I\}$ е произволна фамилија R-модули, M е кој било R-модул и $\{f_i : M \to A_i \mid i \in I\}$ која било фамилија R-хомоморфизам. Да се покаже дека постои еднозначно определен R-хомоморфизам $f : M \to P$, $P = \prod_i A_i$ таков што $\pi_i f = f_i$, каде што π_i е i-тата проекција на P.

Упатство. Види 2.45.

9.22. Нека $\{A_i \mid i \in I\}$ е фамилија R-модули, A е даден R-модул и $\{g_i : A \to A_i\}$ е фамилија R хоморфизми, така што за секој R-модул M и секоја фамилија R-хомоморфизми $f_i : M \to A_i$ постои еднозначно определен R-хомоморфизам $f : M \to A$ со својството $g_i f = f_i\ \forall i \in I$. Да се покаже дека A е изоморфен со директниот производ $P = \prod_{i \in I} A_i$,

Упатство. Види 2.46.

9.23. Нека $P = \prod_i A_i$ е директниот производ на фамилијата R-модули A_i, $i \in I$, а $\lambda_i : A_i \to P$ нека е дефинирано со:

$(\forall a_i \in A_i)\ \lambda_i(a_i) = (0a_i0)$,

каде што $(0a_i0)$, е елемент во P чија i-та компонента е a_i а сите други се нули. Да се покаже дека:

а) λ_i е R-мономорфизам за секој $i \in I$.

б) $\pi_i\lambda_i = 1_{A_i}$, $\pi_k\lambda_i = 0$ при $k \neq i$,

каде што π_i е i–тата проекција на директниот производ. За λ_i велиме дека е *i–та инјекција* на директниот производ.

Решение. а) Ако $a_i, b_i \in A_i$ и $r \in R$, тогаш

$$\lambda_i(a_i + b_i) = (0\ a_i + b_i\ 0) = (0\ a_i\ 0) + (0\ b_i\ 0) = \lambda_i(a_i) + \lambda_i(b_i),$$

$$\lambda_i(ra_i) = (0\ ra_i\ 0) = r(0\ a_i\ 0) = r\lambda_i(a_i),$$

т.е. λ_i е R–хомоморфизам.

Потоа, ако $\lambda_i(a_i) = \lambda_i(b_i)$, тогаш $(0\ a_i\ 0) = (0\ b_i\ 0)$ од што следува дека $a_i = b_i$, т.е. λ_i е инјекција.

Значи, λ_i е R–мономорфизам.

б) Нека a_i е кој било елемент од A_i. Имаме :

$$(\pi_i \lambda_i)(a_i) = \pi_i(\lambda_i(a_i)) = \pi_i((0\ a_i\ 0)) = a_i = 1_{A_i}(a_i),$$

$$(\pi_k \lambda_i)(a_i) = \pi_k \lambda_i(a_i)) = \pi_k((0\ a_i\ 0)) = 0,$$

што значи дека $\pi_i\lambda_i = 1_{A_i}$, $\pi_k\lambda_i = 0$ при $k \neq i$.

9.24. Да го означиме со S подмножеството од R–модулот $P = \prod_i A_i$ (од 9.20), кое се состои од сите елементи што имаат конечно многу компоненти различни од нула. Да се покаже дека S е подмодул од P. S се вика *директна сума на фамилијата* $\{A_i \mid i \in I\}$ и се означува со $\oplus \sum_{i \in I} A_i$. Во случај на конечна фамилија R–модули, т.е. кога е $I = \{1, 2, \ldots, n\}$, пишуваме $S = A_1 \oplus A_2 \oplus \ldots \oplus A_n$; во овој случај е јасно дека S и P се совпаѓаат.

Решение. Ако $a, b \in S$, тогаш $ra, sb \in S$, за кои било $r, s \in R$ а исто така $ra + sb \in S$, што значи дека S е подмодул од P.

9.25. Да се покаже дека секој елемент $a = (a_i)$ од директната сума S на фамилијата R–модули A_i, $i \in I$, може да се претстави на единствен начин во облик

$$a = \sum_i \lambda_i(a_i) \qquad (1)$$

каде што збирот е конечен, а λ_i се инјекциите на директната сума.

Решение. Кој било елемент $a = (a_i)$ од S има само конечно многу компоненти различни од нула, на пример $a_{i_1}, \ldots, a_{i_n}$, па според тоа имаме:

$$s = (a_i) = (0\,a_{i_1}\,0)+\ldots+(0\,a_{i_n}\,0) = \lambda_{i_1}(a_{i_1})+\ldots+\lambda_{i_n}(a_{i_n}) =$$

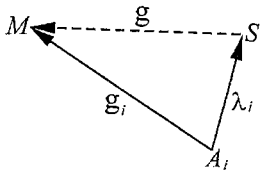
$$= \sum_{v=1}^{n} \lambda_{i_v}(a_{i_v}).$$

Ако $a = \sum_{v=1}^{m} \lambda_{j_v}(b_{j_v})$ е друго претставување на елементот a во облик (1), тогаш можеме да ставиме $a = (b_j)$, при што само компонентите $j_1, \ldots, j_m$ не се нули, па од $(b_j) = (a_i)$ следува дека $m = n$ и дека соодветните компоненти се еднакви, т.е. $b_{j_v} = a_{j_v}$; $v = 1,\ldots,n$.

Значи, претставувањето (1) е еднозначно.

9.26. Нека $\{A_i \mid i \in I\}$ е произволна фамилија R–модули, M е кој било R-модул и $\{g_i : A_i \to M\}$ е која било фамилија R–хомоморфизми. Да се покаже дека постои еднозначно определен R–хомоморфизам $g : S \to M$, таков што $g_i = g\lambda_i$, каде што λ_i е i–тата инјекција на директната сума.

Решение. Нека $a = (a_i)$ е кој било елемент од S и $g_i : A_i \to M$ нека е определено со $g_i(a_i) = y_i$. Да дефинираме пресликување $g : S \to M$ на следниов начин:



$$g(a) = \sum_i g_i(a_i).$$

Сумата $\sum_i g_i(a_i)$ е конечна, зашто $a = (a_i)$ има само конечно многу компоненти различни од нула, па таа е еднозначно определен елемент од M, што значи дека пресликувањето g е добро дефинирано. Бидејќи g_i се R–хомоморфизми, R-хомоморфизам е и g.

Ако $h : S \to M$ е R–хомоморфизам со својството $g_i = h\lambda_i$, $i \in I$, тогаш користејќи го резултатот од 9.25., имаме:

$$h(a) = h\Big(\sum_i \lambda_i(a_i)\Big) = \sum_i h\lambda_i(a_i) = \sum_i g_i(a_i) = g(a),$$

што значи дека $h = g$, т.е. g е единствен со тоа својство.

9.27. Да се покаже дека за инјекцијата λ_i и проекциите π_i на директната сума $S = A_1 \oplus A_2$ важи равенството

$$\lambda_1 \pi_1 + \lambda_2 \pi_2 = 1_S \qquad (1)$$

и, поопшто, ако S е директна сума на фамилијата R–модули A_i, $i \in I$, тогаш

$$\sum_i \lambda_i \pi_i = 1_S, \tag{2}$$

при што збирот е конечен.

Решение. Нека (a_1, a_2) е кој било елемент од S. Имаме:

$$(\lambda_1 \pi_1 + \lambda_2 \pi_2)((a_1, a_2)) = \lambda_1 \pi_1((a_1, a_2)) + \lambda_2 \pi_2((a_1, a_2)) =$$
$$= \lambda_1(a_1) + \lambda_2(a_2) = (a_1, 0) + (0, a_2) = (a_1, a_2),$$

што значи дека равенството (1) е точно.

Ако (a_i) е кој било елемент од S, тогаш тој има само конечно многу компоненти различни од нула, да ги означиме нив со $a_{i_1}, \ldots, a_{i_n}$ Ако со $\lambda_{i_1}, \ldots, \lambda_{i_n}$ ги означиме соодветните инјекции, а со $\pi_{i_1}, \ldots, \pi_{i_n}$ соодветните проекции на S, тогаш имаме

$$\pi_{i_v}((a_i)) = a_{i_v}, \lambda_{i_v}(a_{i_v}) = (0 a_{i_v}\ 0), v = 1, 2, \ldots, n,$$ па според тоа:

$$(\sum_{v=1}^{n} \lambda_{i_v} \pi_{i_v})((a_i)) = \sum_{v=1}^{n} \lambda_{i_v}(a_{i_v}) = \sum_{v=1}^{n} (0 a_{i_v}) = a_i),$$

т.е. точно е равенството (2).

9.28. Дадени се R–хомоморфизми $f_{ij} : A_i \to A'_j$, $i, j = 1,2$. Да се покаже дека постои единствен R–хомоморфизам $g : S \to S'$, $S = A_1 \oplus A_2$ и $S' = A'_1 \oplus A'_2$, што ги задоволува равенствата

$$\pi_j g \lambda_i = f_{ij}, \quad i, j = 1, 2, \tag{1}$$

каде што λ_i е i–тата инјекција на S, а π'_j е j–тата проекција на S'.

Решение. Пресликувањето $g : S \to S'$, дефинирано со:

$$g(a_1, a_2) = (f_{11}(a_1) + f_{21}(a_2),\ f_{12}(a_1) + f_{22}(a_2)) \tag{2}$$

е R–хомоморфизам што ги задоволува равенствата (1), т.е. $\pi'_j h \lambda_i = f_{ij}$. Бидејќи $\lambda'_j \pi'_j h \lambda_i = \lambda'_j f_{ij}$, $(i, j = 1,2)$, добиваме:

$$(\lambda'_1 \pi'_1 + \lambda'_2 \pi'_2) h \lambda_i = \lambda'_1 f_{i1} + \lambda'_2 f_{i2},$$

а според 9.27., добиваме $h\lambda_i = \lambda'_1 f_{i1} + \lambda'_2 f_{i2}$,

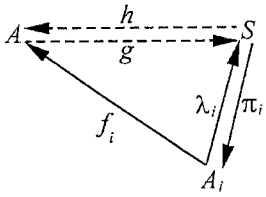
На ист начин добиваме $g\lambda_i = \lambda'_1 f_{i1} + \lambda'_2 f_{i2}$, што значи $h\lambda_i = g\lambda_i$. Од ова равенство, поради $\lambda_i \pi_i = 1_{A_i}$, добиваме $h = g$, што значи дека g, определен со (2), е единствениот R-хомоморфизам што ги задоволува равенствата (1).

9.29. Нека $\{A_i \mid i \in I\}$ е фамилија R–модули и A е даден R–модул, така што се исполнети условите:

(i) постојат R–хомоморфизми $f_i : A_i \to A$ $(i \in I)$;

(ii) за секој R–модул M и за секоја фамилија R–хомоморфизми $g_i : A_i \to M$ $(i \in I)$ постои еднозначно определен R–хомоморфизам $g : A \to M$, таков што $gf_i = g_i$.

Да се покаже дека A е изоморфен со директната сума S на дадената фамилија R–модули.



Решение. Ако на местото од M и од g_i, $i \in I$ ја ставиме директната сума S и инјекциите λ_i, $i \in I$, тогаш постои еднозначно определен R-хомоморфизам g: $A \to S$, таков што $gf_i = \lambda_i$. Според 9.23. имаме $\pi_i\lambda_i = 1_{A_i}$, а според 9.27. имаме $\sum_i \lambda_i\pi_i = 1_S$ каде што π_i е i–тата проекција на S. Потоа, според 9.26. постои еднозначно определен R–хомоморфизам $h : S \to A$, таков што $h\lambda_i = f_i$.

Имаме:

$$gh = gh1_S = gh \sum_i \lambda_i\pi_i = g\sum_i h\lambda_i\pi_i = g\sum_i f_i\pi_i = \sum_i gf_i\pi_i = \sum_i \lambda_i\pi_i = 1_S,$$

што значи дека $g : A \to S$ е изоморфизам, $g^{-1} = h$.

9.30. Да се покаже дека R–модулот M е (внатрешна) директна сума на своите подмодули A_1 и A_2 ако и само ако $M = A_1 + A_2$ и $A_1 \cap A_2 = 0$. Резултатот да се обопшти за произволна фамилија подмодули.

9.31. R-модулот A е *директен суманд* на R–модулот M (т.е. постои R–модул B, таков што $M = A \oplus B$) ако и само ако постои инјекција $\lambda : A \to M$ и проекција $\pi : M \to A$, такви што $\pi\lambda = 1_A$

9.32. Нека $f_i : A_i \to B$, и $i = 1,2$, се дадени R–хомоморфизми. Да се покаже дека R–модулот B е дирекна сума од A_1, A_2 ако и само ако:

(i) $B = f_1(A_1) + f_2(A_2)$ и

(ii) постојат R–хомоморфизми $\pi_i : B \to A_i$, такви што $\pi_i f_i = 1_{A_i}$, $\pi_k f_k = 0$ при $k \neq i$ $(i, k = 1,2)$.

Да се обопшти за произволна фамилија $\{f_i : A_i \to B\}$.

9.33. Нека U и V се векторски простори над полето P, при што $\dim U = m$, $\dim V = n$. Ако $W = U \times V$, да се покаже дека $\dim W = m + n$.

Решение. Нека $\dim U = m$, $\dim V = n$, при што $u_1, u_2, \ldots, u_m$ е база на U, а $v_1, v_2, \ldots, v_n$ е база на V. Множеството вектори

$$(u_1, 0), \ldots, (u_m, 0), \quad (0, v_1), \ldots, (0, v_n) \qquad (1)$$

е линеарно независно во W. Навистина, од равенството

$$x_1(u_1, 0) + \ldots + x_m(u_m, 0) + y_1(0, v_1) + \ldots + y_n(0, v_n) = 0,$$

следува дека

$$x_1 u_1 + \ldots + x_m u_n = 0, \quad y_1 v_1 + \ldots + y_n v_n, = 0,$$

а бидејќи $u_1, \ldots, u_m$ и $v_1, \ldots, v_n$ се бази во U, односно V, добиваме

$$x_1 = \ldots = x_m = y_1 = \ldots y_n = 0.$$

Нека сега $(u,v) \in W$ е произволен елемент; тогаш постојат единствени скалари $x_i, y_j \in P$, $i = 1,2, \ldots, m$ $j = 1,2, \ldots, n$ такви што

$$u = x_1 u_1 + \ldots + x_m u_m, \quad v = y_1 v_1 + \ldots + y_n v_n,$$

па имаме

$$(u, v) = x_1(u_1, 0) + \ldots + x_m(u_m, 0) + y_1(0, v_1) + \ldots + y_n(0, v_n),$$

од што следува дека множеството вектори (1) е база во W. Бидејќи множеството (1) содржи $m + n$ елементи, добиваме

$$\dim W = m + n.$$

9.34. Нека $L(U, V)$ е множеството од сите линеарни пресликувања од векторскиот простор U во векторскиот простор V (над полето P). Во $L(U, V)$ дефинирани се операциите собирање и множење со скалар како во 9.15. Да се покаже дека $L(U, V)$ е векторски простор над полето P.

Упатство. Види 9.15.

9.35. Нека U и V се векторски простори над исто поле P.

Нека $u_1, u_2, \ldots, u_n$ е база на U и $v_1, v_2 \ldots, v_n$ произволни вектори од V.

Тогаш постои единствено линеарно пресликување $f : U \to V$, такво што

$$f(u_i) = v_i, \quad i = 1, 2, \ldots, n. \tag{1}$$

Решение. За кој било вектор $u \in U$ постојат еднозначно определени скалари $x_1, \ldots, x_n$, така што $u = x_1 u_1 + \ldots + x_n u_n$. Да дефинираме пресликување $f: U \to V$ со:

$$(\forall u \in U) f(u) = x_1 v_1 + \ldots + x_n v_n. \tag{2}$$

Бидејќи $u_i = 0 \cdot u_1 + \ldots + 1 \cdot u_i + 0 \cdot u_{i+1} + \ldots + 0 \cdot u_n$, имаме $f(u_i) = v_i$ за секој $i = 1, 2, \ldots, n$.

Вака дефинираното пресликување е линеарно, па значи постои барем едно линеарно пресликување $f : U \to V$ со својството (1).

Да покжеме дека тоа е и единствено. Затоа нека $g : U \to V$ е линеарно пресликување со својството $g(u_i) = v_i$ $i = 1, \ldots, n$. За $u = x_1 u_1 + \ldots + x_n u_n$ имаме:

$g(u) = g(x_1 u_1 + \ldots + x_n u_n) = x_1 g(u_1) + \ldots + x_n g(u_n) =$
$= x_1 v_1 + \ldots + x_n v_n = f(u).$

Значи, за секој $u \in U$ имаме $g(u) = f(u)$, т.е. $g = f$.

9.36. Ако U и V се векторски простори над полето P и ако $\dim U = m$, $\dim V = n$, тогаш $\dim L(U, V) = mn$.

Решение. Да претпоставиме дека $u_1, \ldots, u_m$ е база на U, а $v_1, \ldots, v_n$ е база на V. Според 9.35. секој елемент $f \in L(U, V)$ е еднозначно определен ако се познати елементите $f(u_i) \in V$, $i = 1, 2, \ldots, m$. Да ги дефинираме линеарните пресликувања $f_{ij} \in L(U, V)$, $j = 1, \ldots, n$ со:

$f_{ij}(u_i) = v_j$, $f_{ij}(u_k) = 0$ за $k \neq i$.

Нека f е произволен елемент од $L(U, V)$, при што $f(u_i) = w_i$, $i = 1, 2, \ldots, m$. Секој w_i е линеарна комбинација од $v_1, \ldots, v_n$, па

$$w_k = x_{k1} v_1 + \ldots + x_{kn} v_n, \quad k = 1, 2, \ldots, m, \quad x_{ij} \in P \quad . \tag{1}$$

Пресликувањето $g : U \to V$, дефинирано со:

$$g = \sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} f_{ij}$$

е линеарно и притоа имаме :

$$g(u_k) = \sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} f_{ij}(u_k) = \sum_{j=1}^{n} x_{kj} f_{kj}(u_k) = \sum_{j=1}^{n} x_{kj} v_j =$$
$$= x_{k1} v_1 + \ldots + x_{kn} v_n = w_k.$$

Но бидејќи $f(u_k) = w_k$, следува дека $g = f$. Значи, множеството $\{f_{ij}\}$ го генерира $L(U,V)$.

Да покажеме дека множеството $\{f_{ij}\}$ е линеарно независно. Затоа, нека

$$\sum_{i=1}^{m} \sum_{j=1}^{n} x_{ij} f_{ij} = \omega,$$

каде што ω е нулата во $L(U,V)$. За u_k, $k = 1, \ldots, m$, равенството се сведува на:

$$x_{k1} v_1 + x_{k2} v_2 + \ldots + x_{kn} v_n = 0,$$

од каде што следува $x_{k1} = x_{k2} = \ldots = x_{kn} = 0$, за $k = 1, 2, \ldots, m$, т.е. множеството $\{f_{ij}\}$ е линеарно независно.

Значи, $\{f_{ij}\}$ е база за $L(U,V)$, а бидејќи тоа има mn елементи, следува дека $\dim L(U, V) = mn$.

9.37. Ако U е векторски простор над полето P, тогаш секој елемент од $L(U, U)$ се вика *линеарна трансформација* на U. Да се покаже дека $L(U, U)$ е прстен.

Решение. Според 9.15. $L(U, U)(+)$ е комутативна група. Да покажеме дека производ fg на линеарни трансформации f, g е линеарна трансформација. Имаме:

$(\forall u,v\in U)\ (fg)(u+v)=f(g(u+v))=f(g(u)+g(v))=$
$=f(g(u))+f(g(v))=(fg)(u)+(fg)(v)$;

$(\forall u\in U, r\in P)\ (fg)(ru)=f(g(ru))=f(rg(u))=rf(g(u))=r(fg)(u)$.

Потоа, ако f, g и h се линеарни трансформации, а u кој било елемент од U, имаме:

$((f+g)h)(u)=(f+g)(h(u))=f(h(u))+g(h(u))=(fh)(u)+(gh)(u)$, т.е.

$(f+g)h=fh+gh$,

а слично и $f(g+h)=fg+fh$. Значи, $L(U, U)$ е прстен. Да забележиме дека овој прстен е асоцијативен и има единица.

9.38. Ако V е векторски простор над полето P со $\dim V = n$, тогаш прстенот $L(V, V)$ е изоморфен со прстенот M_n од сите матрици со ред n над полето P.

Решение. Според 9.35. секоја линеарна трансформација на V е еднозначно определена ако се познати сликите на базните вектори.

Нека $e_1, e_2,\ldots, e_n$ е база на V и линеарната трансформација α на V нека е определена со: $\alpha(e_i)=e_i'$, $i=1,\ldots,n$. Претставувајќи го секој вектор e_i' како линеарна комбинација од базните вектори e_i, т.е. $e_i'=a_{1i}e_1+a_{2i}e_2+\ldots+a_{ni}e_n$, имаме:

$$\alpha(e_i)=e_i'=\sum_{k=1}^{n}a_{ki}e_k,\quad i=1,2,\ldots,n \tag{1}$$

Од равенството (1) можеме да ја формираме матрицата $[a_{ij}]$ со ред n. Значи, постои пресликување $f: L(V,V)\to M_n$, коешто е инјекција. Да покажеме дека f е сурјекција. Затоа, нека $A=[a_{ij}]$ е која било матрица со ред n. Да ги формираме векторите

$v_i=a_{1i}e_1+a_{2i}e_2+\ldots+a_{ni}e_n,\quad i=1,2,\ldots,n$.

Пресликувањето $\alpha: V\to V$, дефинирано со $\alpha(e_i)=v_i$, е линеарна трансформација и $f(\alpha)=A$. Според тоа, f е биекција.

Нека $\alpha,\beta\in L(V, V)$ и нека $f(\alpha)=[a_{ij}]$, $f(\beta)=[b_{ij}]$.

Тогаш имаме:

$$(\alpha+\beta)(e_j)=\sum_{k=1}^{n}(a_{kj}+b_{kj})e_k,$$

$$(\alpha\beta)(e_j)=\alpha(\beta(e_j))=\alpha\left(\sum_{k=1}^{n}b_{kj}e_k\right)=\sum_{k=1}^{n}\alpha(b_{kj}e_k)=$$

$$= \sum_{k=1}^{n} b_{kj}\alpha(e_k) = \sum_{k=1}^{n} b_{kj}\left(\sum_{i=1}^{n} a_{ik}e_i\right) = \sum_{k=1}^{n}\sum_{i=1}^{n}(b_{kj}a_{ik}e_i)$$

$$= \sum_{i=1}^{n}\left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)e_i, \quad \text{т.е}$$

$f(\alpha+\beta) = [a_{ij} + b_{ij}] = f(\alpha) + f(\beta)$ и

$$f(\alpha\beta) = \left[\sum_{k=1}^{n} a_{ik}\, b_{kj}\right] = [a_{ij}][b_{ij}] = f(\alpha)f(\beta)$$

Значи, f е изоморфизам.

9.39. Нека V е векторски простор над полето P, а S нека е потполе од P. Да се покаже дека V е векторски простор и над S. Каква врска постои меѓу димензиите на V над P и над S ?

Решение. Јасно е дека V е векторски простор и над S. Со V_P да го означиме векторскиот простор над P, а со V_S векторскиот простор над S. Нека $v_1, v_2,\ldots, v_n$ е база за V_P; да го разгледаме равенството

$$x_1 v_1 + \ldots + x_n v_n = 0, \qquad (1)$$

каде што $x_i \in S$. Бидејќи $x_i \in P$, а $v_1, \ldots, v_n$ е база за V_P, од (1) следува $x_i = 0$, $i = 1,\ldots, n$. Значи множеството $v_1,\ldots, v_n$ е линеарно независно во V_S, од каде што следува дека

$$\dim V_P \le \dim V_S . \qquad (2)$$

Дека во (2) не мора да важи равенството покажуваат следниве примери:

1) $\dim \mathbb{C}_{\mathbb{C}} = 1$, $\dim \mathbb{C}_{\mathbb{R}} = 2$; 2) $\dim \mathbb{R}_{\mathbb{R}} = 1$, $\dim \mathbb{R}_{\mathbb{Q}} = \infty$.

9.40. Нека V е векторски простор над P со димензија n. Да се покаже дека секој потпростор W од V има конечна димензија не поголема од n, а ако W е вистински потпростор од V, тогаш $\dim W < n$.

Решение. Ако W е нултиот простор, тогаш $\dim W = 0$, па значи $\dim W \le n$. Ако W содржи ненулти вектор w_1, тогаш можеме да формираме потпростор W_1 генериран од w_1. Ако $W_1 = W$, тогаш $\dim W = 1$. Ако пак $W_1 \neq W$, тогаш нека w_2 е елемент од W што не се содржи во W_1 и W_2 нека е потпросторот генериран од w_1 и w_2; итн. Бидејќи не можат да се најдат $n + 1$ линеарно независни вектори, овој процес ќе се заврши по n постапки. Според тоа, имаме $\dim W \le n$.

Нека W е вистински потпростор од V и нека $w_1,\ldots, w_m$ е база на W. Бидејќи W е вистински потпростор од V, постои $v \in V \setminus W$, па тогаш потпросторот генериран од $w_1,\ldots, w_m, v$ го содржи W и има

димензија $m+1$. Бидејќи пак тој е потпростор од V, имаме $m+1 \leq n$, т.е. $m < n$. Значи, $\dim W < n$.

9.41. Да се покаже дека резултатот од задачата 9.40 не важи за бесконечно димензионални векторски простори.

Решение. Векторскиот простор $\mathbb{R}$ над полето од рационалните броеви, $\mathbb{Q}$, има бесконечна димензија, а множеството A од сите алгебарски броеви е негов нетривијален потпростор, чија димензија е исто така, бесконечна. Значи, $\dim A \not< \dim \mathbb{R}$.

9.42. Ако V и V' се векторски простори над P со иста димензија n, тогаш тие се изоморфни.

Решение. Нека $v_1,\ldots, v_n$ е база на V, а $v_1',\ldots,v_n'$ е база на V'. Според 9.35. пресликувањето $f: V \to V'$, дефинирано со

$$f(v_i) = v_i', \quad i = 1,\ldots, n,$$

е линеарно. Да претпоставиме дека $f(u) = f(v)$, за некои $u, v \in V$.

Ако $u = x_1v_1 + \ldots + x_n v_n$, $v = y_1v_1 + \ldots + y_nv_n$, тогаш имаме

$$f(x_1v_1 + \ldots + x_nv_n) = f(y_1v_1 + \ldots + y_nv_n),$$

$$x_1v_1' + \ldots + x_nv_n' = y_1v_1' + \ldots + y_nv_n'$$

т.е. $x_i = y_i$, $i = 1,\ldots, n$. Значи, од $f(u) = f(v)$ следува $u = v$, т.е. f е инјекција. Потоа, нека v' е произволен елемент од V'; тогаш постојат скалари $x_1,\ldots, x_n \in P$, такви што $v' = x_1v_1' + \ldots + x_nv_n'$.

Векторот $v = x_1v_1 + \ldots + x_nv_n \in V$, а притоа имаме $f(v) = v'$, што значи дека f е сурјекција.

Од сето тоа следува дека f е изоморфизам, т.е. дека V и V' се изоморфни.

9.43. Подмножеството $B = \{b_i \mid i \in I\}$ е база на векторскиот простор V над полето P ако и само ако секој елемент $v \neq 0$ од V може на единствен начин да се претстави во вид

$$v = x_1b_{i_1} + \ldots + x_nb_{i_n} \tag{1}$$

каде што $b_{i_1},\ldots,b_{i_n} \in B$, а $x_1,\ldots, x_n$ се елементи од P различни од нула и $n \geq 1$.

Решение. Нека B е база на V. Од дефиницијата за база следува дека кој било елемент $v \in V$ може да се претстави во облик (1). Да покажеме дека тоа претставување е единствено.

Ако $v = y_1 b_{j_1} + \ldots + y_m b_{j_m}$ би било друго претставување на v, тогаш би имале

$$x_1 b_{i_1} + \ldots + x_n b_{i_n} + (-y_1) b_{j_1} + \ldots (-y_m) b_{j_m} = 0,$$

т.е. унијата на двата потсистема $b_{i_1}, \ldots, b_{i_n}$ и $b_{j_1}, \ldots, b_{j_m}$ од базата B би била зависен систем, што противречи на линеарната независност на базата B.

Обратно, нека секој $v \in V$ $(v \neq 0)$ се претставува на единствен начин во обликот (1). Треба да докажеме уште дека множеството B е линеарно независно, т.е. дека кој било конечен потсистем вектори од B е линеарно независен. Да претпоставиме дека постои конечен потсистем $b_1, b_2, \ldots, b_n$ вектори од B којшто е линеарно зависен. Тогаш некој од овие вектори, на пример b_1, може да се изрази како линеарна комбинација од преостанатите: $b_1 = x_2 b_2 + \ldots + x_n b_n$. (Притоа, можеме да сметаме дека $b_1 \neq 0$.) Меѓутоа, векторот b_1 може да се престави и во обликот:

$b_1 = 1 \cdot b_1 + 0 \cdot b_2 + \ldots + 0 \cdot b_n$,

т.е. векторот b_1 би имал две различни претставувања, спротивно на условот за единствено претставување. Од тоа следува дека B е линеарно независно, па значи B е база на V.

9.44. Подмножеството B е база на векторскиот простор V ако и само ако тоа е максимално линеарно независно подмножество од V.

9.45. Ако A и B се две бази на векторскиот простор V над полето P, тогаш A и B имаат ист кардинален број, $|A| = |B|$.

Решение. Во случајот кога некое од множествата A, B е конечно, резултатот следува лесно од дефиницијата за база.

Нека двете множества A, B се бесконечни и $|A| = \mathfrak{m}$, $|B| = \mathfrak{n}$.

Според 9.34. секој елемент a од базата A може да се изрази во вид

$$a = \sum_{b_i \in B} x_i b_i, \quad x_i \in P,$$

каде што само конечен број коефициенти x_i се различни од нула, т.е. елементот $a \in A$ може да се изрази со помош на конечен систем B_a од елементи од B. Да ја означиме со B' унијата на сите такви конечни системи B_a кога a се менува во целата база A, т.е.

$$B' = \bigcup_{a \in A} B_a.$$

Бидејќи секое од множествата B_a е конечно, а A има кардинален број $\mathfrak{m}$, кардиналниот број на B' ќе биде исто така $\mathfrak{m}$, па

значи B' е вистинско подмножество од A. Нека b е кој било елемент од $B \setminus B'$. Според 9.43. тој се изразува линеарно со помош на конечен систем елементи $a_1,\ldots, a_n \in A$, па значи и со помош на конечен систем $\bigcup_{i=1}^{n} B_{a_i}$ од множеството B', што е противречно на линеарната независност на базата B.

Според тоа, $\mathfrak{m} \not< \mathfrak{n}$, а од причини на симетрија $\mathfrak{n} \not< \mathfrak{m}$. Следствено $\mathfrak{m} = \mathfrak{n}$.

9.46. Да се покаже дека два векторски простора V и V' над исто поле P се изоморфни ако и само ако тие имаат иста димензија.

Решение. Нека $f: V \to V'$ е изоморфизам. Ако B е база на V, тогаш $f(B)$ е база на V' и $|B| = |f(B)|$, па $\dim V = \dim V'$.

Обратно, нека векторските простори V и V' имаат бази B и B' соодветно, такви што $|B| = |B'|$. Од тоа следува дека постои биекција g од B на B', $g(b) \in B'$ за секој $b \in B$. Ова пресликување можеме да го прошириме на целиот простор V на следниов начин: ако елементот $a \in A$ со помош на базата B се претставува во вид

$$a = \sum_{b_i \in B} x_i b_i,\ x_i \in P \quad \text{и само конечно многу } x_i \neq 0,$$

тогаш ставаме

$$g(a) = \sum_{b_i \in B} x_i g(b_i).$$

Пресликувањето g е биекција од V во V', а имајќи ја предвид задачата 9.43. добиваме дека g е изоморфизам.

9.47. Нека V е n–димензионален векторски простор, а A и B се потпростори од V, такви што $\dim A = k$, $\dim B = m$. Ако потпросторите $A \cap B$ и $A + B = \{a + b \mid a \in A, b \in B\}$ имаат димензии p и s соодветно, да се покаже дека тогаш

$$s = k + m - p.$$

§ 10. ПОДГРУПИ

10.1. Нека A, B и C се подмножества од групата G, и A има барем два елементa. Дали се точни равенствата

$A(B \cap C) = AB \cap AC$, $(B \cap C)A = BA \cap CA$?

Решение. Равенствата не мора да се точни. На пример, ако

$G = \mathbb{Z}(+), A = \{2, 3\}, B = \mathbb{Z} \setminus \{4\}, C = \mathbb{Z} \setminus \{5\}$, тогаш имаме:

$B \cap C = \mathbb{Z} \setminus \{4, 5\}$, $A + (B \cap C) = \mathbb{Z} \setminus \{7\}$, $(A + B) \cap (A + C) = \mathbb{Z}$.

10.2. Ако A, B, C, D се подмножества од групата G, тогаш

$A \subseteq B, C \subseteq D \Rightarrow AC \subseteq BD, A^{-1} \subseteq B^{-1}$.

10.3. Да се даде пример на непразно подмножество H од групата G со:

а) $H = H^{-1}$,

б) $HH = H$,

но сепак H да не е подгрупа.

Решение. а) Нека G е група и $a \neq e$ произволен елемент од G. Ако $H = \{a, a^{-1}\}$, тогаш имаме $H^{-1} = \{a^{-1}, a\} = H$, но H не е подгрупа од G.

б) Нека $G = \mathbb{Z}(+)$, а $H = \{0, 2, 4, 6, \ldots, 2n \ldots\}$; тогаш имаме $H + H = H$, но H не е подгрупа од $\mathbb{Z}(+)$.

10.4. Ако H е конечно непразно подмножество од групата G и ако $HH \subseteq H$, тогаш H е подгрупа од G.

Решение. Нека $a \in H$; од $HH \subseteq H$, следува $aH \subseteq H$, па значи $f : h \to ah$ е пресликување од H во H. Бидејќи G е група, f е инјекција, а бидејќи H е конечно подмножество од G, следува дека f е биекција. Значи, $aH = H$, па постои $h \in H$, таков што $ah = a = ae$, т.е. $h = e \in H$, а потоа од $e \in aH$ следува $a^{-1} \in H$.

Значи H е подгрупа.

10.5. Нека $\{H_i \mid i \in I\}$ е верига подгупи од групата G. Да се покаже дека $H = \bigcup_i H_i$ е исто така подгрупа од G.

Решение. Бидејќи фамилијата подгрупи $\{H_i \mid i \in I\}$ е верига, следува дека за кои било $i, j \in I$, $H_i \subseteq H_j$ или $H_j \subseteq H_i$.

Нека $x, y \in H$; тоа значи дека постојат $i, j \in I$, такви што $x \in H_i$, $y \in H_j$. Можеме да претпоставиме дека $H_j \subseteq H_i$, па добиваме дека $x, y \in H_i$. Бидејќи H_i е подгрупа од G, имаме $xy^{-1} \in H_i$, па и $xy^{-1} \in \bigcup_i H_i$

Значи, H е подгрупа од G.

Да забележиме дека во општ случај унија на подгрупи не е подгрупа.

10.6. Ако H и K се подгрупи од G и ако $KH \subseteq HK$, тогаш $KH = HK$ е подгрупа од G. Дали важи и обратното, т.е. дали од тоа што KH е подгрупа на G следува дека $KH = HK$?

Решение. Од $KH \subseteq HK$, според 10.2, имаме $(KH)^{-1} \subseteq (HK)^{-1}$, т.е.

$H^{-1}K^{-1} \subseteq K^{-1}H^{-1}$. Но, H и K се подгрупи на G, па $H^{-1} = H$ и $K^{-1} = K$.

Значи, имаме $HK \subseteq KH$, кое заедно со $KH \subseteq HK$, дава $KH = HK$. Бидејќи

$(KH)^{-1} = H^{-1}K^{-1} = HK = KH$,

добиваме дека KH е подгрупа на G.

Да претпоставиме сега дека KH е подгрупа на G. Од $H, K \subseteq KH$, следува $HK \subseteq KH$, а потоа и $(HK)^{-1} \subseteq (KH)^{-1}$, т.е. $KH \subseteq HK$. Значи, ако H, K и KH се подгрупи од G, тогаш $KH = HK$.

10.7. Да се даде пример на група со својството: секоја *нетривијална* подгрупа H од G, да е изоморфна со G.

Решение. $\mathbb{Z}(+)$. Навистина, секоја подгрупа P од $\mathbb{Z}(+)$ е од обликот

$P_a = \{ax \mid x \in \mathbb{Z}\}$, $a \in \mathbb{N}$,

и, притоа пресликувањето $f: \mathbb{Z} \to P_a$, дефинирано со

$(\forall x \in \mathbb{Z})\ f(x) = ax$,

е изоморфизам.

10.8. Да се најдат сите подгрупи од диедралната група D_4 (в.6.5.).

Решение. Од шемата на D_4 дадена подолу, заклучуваме дека подгрупи се:

$E = \{a_0\}$, $H_1 = \{a_0, a_2\}$, $H_2 = \{a_0, b_0\}$, $H_3 = \{a_0, b_1\}$,

$H_4 = \{a_0, b_2\}$, $H_5 = \{a_0, b_3\}$, $H_6 = \{a_0, a_1, a_2, a_3\}$,

$H_7 = \{a_0, a_2, b_0, b_2\}$, $H_8 = \{a_0, a_2, b_1, b_3\}$, G.

Шемата на D_4 е:

$*$	a_0	a_1	a_2	a_3	b_0	b_1	b_2	b_3
a_0	a_0	a_1	a_2	a_3	b_0	b_1	b_2	b_3
a_1	a_1	a_2	a_3	a_0	b_1	b_2	b_3	b_0
a_2	a_2	a_3	a_0	a_1	b_2	b_3	b_0	b_1
a_3	a_3	a_0	a_1	a_2	b_3	b_0	b_1	b_2
b_0	b_0	b_3	b_2	b_1	a_0	a_3	a_2	a_1
b_1	b_1	b_0	b_3	b_2	a_1	a_0	a_3	a_2
b_2	b_2	b_1	b_0	b_3	a_2	a_1	a_0	a_3
b_3	b_3	b_2	b_1	b_0	a_3	a_2	a_1	a_0

10.9. Во множеството $D = \{a_m \mid m\in\mathbb{Z}\} \cup \{b_m \mid m\in\mathbb{Z}\}$ е определена е операција "$*$" со:

$a_i * a_j = a_{i+j}$, $a_i * b_j = b_{i+j}$, $b_i * b_j = a_{i-j}$, $b_i * a_j = b_{i-j}$

Да се покаже дека $D(*)$ е група и да се најдат сите подгрупи на D.

Решение. Дека $D(*)$ е група, лесно се покажува. Да споменеме само дека единица во $D(*)$ е елементот a_0, инверзен на a_i е a_{-i}, а инверзен на b_i е b_i.

Да ги најдеме подгрупите на $D(*)$. Јасно е дека $E = \{a_0\}$ и $H_i = \{a_0, b_i\}$, $i\in\mathbb{Z}$, се подгрупи. Пресликувањето $f: \mathbb{Z} \to D$, дефинирано со: $(\forall i\in\mathbb{Z})$ $f(i) = a_i$, е мономорфизам, па значи подмножеството

$K_1 = f(\mathbb{Z}) = \{a_m \mid m\in\mathbb{Z}\}$

е подгрупа од $D(*)$. Бидејќи секоја подгрупа од $\mathbb{Z}$ е од облик $\{ni \mid i\in\mathbb{Z}\}$, $n\in\mathbb{N}$, заклучуваме дека секое подмножество

$K_n = \{a_{ni} \mid i\in\mathbb{Z}\}$, $n\in\mathbb{N}$,

е подгрупа од D. Други подгрупи од D што содржат само елементи од облик a_i не постојат.

Бидејќи $b_i * b_j = a_{i-j}$, следува дека не постои подгрупа од D што содржи само a_0 и елементи со облик b_i, а да е различна од H_i. Значи, ако постои подгрупа L што содржи елементи со облик b_i, тогаш таа мора да содржи подгрупа со облик K_n. Затоа, нека L е подгрупа од D, за која K_n, n – фиксен природен број, е нејзина подгрупа. Ако b_i и b_j се два различни елементи од L, тогаш имаме $b_i * b_j = a_{i-j} \in K_n$, од каде што следува $i - j = nk$ за некој $k\in Z$, т.е. $i \equiv j \pmod{n}$. Значи, имаме

$i = nk_1 + s$ и $j = nk_2 + s$, каде што $s = 0, 1, 2, \ldots, n-1$.
Од ова следува дека секое подмножество
$L_{n,s} = K_n \cup \{b_{ni+s} \mid i \in \mathbb{Z}\}$, $n \in \mathbb{N}$, $s = 0, 1, 2, \ldots, n-1$
е подгрупа од D. Со тоа се најдени сите подгрупи на D.

10.10. Да се најдат десните комплекси на S_3 во однос на подгрупата $\{1, \sigma_3\}$ (види 5.36.).

Одговор. $\{1, \sigma_3\}$, $\{\sigma_1, \rho_1\}$, $\{\sigma_2, \rho_2\}$.

10.11. Да се најдат десните и левите комплекси на кватернионската група K (види 6.6) во однос на подгрупата $H = \{1, -1\}$.

Одговор. $\{1,-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$. Левите и десните комплекси се совпаѓаат.

10.12. Ако K е десен (лев) комплекс на подгрупата H во групата G, тогаш
$x, y, z \in K \Rightarrow xy^{-1}z \in K$.

10.13. Нека K е непразно подмножество од групата G, коешто го задоволува условот
$x, y, z \in K \Rightarrow xy^{-1}z \in K$. (1)
Да се покаже дека постои единствена подгрупа H од G, така што K е десен комплекс на H.

Решение. Да го разгледаме подмножеството H од G, дефинирано со
$H = \{ab^{-1} \mid a, b \in K\}$. (2)
Бидејќи $(a_1b_1^{-1})(a_2b_2^{-1})^{-1} = (a_1b_1^{-1}b_2)a_2^{-1}$, а според (1) $a_1b_1^{-1}b_2 \in K$, добиваме $(a_1b_1^{-1})(a_2b_2^{-1})^{-1} \in H$, т.е. H е подгрупа од G. Од (2) следува $K = Hb$, $b \in K$, па значи K е десен комплекс на H.

Според тоа, постои барем една подгрупа H од G, така што K е десен комплекс на H во G. Нека L е друга таква подгрупа. Бидејќи
$a \in Lb \Leftrightarrow ab^{-1} \in L$,
заклучуваме дека $L = H$, т.е. подгрупата H е единствена.

10.14. Нека S е непразно подмножество од групата G и нека
$x \alpha y \Leftrightarrow x^{-1}y \in S$. (1)
Да се покаже дека α е еквивалентност ако и само ако S е подгрупа од G и дека тогаш класите на еквивалентноста α се совпаѓаат со левите комплекси на S во G.

Решение. Нека S е подгрупа од G и релацијата α нека е дефинирана со (1). За кој било $x\in G$ имаме $x^{-1}x = e\in S$, а тоа значи дека $x\alpha x$. Ако $x\alpha y$, тогаш $x^{-1}y\in S$, но и $y^{-1}x = (x^{-1}y)^{-1}\in S$, т.е. имаме $y\alpha x$. Нека $x\alpha y$ и $y\alpha z$; тогаш $x^{-1}y$, $y^{-1}z\in S$, па и $x^{-1}z = (x^{-1}y)(y^{-1}z)\in S$, т.е. $x\alpha z$. Од сето тоа следува дека α е еквивалентност во G.

Обратно, нека S е непразно подмножество од G и релацијата α, дефинирана со (1), е еквивалентност во G. За кој било $x\in G$ имаме $x\alpha x$, па $e = x^{-1}x\in S$, Ако x, $e\in S$, тогаш $x\alpha e$, па $x^{-1} = x^{-1}e\in S$. Нека x, $y\in S$, тогаш и $x^{-1}\in S$, па од x^{-1}, $y\in S$ следува $xy\in S$, т.е. S е подгрупа од G. Потоа, имаме:

$$x^{\alpha} = \{y \mid x\,\alpha\, y\} = \{y \mid x^{-1}y \in S\} = \{y \mid y \in xS\} = xS,$$

т.е. класите на еквивалентноста α се совпаѓаат со левите комплекси на S.

10.15. Ако K и H се подгрупи од групата G, при што $H \subseteq K$, тогаш

$$(G : H) = (G : K)(K : H). \tag{1}$$

Решение. Нека $\{x_iK \mid i\in I\}$ е множеството леви комплекси на K во G, а $\{y_jH \mid j\in J\}$ е множеството леви комплекси на H во K. Тогаш имаме

$$G = \bigcup_i x_iK, \qquad K = \bigcup_j y_jH,$$

од каде што добиваме

$$G = \bigcup_{i,j} x_iy_jH. \tag{2}$$

За да го докажеме равенството (1), доволно е да покажеме дека (2) е дисјунктна унија. Ако претпоставиме дека

$x_{i_1}y_{j_1}H = x_{i_2}y_{j_2}H$, тогаш множејќи оддесно со K, добиваме

$x_{i_1}y_{j_1}HK = x_{i_2}y_{j_2}HK$. Но, H е подмножество од K, па $HK = K$. Затоа имаме $x_{i_1}y_{j_1}K = x_{i_2}y_{j_2}K$, т.е. $x_{i_1}K = x_{i_2}K$, зашто $y_j\in K$, но ова не е можно, зашто $x_{i_1}K \cap x_{i_2}K = \varnothing$. Значи, (2) е дисјунктна унија, па важи (1).

10.16. Во мултипликативната група од сите несингуларни матрици од втор ред над $\mathbb{C}$ да се најде редот на следниве елементи :

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} -2+3i & -2+2i \\ 1-i & 3-2i \end{bmatrix}.$$

Решение. 2; ∞; 4; ∞; ∞.

10.17. Во мултипликативната група на сите комплексни броеви, различни од нулата, да се најдат:

а) $[\,i\,]$; б) $\left[-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right]$; в) $\left[\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right]$; г) $\left[-\frac{1}{2}i\right]$;

д) $[\{2,-3\}]$.

Решение. а) $\{\,1,-1,i,-i\,\}$. б) $\left\{\;1,\ -\frac{1}{2}+\frac{\sqrt{3}}{2}i,-\frac{1}{2}-\frac{\sqrt{3}}{2}i\;\right\}$.

в) $\left\{1,-\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i,-\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i,\frac{\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i,\frac{\sqrt{2}}{2}+\frac{2}{2}i,i,-i,-1\;\right\}$.

г) $\left\{2^{4k},2^{4k+1}i,-2^{4k+2},-2^{4k+3}i\,\middle|\,k\in\mathbb{Z}\;\right\}$.

д) $\{(-1)^s 2^r 3^s \,|\, r,s\in\mathbb{Z}\;\}$.

10.18. Да се даде пример на група G и елементи $a,b\in G$ со конечни редови, а нивниот производ ab да има бесконечен ред.

Ако a и b се со конечни редови и $ab = ba$, тогаш редот на ab е конечен. Во овој случај, каков однос постои меѓу редовите на a, b и ab?

Решение. Нека G е групата D од 10.9. елементите b_2 и b_1 имаат ред 2, но $b_2 * b_1 = a_1$ има бесконечен ред.

Нека a има ред m, а b – ред n. Ако $ab = ba$, тогаш имаме:

$(ab)^{mn} = a^{mn}b^{mn} = e^n e^m = e$,

што значи дека редот на ab е исто така конечен. Ако s е најмалиот заеднички содржател на m и n, тогаш $(ab)^s = e$, па значи редот k на ab е делител на s. Ќе дадеме неколку примери дека редот на ab може да биде : 1, s или $k \mid s, k \neq 1, s$.

Ако $b = a^{-1}$, тогаш редот на ab е 1.

Ако $G = \{e, a, a^2, a^3, a^4, a^5\}$ е цикличната група со ред 6, тогаш, елементот a^2 има ред 3, елементот a^3 има ред 2, но елементот $a^2a^3 = a^5$ има ред 6. Во истата група, имаме $a^5a^3 = a^2$, чијшто ред е 3, различен од 1 и 6.

10.19. Да се покаже дека групата $\mathbb{Q}(+)$ не е циклична.

Решение. Кога $\mathbb{Q}(+)$ би била циклична, би постоел рационален број $q = \frac{m}{n}$, таков што $\left[\frac{m}{n}\right] = \mathbb{Q}(+)$. Тогаш, на пример, за рационал-

ниот број $\frac{1}{2n}$ би имале $\frac{1}{2n} = r\frac{m}{n}$, $r \in \mathbb{Z}$, од каде што се добива $2mr = 1$, а оваа равенка нема решение по r во целите броеви. Значи $\frac{1}{2n} \notin \left[\frac{m}{n}\right]$, од каде што заклучуваме дека $\mathbb{Q}(+)$ не е циклична.

10.20. Ако G е конечна циклична група со ред n и $(r, n) = 1$, тогаш
$a^r = b^r \Rightarrow a = b.$ (1)
Дали (1) е точно во случај да е $(r,n) \neq 1$?

Решение. Бидејќи G е комутативна, имаме
$(ab^{-1})^r = a^r (b^{-1})^r = a^r (b^r)^{-1} = a^r (a^r)^{-1} = e.$

Ако $G = [x]$, тогаш постои некој s, таков што $ab^{-1} = x^s$, и притоа имаме $(x^s)^r = e$. Значи, $n \mid rs$, а бидејќи $(n, r) = 1$, следува $n \mid s$, т.е. $s = nq$. Според ова имаме
$ab^{-1} = x^s = x^{nq} = e$, т.е. $a = b$.

Ако $(n,r) = d \neq 1$, тогаш од $a^r = b^r$ не мора да следува $a = b$. На пример, ако $G = \mathbb{Z}_6(+)$, тогаш имаме $3 \cdot 2 = 0$ и $3 \cdot 4 = 0$, но $2 \neq 4$.

10.21. Нека $G = [a]$ е циклична група со ред n и генератор a.
Да се покаже дека :
а) a^k е генератор на $G \Leftrightarrow (k,n) = 1$.
б) за секој делител d на n постои една и само една подгрупа на G со ред d.

Решение. а) Нека $(k, n) = 1$ и
$[a^k] = \{e, a^k, a^{2k}, \ldots, a^{(r-1)k}\}$,
каде што r е најмалиот природен број со својството $a^{rk} = e$. Од e следува $n \mid rk$, а бидејќи е $(k,n) = 1$, добиваме $n \mid r$. Значи, во $[a^k]$ постојат барем n различни елементи. Бидејќи $[a^k] \subseteq G$, а G има n елементи, следува дека $[a^k] = G$.

б) Нека d_i, $i = 1, 2, \ldots, s$, се сите различни делители на n. Ставајќи $H_i = \left[a^{d_i}\right]$, $i = 1,\ldots, s$, добиваме s подгрупи од G. Бидејќи $d_i \neq d_j$ за $i \neq j$, имаме $H_i \neq H_j$. Значи за секој делител d_i на n, постои подгрупа од G со ред d_i. Да покжеме дека нема други подгрупи во G освен подгрупите $H_1, \ldots, H_s$. Навистина, нека H е која било подгрупа од G, а d најмалиот број, таков што $a^d \in H$. Тогаш $H = [a^d]$ и $d \mid n$. Значи, $d = d_i$, за некој $i = 1, \ldots, s$, па $H = H_i$.

10.22. Нека G е циклична група со ред 15. Да се определат оние елементи $x \in G$, такви што $[x] = G$. Колку подгрупи има G?

Решение. Според 10.21, ако $x = a^i$ ја генерира G, тогаш мора да биде $(i,15) = 1$, па бараните елементи x се: a, a^2, a^4, a^7, a^8, a^{11}, a^{13}, a^{14}. Во G постојат само две вистински подгрупи и тоа $[a^3]$, која е со ред 5 и $[a^5]$, која е со ред 3.

10.23. Дали со некоја од приложените шеми е определена група?

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	e	d	c
b	b	c	a	b	e
c	c	d	c	e	a
d	d	e	d	a	b

	e	a	b	c	d	u	v
e	e	a	b	c	d	u	v
a	a	e	c	d	u	v	b
b	b	c	d	u	v	e	a
c	c	d	u	v	b	a	e
d	d	u	v	a	e	b	c
u	u	v	e	b	a	c	d
v	v	b	a	e	c	d	u

Решение. Не. Имено, секоја група со прост ред е циклична, а секоја циклична група е комутативна. Дадените групоиди имаат пет, односно седум елементи и се некомутативни.

10.24. Најмалиот природен број m со својството $(\forall x \in G)\ x^m = e$ се вика *експонент* на групата G.

а) Да се покаже дека експонентот на секоја конечна група е делител на редот на групата.

б) Да се даде пример на периодична група што нема конечен експонент.

Решение. а) Нека G има конечен ред n. Секоја конечна група има експонент, кој е најмал заеднички содржател од редовите на елементите од G. Ако r_i е редот на елементот $a_i \in G$, тогаш r_i е фактор во n, па и $m = [r_i, \ldots, r_n]$ е фактор во n. Да забележиме дека, ако G е циклична група со ред n, тогаш експонентот m е еднаков со n.

б) Таква група е, на пример, групата

$G = \{z \mid z \in \mathbb{C},\ (\exists n \in \mathbb{N})\ z^n = 1\}$,

во однос на операцијата множење на комплексни броеви.

10.25. Ако G е некомутативна група, дали може периодичниот дел $T(G)$ да не биде подгрупа?

Решение. Може. На пример, ако G е групата D од 10.9, тогаш
$T(G) = \{a_0\} \cup \{b_i \mid i \in \mathbb{Z}\}$ што не е подгрупа.

10.26. Да се дадат примери на бесконечни периодични групи и тоа, барем една комутативна и барем една некомутативна.

Решение. Бесконечна периодична група е, на пример, групата G од задачата 10.24, б).

Нека G е некомутативна група со конечен ред m. Таква група е, на пример, групата S_3, $m = 6$. Ако

$H = G^{\mathbb{N}} = \{(a_1, a_2, \dots, a_n, \dots) \mid a_n \in G,\ n \in \mathbb{N}\}$

е групата од сите бесконечни низи, при што

$(a_1, \dots, a_n, \dots)(b_1, \dots, b_n, \dots) = (a_1 b_1, \dots, a_n b_n, \dots)$

тогаш H е бесконечна и некомутативна. Притоа имаме

$(a_1, \dots, a_n, \dots)^m = (a_1^m, \dots, a_n^m, \dots) = (e, \dots, e, \dots)$

т.е. H е периодична.

10.27. Нека G е конечна група. Да се покаже дека бројот на елементите во множеството $A = \{x \mid x \in G, x^{-1} \neq x\}$ е парен.

Решение. Ако $x \in A$, т.е. $x^{-1} \neq x$, тогаш и $(x^{-1})^{-1} = x \neq x^{-1}$, т.е. $x^{-1} \in A$, од каде што и следува дека во A има парен број елементи.

Да споменеме дека може да се случи A да биде и празно.

10.28. Ако G е група со ред $2n$, тогаш постои барем еден елемент $b \in G$, таков што $b \neq e$ и $b^2 = e$.

Решение. Според претходната задача, бројот на елементите во G, со својството $x \neq x^{-1}$, е парен. Но, имаме $e = e^{-1}$, па бидејќи редот на G е $2n$, мора да постои барем уште еден елемент $b \in G$, $b \neq e$, $b^2 = e$. Да споменеме дека бројот на такви елементи во G е непарен.

10.29. Нека G е група со ред $2n$. Ако во G постојат точно n елементи со ред 2, тогаш множеството

$A = \{x \mid x \in G, x$ нема ред $2\}$

е комутативна подгрупа од G.

Решение. Според 10.28, следува дека n е непарен број. Нека

$B = \{b_1, b_2, \dots, b_n\}$

е множеството од сите елементи со ред 2, а

$A = \{a_1, a_2, \ldots, a_n\}$

е множеството од сите елементи во G, коишто не се со ред 2.

Да ги разгледаме елементите $b_i\, b_j$. Ако $b_i\, b_j \in B$, тогаш $b_i\, b_j = b_k$, па

$$b_i\, b_j = b_k = b_k^{-1} = (b_i\, b_j)^{-1} = b_j^{-1} b_i^{-1} = b_j b_i\,.$$

Но, условот $b_i\, b_j = b_j\, b_i$, повлекува дека множеството $\{1, b_i, b_j, b_i\, b_j\}$ е подгрупа од G со ред 4, па $4 \mid 2n$. Меѓутоа, n е непарен број, па $4 \nmid 2n$, т.е.

$(\forall b_i, b_j \in B) b_i\, b_j \notin B$.

Значи, $b_i\, b_j \in A$ за кои било $b_i, b_j \in B$, па $b_i b_j = a_k$. Можеме да претпоставиме дека елементите во A се така подредени што е $b_1 b_i = a_i$. Притоа имаме $a_i^{-1} = b_i b_1$. Нека $a_r, a_s \in A$; тогаш $a_r = b_1\, b_r$, $a_s = b_1\, b_s$, па имаме $a_r\, a_s = (b_1\, b_r)\,(b_1\, b_s) = (b_1 b_r b_1) b_s$. Но,

$(b_1\, b_r b_1)^2 = (b_1\, b_r b_1)\,(b_1\, b_r b_1) = e$,

па $b_1 b_r b_1 \in B$. Бидејќи и $b_s \in B$, следува дека $a_r\, a_s = b_1\, b_r\, b_1\, b_s \notin$ B, т.е. $a_r\, a_s \in A$. Од сето тоа следува дека A е подгрупа од G. Од $a_r\, a_s = a_k$, добиваме

$b_1\, b_r b_1\, b_s = b_1\, b_k$, т.е.

$b_r\, b_1\, b_s = b_k = b_k^{-1} = b_s b_1\, b_r$,

а од ова следува $a_r\, a_s = a_s\, a_r$, т.е. подгрупата A е комутативна.

10.30. Да се најде кои од матриците

$$A = \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}, \quad C = \begin{bmatrix} 2 & 1 \\ -2 & 0 \end{bmatrix},$$

се конјугирани меѓу себе во мултипликативната група од сите несингуларни матрици од втор ред.

Решение. За да провериме дали A и B се конјугирани, треба да видиме дали равенката

$$X^{-1} AX = B \tag{1}$$

има решение по X.

Ако $X = \begin{bmatrix} x & y \\ u & v \end{bmatrix}$, тогаш од (1) добиваме $x = y = u = v = 0$, а тоа значи дека A и B не се конјугирани.

За A и C равенката $X^{-1} AX = C$ се сведува на системот

$x - 2y - u = 0, \quad x - y - v = 0, \quad x + u - 2v = 0, \quad y + u - v = 0,$

којшто има нетривијални решенија.

Едно такво решение е $x = u = v = 1$, $y = 0$ и имаме

$$\det X = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix} = 1 \neq 0.$$

Според тоа, матриците A и C се конјугирани.

Матриците B и C не се конјугирани, зашто ако би биле, тогаш би морале да бидат конјугирани A и B.

10.31. Да се најдат класите на конјугирани елементи во S_3.

Решение. Елементите на S_3 се 1, ρ_1, ρ_2, σ_1, σ_2, σ_3, (в.5.36.), каде што $\sigma_i^2 = 1$ и $\rho_1^{-1} = \rho_2$. Бидејќи за секој $x \in S_3$ важи равенството $x^{-1}1x = 1$, една од класите конјугирани елементи е $K_1 = \{1\}$. Да ги најдеме елементите конјугирани со ρ_1. Имаме

$\rho_i^{-1}\rho_1\rho_i = \rho_1, \quad i = 1,2,$

$\sigma_1^{-1}\rho_1\sigma_1 = \sigma_1\rho_1\sigma_1 = \sigma_2\sigma_1 = \rho_2$

$\sigma_2^{-1}\rho_1\sigma_2 = \sigma_2\rho_1\sigma_2 = \sigma_3\sigma_2 = \rho_2,$

$\sigma_3^{-1}\rho_1\sigma_3 = \sigma_3\rho_1\sigma_3 = \sigma_1\sigma_3 = \rho_2.$

Значи, имаме $K_2 = \{\rho_1, \rho_2\}$. Слично добиваме и $K_3 = \{\sigma_1, \sigma_2, \sigma_3\}$.

10.32. Да се најдат класите на конјугирани елементи на кватернионската група K (види 6.6.).

Решение. $\{1\}$, $\{-1\}$, $\{i, -i\}$, $\{j, -j\}$, $\{k, -k\}$.

10.33. Во диедралната група D_4 (види 10.8) да се најдат:

а) класите на конјугирани елементи.

б) класите на конјугирани подгрупи.

Решение. а) $\{a_0\}$, $\{a_2\}$, $\{a_1, a_3\}$, $\{b_0, b_2\}$, $\{b_1, b_3\}$.

б) Во 10.8 се најдени подгрупите на D_4. Класите на конјугирани подгрупи се: $\{E\}$, $\{H_1\}$, $\{H_2, H_4\}$, $\{H_3, H_5\}$, $\{H_6\}$, $\{H_7\}$, $\{H_8\}$ и $\{G\}$.

10.34. Во групата D од задачата 10.9 да се најдат:

а) класите од конјугирани елементи.

б) клажсите од конјугирани подгрупи.

Решение. а) Една класа конјугирани елементи е $\{a_0\}$. Бидејќи

$b_i * a_n * b_i = a_{-n}$, а $a_i * a_n * a_{-i} = a_n$, за секој $i \in \mathbb{Z}$, други класи на конјугирани елементи се подмножествата $\{a_n, a_{-n} \mid n \in \mathbb{N}\}$. Слично добиваме дека останатите класи конјугирани елементи се подмножествата $\{b_{2k+1} \mid k \in \mathbb{Z}\}$.

б) $\{E\}$, $\{H_{2k} \mid k \in \mathbb{Z}\}$, $\{H_{2k+1} \mid k \in \mathbb{Z}\}$, $\{K_n\}$, $n \in \mathbb{N}$,

$\{L_{n,s}\}$, $n \in \mathbb{N}$, $s = 0, 1, \ldots, n-1$.

10.35. Ако елементите a и b од групата G се конјугирани, тогаш тие имаат исти редови.

10.36. Да се покаже дека елементите ab и ba имаат ист ред.

Решение. Бидејќи $a^{-1}(ab)a = ba$, следува дека ab и ba се којугирани, па, според претходната задача, тие имаат исти редови.

10.37. Да се најдат сите конечни групи, коишто имаат само две класи конјугирани елементи.

Решение. Нека G е конечна група со ред n, и нека K_1, K_2 се класите конјугирани елементи во G, т.е. $G = K_1 \cup K_2$. Бидејќи за секое $x \in G$ важи равенството $x^{-1}ex = e$, едната класа е $K_1 = \{e\}$, а другата $K_2 = G \setminus \{e\}$. Но, бројот на елементите во K_2 е $n - 1$, а од $(n-1) \mid n$ и $(n-1, n) = 1$, следува $n - 1 = 1$, т.е. $n = 2$. Значи, единствената група G што има само две класи конјугирани елементи е групата со два елемента.

10.38. Во групата на сите реални несингуларни матрици од втор ред да се најде нормализаторот на секој од следниве елементи:

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}, \quad B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Решение. Да го најдеме нормализаторот $N(A)$. Според дефиницијата, имаме

$$N(A) = \{X \mid X = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \ \det X \neq 0, \ X^{-1}AX = A\}.$$

Бидејќи $X^{-1} = \dfrac{1}{\det X}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$,

имаме : $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} \det X & 0 \\ 0 & 2\det X \end{bmatrix}$, т.е.

$$\begin{bmatrix} ad - 2bc & -bd \\ ac & 2ad - bc \end{bmatrix} = \begin{bmatrix} ad - bc & 0 \\ 0 & 2(ad - bc) \end{bmatrix},$$

од каде што добиваме $b = c = 0, \quad a \neq 0, \quad d \neq 0$. Значи :

$$N(A) = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \mid a \neq 0,\ d \neq 0 \right\}.$$

Слично добиваме :

$$N(B) = G, \qquad N(C) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \middle| \ a \neq 0 \right\}$$

10.39. Во групата $G = \mathbb{Z} \times \mathbb{Z}$, каде што операцијата е определена како во 6. 3, т.е. со:

$(a, b) \circ (c, d) = (a + c, (-1)^c b + d)$,

да се најде:

а) $N(x)$ за секој $x \in G$.

б) Бројот на елементите конјугирани со $x \in G$.

Решение. а) Нека $x = (m, n) \in G$. Ако $y = (a, b)$, тогаш $y^{-1} = (-a, (-1)^{a+1} b)$ па равенката $y^{-1} \circ x \circ y = x$ се сведува на

$(m, ((-1)^{m+1} + 1)\, b + (-1)^a n) = (m, n)$,

од каде што добиваме

$$((-1)^{m+1} + 1)b + (-1)^a n = n. \tag{1}$$

Ако $m = 2k + 1$, тогаш (1) се сведува на $2b + (-1)^a n = n$, од каде што добиваме $b = 0$ за $a = 2z$, и $b = n$ за $a = 2z + 1$. Ако пак $m = 2k$, тогаш (1) се сведува на $(-1)^a n = n$, од каде што добиваме

$a = 2z$ за $n \neq 0$, и $a = z$ за $n = 0$. Според тоа имаме :

$$N((2k + 1, n)) = \{(2z, 0) \mid z \in \mathbb{Z}\} \cup \{(2z + 1, n) \mid z \in \mathbb{Z}\}, \tag{2}$$

$$N((2k, 0)) = \{(2z, b) \mid z, b \in \mathbb{Z}\}, \tag{3}$$

$$N((2k, n), n \neq 0) = \{(z, b) \mid z, b \in \mathbb{Z}\} = G. \tag{4}$$

б) За да го најдеме бројот на елементите, конјугирани со $x \in G$, треба да го најдеме индексот на $N(x)$ во G.

Ако $x = (2k + 1, n)$, тогаш нормализаторот $N(x)$ е даден со (2). За секој $(2z + 1, n) \in N(x)$ и $(2u, a) \notin N(x)$ имаме:

$(2z + 1, n) \circ (2u, a) = (2(z + u) + 1, n + a) = (2(z + u) + 1, n) \circ (0, a)$ т.е.

$N(x) \circ (2u, a) = N(x) \circ (0, a)$.

Значи, $N(x) \setminus G \supseteq \{N(x) \circ (0, a) \mid a \in \mathbb{Z},\ a \neq 0\}$, а бидејќи множеството $\{N(x) \circ (0, a) \mid a \in \mathbb{Z},\ a \neq 0\}$ е бесконечно, следува дека индексот на $N(x)$ е бесконечен, па и бројот на елементите конјугирани со $x = (2k+1, n)$ е бесконечен. Ако $x = (2k, n)$, $n \neq 0$, тогаш $N(x)$ е даден со (3) и притоа имаме:

$N(x) \setminus G = \{N(x), N(x) \circ (1, 1)\}$,

т.е. индексот на $N(x)$ е 2, па и бројот на елементите конјугирани со $x = (2k, n)$, $n \neq 0$, е 2.

Ако пак $x = (2k, 0)$, тогаш $N(x) = G$, т.е. индексот на $N(x)$ е 1, па секој елемент $x = (2k, 0)$ е конјугиран само со себе.

10.40. Ако N е нормализатор на елементот a од групата G, тогаш $(\forall g \in G)\ \ N(g^{-1}ag) = g^{-1}Ng$.

Решение. Нека $x \in N(g^{-1}ag)$; тоа значи дека $x^{-1}(g^{-1}ag)x = g^{-1}ag$, а тоа е еквивалентно со $(gxg^{-1})^{-1}a(gxg^{-1}) = a$, т.е.

$x \in N(g^{-1}ag) \Leftrightarrow gxg^{-1} \in N \Leftrightarrow x \in g^{-1}Ng$.

Значи, имаме $N(g^{-1}ag) = g^{-1}Ng$.

10.41. Да се најде центарот на диедралната група D_4.

Решение. Од шемата на D_4 (10.8), се гледа дека центарот е $C(D_4) = \{a_0, a_2\}$.

10.42. Да се најде центарот $C(D)$ на групата D од 10.9.

Решение. $C(D) = \{a_0\}$.

10.43. Нека $\mathbb{K}$ е множеството од сите кватерниони, т.е.

$\mathbb{K} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}^*\}$,

и нека во $\mathbb{K}$ е дефинирано множење со:

$$(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) =$$
$$= (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_1 b_2 + a_2 b_1 + c_1 d_2 - c_2 d_1)i +$$
$$+ (a_1 c_2 + a_2 c_1 + d_1 b_2 - d_2 b_1)j + (a_1 d_2 + a_2 d_1 + b_1 c_2 - b_2 c_1)k$$

Да се покаже дека $\mathbb{K}(\cdot)$ е група, а потоа да се покаже дека $C(\mathbb{K}) = \mathbb{R}^*$.

Решение. Дека $\mathbb{K}(\cdot)$ е група, лесно се покажува.

Да споменеме дека групата $\mathbb{K}(\cdot)$ е некомутативна. На пример, $ij = k \neq -k = ji$.

Да го најдеме центарот $C(\mathbb{K})$. Јасно е дека секој реален број $a \neq 0$ му припаѓа на центарот $C(\mathbb{K})$. Да видиме дали има и други. Нека елементот $a + bi + cj + dk \in C(\mathbb{K})$. Тоа значи дека

$$(a + bi + cj + dk)(x + yi + zj + uk) = (x + yi + zj + uk)(a + bi + cj + dk),$$

за кои било $x, y, z, u \in \mathbb{R}^*$. Ова равенство е еквивалентно со равенките

$$dz - cu = 0, \qquad bu - dy = 0, \qquad bz - cy = 0,$$

коишто треба да бидат задоволени за кои било $y, z, u \in \mathbb{R}^*$, па значи имаме $b = c = d = 0$. Според тоа:

$a + bi + cj + dk \in C(\mathbb{K}) \Leftrightarrow a \in \mathbb{R}^*, \quad b = c = d = 0$,

т.е. $C(\mathbb{K}) = \mathbb{R}^*$.

§11. ГРУПИ ОД ПЕРМУТАЦИИ

11.1. Да се најдат циклусите на пермутацијата $\alpha : \mathbb{R} \to \mathbb{R}$ определена со $(\forall x \in \mathbb{R})\ \alpha(x) = x^3$.

Решение. Бидејќи $\alpha(-1) = -1$, $\alpha(0) = 0$, $\alpha(1) = 1$, и $\alpha(a) \neq a$ за секој друг реален број a, циклусите на α се:

$(-1), (0), (1), (\ldots, \sqrt[9]{a}, \sqrt[3]{a}, a, a^3, a^9, \ldots), a \neq -1, 0, 1.$

11.2. Нека $\alpha, \beta, \gamma : \mathbb{Z} \to \mathbb{Z}$ се дефинирани на следниот начи $(\forall z \in \mathbb{Z})\ \alpha(z) = z + 1$,

$$\beta(z) = \begin{cases} z, & z = 2k \\ z+2, & z = 2k+1, \end{cases} \qquad \gamma(z) = \begin{cases} z+2, & z = 2k \\ z, & z = 2k+1 \end{cases}$$

Да се покаже дека $\alpha, \beta, \gamma \in S_{\mathbb{Z}}$ и дека $\alpha\alpha = \beta\gamma = \gamma\beta$.

11.3. Да се даде пример на пермутација со бесконечно многу нетривијални циклуси, а со конечен ред. Да се окаракеризираат сите такви пермутации.

Решение. Нека $\alpha : \mathbb{N} \to \mathbb{N}$ е определено со:

$\alpha = (1\ 2)\ (3\ 4\ 5)\ (6\ 7)\ (8\ 9\ 10)\ (11\ 12)\ (13\ 14\ 15)\ (16\ 17)\ \ldots$

имаме

$\alpha^2 = (3\ 5\ 4)\ (8\ 10\ 9)\ (13\ 15\ 14)\ldots$,

$\alpha^3 = (1\ 2)\ (6\ 7)\ (11\ 12)\ \ldots$

$\alpha^6 = 1_{\mathbb{N}}$.

Значи, α има ред 6, но α има бесконечно многу циклуси со должина 2, како и бесконечно многу со должина 3.

Да претпоставиме сега дека α е пермутација на множеството X и дека $\alpha^n = 1_X$ е идентичната пермутација. Должината на секој циклус $(\ldots a_{i-1}\ a_i\ a_{i+1} \ldots)$ од α е делител на n. Според тоа, една пермутација α има ред n ако и само ако најмалиот заеднички содржател на редовите од циклусите на α е n.

11.4. Нека $A \subseteq M$, а G нека е подгрупа од S_M. Множествата G' и G'' се определени со:

$G' = \{f \mid f \in G,\ (\forall a \in A)\ f(a) = a\}$,

$G'' = \{f \mid f \in G,\ f(A) = A\}$.

Да се покаже дека G' и G'' се подгрупи од S_M и притоа $G' \subseteq G''$.

Решение. Јасно е дека $G' \subseteq G''$. Да покажеме дека G''.е подгрупа од S_M. Навистина, $1 \in G''$, а ако $f, g \in G''$. тогаш имаме

$(fg)(A) = f(g(A)) = f(A) = A$, т.е. $fg \in G''$.

Понатаму, ако $f \in G''$, тогаш $f(A) = A$, па и $f^{-1}(A) = A$, што значи дека $f^{-1} \in G''$. Според тоа, G'' е подгрупа од S_M.

11.5. Да се покаже дека множеството

$S^* = \{f \mid f \in S_{\mathbb{N}}, f(n) \neq n$ само за конечно многу $n \in \mathbb{N}\}$ е подгрупа од $S_{\mathbb{N}}$.

Решение. Јасно е дека $1 \in S^*_{\mathbb{N}}$. Ако $f \in S^*_{\mathbb{N}}$, тогаш и $f^{-1} \in S^*_{\mathbb{N}}$, зашто ако f има m нефиксни броеви, тогаш и f^{-1} има m нефиксни броеви. Ако пак $f \in S^*_{\mathbb{N}}$ т.е. ако f има k нефиксни броеви, а g има m нефиксни броеви, тогаш fg има најмногу $k + m$ нефиксни броеви, т.е. $fg \in S^*_{\mathbb{N}}$. Значи, $S^*_{\mathbb{N}}$ е подгрупа од $S_{\mathbb{N}}$

11.6. Ако $G_n = \{f \mid f \in S_{\mathbb{N}}, (\forall m \in N;\ m > n) f(m) = m\}$, да се покаже дека $S^*_{\mathbb{N}} = \bigcup_{n=1}^{\infty} G_n$.

11.7 Да се покаже дека:

а) секоја конечна група;

б) секоја бесконечна пребројлива група,

е изоморфна со некој подгрупа од групата $S_{\mathbb{N}}$ на сите пермутации од множеството на природните броеви.

Решение. а) Ако G е група со ред n, тогаш, ставајќи $\varphi_a(x) = ax$, добиваме дека $a \to \varphi_a$ е мономорфизам од G во S_G. Според тоа, G е изоморфна со подгрупа од S_n. Од друга страна, ако $\psi \in S_n$ и ако ставиме $\overline{\psi}(i) = \psi(i)$, за $i \leq n$, $\overline{\psi}(m) = m$, за $m > n$, добиваме мономорфизам од S_n во $S_{\mathbb{N}}$

б) Нека $G = \{e, a_1, a_2, \ldots, a_n, \ldots\}$ е пребројлива група. Ако ставиме $\varphi_a(x) = ax$, добиваме мономорфизам од G во S_G. Според тоа, G е изоморфна со некоја подгрупа од $S_{\mathbb{N}}$.

11.8. Нека A е непразно множество, а $B = \{b\}$, $b \notin A$. Да се покаже дека групите S_A и $S_{A \cup B}$ се изоморфни ако и само ако A е бесконечно множество.

11.9. Дадени се пермутациите

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 6 & 2 & 4 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}.$$

Да се пресметаат $\alpha\beta$, $\beta\alpha$, α^{-1}, β^{-1}, $(\alpha\beta)^{-1}$, $(\beta\alpha)^{-1}$.

Одговор.. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix}$, $\beta\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 6 & 1 \end{pmatrix}$,

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 5 & 1 & 3 \end{pmatrix}, \quad \beta^{-1} = \beta,$$

$$(\alpha\beta)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 5 & 1 & 2 \end{pmatrix}, \quad (\beta\alpha)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 3 & 1 & 5 \end{pmatrix}.$$

11.10. Ако пермутацијата $\alpha = \alpha_1\, \alpha_2 \ldots\, \alpha_k$ е претставена како производ од дисјунктни циклуси, да се покаже дека редот на α е најмалиот заеднички содржател од $n_1, n_2, \ldots, n_k$, каде што n_i е редот на циклусот α_i .

Решение. Ако n е најмалиот заеднички содржател за n_i, $i = 1, 2, \ldots, k$, тогаш $\alpha^n = 1$. Значи, редот m на α мора да е фактор во n. Ако $m < n$, тогаш ќе постои барем еден n_i што не е фактор во m.

Но, $\alpha_i^m \neq 1$ па значи и $\alpha^m \neq 1$. Од ова следува дека $m = n$.

11.11. Дадени се пермутациите

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 5 & 3 & 1 & 2 & 7 & 8 & 9 & 10 \end{pmatrix},$$

$$\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 5 & 10 & 9 & 7 & 2 & 6 & 4 & 3 & 1 \end{pmatrix}$$

а) Да се пртстават φ и ψ како производи од дисјуктни циклуси.

б) Да се претстават φ и ψ како производи од транспозиции и да се одреди нивната парност.

в) Да се најдат редовите на φ и ψ, а потоа на $\varphi\,\psi$ и $\psi\,\varphi$.

Решение. а) $\varphi = (1\,4\,3\,5)\,(2\,6)$, $\psi = (1\,8\,4\,9\,3\,10)\,(2\,5\,7\,6)$.

б) $\varphi = (1\ 5)\ (1\ 3)\ (1\ 4)\ (2\ 6)$,
$\psi = (1\ 10)\ (1\ 3)\ (1\ 9)\ (1\ 4)\ (1\ 8)\ (2\ 6)\ (2\ 7)\ (2\ 5)$.
Двете пермутации се парни.
в) Редот на φ е 4, а редот на ψ е 12.
$\varphi\psi = (1\ 8\ 3\ 10\ 4\ 9\ 5\ 7\ 2)$; $\psi\varphi = (1\ 9\ 3\ 7\ 6\ 5\ 8\ 4\ 10)$.

11.12. Нека φ е циклична пермутација. Да се покаже дека:
а) ако редот на φ е бесконечен, тогаш φ^n, $n > 1$, не е циклична пермутација и φ^n има бесконечни дисјуктни циклуси.
б) ако редот на φ е m, тогаш φ^n е циклична ако и само ако $(m, n) = 1$. Ако $(m, n) = d$, тогаш φ^n има d циклуси.

Решение. а) Нека φ е циклична пермутација со бесконечен ред:
$\varphi = (\ldots -3\ -2\ -1\ 0\ 1\ 2\ 3\ldots)$.
Имаме:
$\varphi^2 = (\ldots -3\ -1\ 1\ 3\ldots)\ (\ldots -2\ 0\ 2\ 4\ldots)$;
$\varphi^3 = (\ldots -3\ \ 0\ \ 3\ \ 6\ldots)\ (\ldots -2\ \ 1\ \ 3\ldots)\ (\ldots -1\ \ 2\ \ 5\ldots)$ и, општо,
$\varphi^n(i) = i + n$, па циклусите на φ^n се:
$(\ldots 0\ \ n\ldots)\ (\ldots 1\ \ n+1\ldots)\ (\ldots 2\ \ n+2\ldots)\ \ldots\ (\ldots (n-1)\ \ 2n-1\ldots)$.
Значи, за $n > 1$, φ^n не е циклична.
б) Нека $\varphi = (1\ \ 2\ \ldots\ m)$. Јасно е дека
$\varphi^n(i) = j \Leftrightarrow j \equiv i+n \pmod m$.
Нека $(m, n) = 1$. Имаме:
$\varphi^n : 1 \to 1 + n \to 1 + 2n \to \ldots \to 1 + kn \to 1$, т.е
$\varphi^n(1 + kn) \equiv 1 \pmod m \Leftrightarrow 1 + kn + n \equiv 1 \pmod m \Leftrightarrow$
$\Leftrightarrow n(k + 1) \equiv 0 \pmod m \Leftrightarrow k + 1 \equiv 0 \pmod m \Leftrightarrow k = m - 1$.
Според тоа, циклусот има должина m, па значи има само еден циклус, т.е. φ^n е циклична.
Ако $(m,n) = d$, тогаш од $\varphi^n(1 + kn) \equiv 1$, имаме $n(k + 1) \equiv 0 \pmod m$, па ставајќи $m = sd$, добиваме дека $k + 1 \equiv 0 \pmod s$, т.е. $k = s - 1$. Според тоа имаме $\varphi^n : i \to i + n \to i + 2n \to i + (s-1)n$ (d циклуси).

11.13. Нека φ и ψ се две циклични пермутации, од кои барем едната има конечна должина, чии циклуси имаат еден заеднички елемент. Да се покаже дека $\varphi\psi$ е циклична пермутација. Ако и двете пермутации се со бесконечна должина, дали $\varphi\psi$ е циклична пермутација?

Решение. Да го разгледаме прво случајот кога и двете пермутации φ, ψ се со конечна должина. Ако a е нивниот заеднички елемент, тогаш нив можеме да ги претставиме во облик
$\varphi = (a\ \ a_1\ \ a_2\ \ldots\ a_m)$, $\psi = (a\ \ b_1\ \ b_2\ \ldots\ b_n)$.

Тогаш имаме $\varphi\psi = (a \quad b_1 \quad b_2 \ldots b_n \quad a_1 \quad a_2 \ldots a_n)$, т.е. $\varphi\,\psi$ е циклична пермутација.

Да претпоставиме сега дека едната од φ, ψ е со бесконечна должина. Ако a е заедничкиот елемент, тогаш нив можеме да ги напишеме во облик

$$\varphi = (a \quad a_1 \ldots a_m), \quad \psi = (\ldots b_{-n} \ldots b_{-1} \quad a \quad b_1 \ldots b_n \ldots).$$

Во овој случај имаме:

$$\varphi\psi = (\ldots b_{-n} \ldots b_{-1} \quad a_1 \quad a_2 \ldots a_m \quad a \quad b_1 \ldots b_n \ldots),$$

т.е. $\varphi\psi$ е циклична пермутација. Ако пак φ е со бесконечна должина, тогаш исто така добиваме дека $\varphi\psi$ е циклична пермутација.

Нека сега цикличните пермутации φ и ψ се со бесконечна должина. Ако c е нивниот заеднички елемент, тогаш можеме да ги напишеме во облик

$$\varphi = (\ldots a_{-2} \quad a_{-1} \quad c \quad a_1 \quad a_2 \ldots), \ \psi = (\ldots b_{-2} \quad b_{-1} \quad c \quad b_1 \quad b_2 \ldots), \text{ па}$$

$$\varphi\,\psi = (\ldots b_{-2} \quad b_{-1} \quad a_1 \quad a_2 \ldots)(\ldots a_{-2} \quad a_{-1} \quad c \quad b_1 \quad b_2 \ldots),$$

т.е. $\varphi\,\psi$ не е циклична пермутација.

11.14. Кои од наведените пермутации се парни, а кои непарни:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 2 & 1 & 5 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 6 & 2 & 5 & 7 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 6 & 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 3 & 2 & 5 \end{pmatrix}$$

Одговор. Парна; непарна; парна; непарна; парна.

11.15. Да се покаже дека секоја парна пермутација може да се претстави како производ од циклуси со должина 3.

Решение. Да забележиме прво дека се точни равенствата

$$(ik)\,(ij) = (ijk), \quad (ij)\,(rs) = (isr)\,(ijr).$$

Ако α е парна пермутација, тогаш α може да се претстави како производ од парен број транспозиции. Користејќи ги горните равенства, заклучуваме дека секоја парна пермутација може да се претстави како производ од циклуси со должина 3.

11.16. Да се покаже дека групата S_n е генерирана од множеството:
а) транспозиции $(1\ 2)$, $(1\ 3),\ldots, (1\ n)$.
б) транспозиции $(1\ 2)$, $(2\ 3),\ldots, (n-1\ n)$.
в) $\{\sigma,\tau\}$, $\sigma = (1\ 2\ldots n)$, $\tau = (1\ 2)$.

Решение.. а) Бидејќи секој елемент од S_n може да се претстави како производ на транспозиции, доволно е да покажеме дека која било транспозиција $(i\ j)$ може да се претстави со помош на дадените транспозиции. Имаме:

$(i\ \ j) = (1\ \ i)^{-1}(1\ \ j)\,(1\ \ i)$.

б) Бидејќи $(1\ i) = (i{-}1\ i)\ldots(2\ \ 3)\,(1\ \ 2)$, а користејќи го резултатот од а), секоја транспозиција $(i\ \ j)$ може да се претстави со помош на дадените транспозиции $(1\ 2)$, $(2\ 3),\ldots, (n-1\ n)$.

в) Бидејќи $(2\ 3) = (1\ 2\ldots n)\,(1\ 2)\,(n\ldots\ 2\ 1) = \sigma\,\tau\,\sigma^{-1}$,
$(3\ 4) = (1\ 2\ldots\ n)\,(2\ 3)\,(n\ldots\ 2\ 1) = \sigma^2\tau\sigma^{-2}$ и општо,
$(i+1\ \ i+2) = \sigma^i\tau\,\sigma^{-i}$, $i = 1, 2,\ldots, n-1$, резултатот следува од а).

11.17. Да се покаже дека
$A_n = S_n \Leftrightarrow n = 1$.

Решение. Нека $n = 1$. Тогаш S_1 содржи само еден елемент и тој е парна пермутација. Значи, $S_1 = A_1$.

Ако $n > 1$, тогаш S_n ја содржи пермутацијата $(1\ 2)$, којашто е непарна, па $(1\ 2)\notin A_n$, т.е. $A_n \subset S_n$.

11.18. Нека $H = \{\varphi \mid \varphi\in S_5\,,\ \varphi(1) = 1\}$, а $K = \{\varphi \mid \varphi\in S_5,\ \varphi(1) = 1$ или $\varphi(1) = 2\}$. Да се покаже дека H е подгрупа од S_5, но K не е подгрупа. Колку е редот на H ?

Решение. Бидејќи $\varphi(1) = 1$, за секоја $\varphi\in H$, следува дека H е изоморфна со S_4 , па значи H е подгрупа од S_5 со ред 24.

Дека K не е подгрупа од S_4, покажува следниов пример.

Ако $\psi = (1\ 2\ 3\ 4\ 5\ )$, тогаш $\psi^2 = (1\ 3\ 5\ 2\ 4\ )$. Пермутацијата $\psi\in K$, но $\psi^2\notin K$, па значи K не е подгрупа од S_5.

11.19. Нека $m, n\in\mathbb{N}$, $m < n$, и нека
$H = \{\varphi \mid \varphi\in S_n,\ \ \varphi(i)\in\{1, 2, \ldots, m\}$, за секој $i\in\{1, 2, \ldots, m\}\}$.
Да се покаже дека H е подгрупа од S_n и да се најде редот на H.

11.20. Да се најде алтернативната група A_4, а потоа и сите нејзини подгрупи.

Решение. Алтернативната група A_4 се состои од сите парни пермутации од четири елементи:

$A_4 = \{(1),\ (1\ 2)\ (3\ 4),\ (1\ 3)\ (2\ 4),\ (1\ 4)\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2),$
$(1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\}.$

Да ги најдеме подгрупите на A_4. Прво, секоја подгрупа ја содржи идентичната пермутација (1). Бидејќи пермутациите со по два циклуса имаат ред 2, секој од нив, заедно со идентичната, формира подгрупа. Според тоа :

$H_1 = \{(1), (1\ 2)\ (3\ 4)\}$, $H_2 = \{(1), (1\ 3)\ (2\ 4)\}$, $H_3 = \{(1), (1\ 4)\ (2\ 3)\}$ се подгрупи од A_4.

Ако постои подгрупа што ги содржи пермутациите (1 2) (3 4) и (1 3) (2 4), тогаш таа мора да го содржи и нивниот производ, т.е. и пермутацијата (1 4) (2 3). Така, и

$H_4 = \{(1), (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$ е подгрупа од A_4.

Ако некоја подгрупа од A_4 ја содржи пермутацијата (1 2 3), тогаш таа мора да ја содржи и пермутацијата $(1\ 2\ 3)^2 = (1\ 3\ 2)$. Бидејќи (1 2 3) (1 3 2) = (1), заклучуваме дека

$K_1 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$ е подгрупа.

Слично добиваме дека и

$K_2 = \{(1), (1\ 2\ 4), (1\ 4\ 2)\}$, $K_3 = \{(1), (1\ 3\ 4), (1\ 4\ 3)\}$,

$K_4 = \{(1), (234), (243)\}$ се подгрупи од A_4.

Подгрупа што содржи барем една пермутација со два циклуса и барем една со должина 3 се совпаѓа со A_4. Подгрупата што содржи две пермутации со облик $(i\ j\ k)$ и $(i\ j\ m)$, при што i, j, k, m се меѓусебно различни, ја содржи и пермутацијата

$(i\ j\ k)\ (i\ j\ m) = (i\ k)\ (j\ m)$, па значи и таа се совпаѓа со A_4.

Според тоа, нетривијални подгрупи од A_4 се само H_i, K_i, $i = 1, 2, 3, 4$. Да забележиме дека не постои подгрупа од A_4 со ред 6.

11.21. Една подгрупа од S_n се вика *регуларна* ако сите нејзини елементи, освен идентичната, ги преместуваат сите n симболи.

Да се најдат регуларните подгрупи од S_4.

Решение. Ако H е регуларна подгрупа од S_4, тогаш таа не може да содржи циклуси со должина 3. Значи, H може да содржи пермутации од облик $(i\ j)\ (k\ m)$ и $(i\ j\ k\ m)$, каде што i, j, k, m се меѓусебно различни броеви. Од ова следува дека подгрупите H_1, H_2, H_3, H_4 од 11.20, се регуларни подгрупи од S_4.

Ако H_5 е друга регуларна подгрупа од S_4, тогаш таа содржи циклус со должина 4. На пример, ако $(1\ 2\ 3\ 4) \in H_5$, тогаш

$H_5 = \{(1), (1\ 2\ 3\ 4), (1\ 3)\ (4\ 2), (1\ 4\ 3\ 2)\}$.

На тој начин добиваме дека и

$H_6 = \{(1), (1\ 2\ 3\ 4), (1\ 4)\ (2\ 3), (1\ 3\ 4\ 2)\}$,

$H_7 = \{(1), (1\ 3\ 2\ 4), (1\ 2)\ (3\ 4), (1\ 4\ 2\ 3)\}$ се регуларни подгрупи од S_4. Така се најдени сите регуларни подгрупи од S_4.

11.22. Нека G се состои од сите матрици со ред n што имаат во секоја колона и во секоја редица само по еден елемент различен од 0 и тој е 1.

Да се покаже дека G е група во однос на операцијата множење на матрици, изоморфна со симетричната група S_n.

12.23. Нека $G_1 \subseteq G_2$ се подгрупи од S_n. Да се покаже дека:

а) ако x, y се сврзани од G_1, тогаш тие се сврзани и од G_2.

б) ако T е една класа на транзитивност на G_2, тогаш таа е унија на класи транзитивности на G_1.

в) ако G_1 е транзитивна, тогаш е транзитивна и G_2.

Решение. а) Ако x, y се сврзани од G_1, тогаш постои $\alpha \in G_1$, така што $\alpha(x) = y$. Бидејќи $G_1 \subseteq G_2$, имаме $\alpha \in G_2$, па x, y се сврзани и од G_2.

б) Ако x^σ е класа елементи сврзани со x во однос на G_1, а x^τ класа елементи сврзани со x во однос на G_2, тогаш од $G_1 \subseteq G_2$ е јасно дека $x^\sigma \subseteq x^\tau$. Нека y^σ е друга класа, различна од x^σ. Ако $y_1 \in y^\sigma$ и y_1 е сврзан со некој елемент $x_1 \in x^\sigma$ во однос на G_2, тогаш и секој $y \in y^\sigma$ е сврзан со x_1 во однос на G_2, т.е. $y^\sigma \subseteq x^\tau$. Значи, класата x^τ е унија од класи x^σ.

в) Ако G_1 е транзитивна, тогаш кои било $x, y \in \{1, 2, \ldots, n\}$ се сврзани во однос на G_1. Но, поради $G_1 \subseteq G_2$, тие се сврзани и во однос на G_2, што значи дека и G_2 е транзитивна.

11.24. Групата S_M е транзитивна, за секое множество M.

Решение. Нека a, b се кои било елементи од множеството M. Пресликувањето $\alpha : M \to M$, дефинирано со:

$\alpha(a) = b$, $\alpha(b) = a$, $\alpha(x) = x$ за $x \neq a, b$, е пермутација на M, т.е. $\alpha \in S_M$.

Значи, за кои било $a, b \in M$, постои $\alpha \in S_M$, така што $\alpha(a) = b$, па според тоа групата S_M е транзитивна.

11.25. Да се најдат класите T на транзитивност на групите:

а) $G_1 = [\{(1\ 6\ 4\ 3), (1\ 3\ 2)\ (4\ 6\ 5)\}]$;

б) $G_2 = [\{(1\ 3\ 2\ 4)\ (5\ 6), (1\ 3\ 2)\}]$;

в) $G_3 = [\{(1\ 4\ 2)\ (5\ 7\ 6), (1\ 2\ 3\ 4)\ (5\ 6)\}]$,

каде што G_1 и G_2 се подгрупи од S_6, а G_3 од S_7, генерирани од дадените пермутации.

Одговор. а) $T = \{ 1, 2, 3, 4, 5, 6, \}$ т.е. G_1 е транзитивна.

б) $T_1 = \{1, 2, 3, 4\}$ и $T_2 = \{5, 6\}$.

в) $T_1 = \{1, 2, 3, 4\}$ и $T_2 = \{5, 6, 7\}$.

11.26. Да се покаже дека класите на транзитивност на цикличната група $[\alpha]$, генерирана од една пермутација α, се всушност циклусите на α.

Решение. Ако x, y се елементи од еден циклус на α, да речеме $x = a_m$, $y = a_n$, при што $(\ldots a_m \ldots a_n \ldots)$ е циклусот, тогаш $\alpha^{n-m}(a_m) = a_n$, па значи x и y се сврзани.

Обратно, ако $\alpha^k(x) = y$ за некој k, тогаш, избирајќи го најмалиот позитивен број k со тоа својство, добиваме дека x и y се во еден циклус, при што $x = a_m$, $y = a_{m+k}$.

11.27. Да се покаже дека алтернативната група A_n, за секој n, е транзитивна.

Решение. Нека i, j се кои било елементи од $\{1, 2, \ldots, n\}$.

Ако $k \neq i, j$, тогаш пермутацијата $\alpha = (i\ j\ k)$ е парна и $\alpha(i) = j$, т.е. A_n е транзитивна.

11.28. Да се даде пример на две изоморфни

а) циклични;

б) нециклични групи,

од кои едната е транзитивна, а другата не е.

Решение. а) Групите $G_1 = [(1\ 2\ 3\ 4\ 5\ 6)]$, $G_2 = [(1\ 2)\ (3\ 4\ 5)]$, т.е.

$G_1 = \{(1), (1\ 2\ 3\ 4\ 5\ 6), (1\ 3\ 5)\ (2\ 4\ 6), (1\ 4)\ (2\ 5)\ (3\ 6), (1\ 5\ 3)\ (2\ 6\ 4),$
$(1\ 6\ 5\ 4\ 3\ 2)\}$,

$G_2 = \{(1), (1\ 2)\ (3\ 4\ 5), (3\ 5\ 4), (1\ 2), (3\ 4\ 5), (1\ 2)\ (3\ 5\ 4)\}$,

се циклични подгрупи од S_6 со ред 6, па тие се изоморфни; G_1 е транзитивна, а G_2 – не е, со класи : $T_1 = \{1, 2\}$, $T_2 = \{3, 4, 5\}$, $T_3 = \{6\}$.

б) Подгрупата од S_4:

$G = \{\varepsilon = (1), \alpha_1 = (1\ 3\ 4), \alpha_2 = (1\ 4\ 3), \beta_1 = (1\ 3), \beta_2 = (1\ 4), \beta_3 = (3\ 4)\}$

не е транзитивна, а S_3 е транзитивна. S_3 и G не се циклични и се изоморфни при $f: \alpha_i \to \rho_i$, $\beta_j \to \sigma_j$ $(i = 1, 2;\ j = 1, 2, 3)$.

§ 12. ХОМОМОРФИЗМИ И НОРМАЛНИ ПОДГРУПИ

12.1. Ако $H \lhd G$, K подгрупа од G и $H \subseteq K$, тогаш $H \lhd K$.

Решение. Ако $k \in K$, тогаш $k \in G$, па од $H \lhd G$, следува дека $kH = Hk$, т.е $H \lhd K$.

12.2. Ако H и K се подгрупи од G, при што $H \lhd K$, тогаш $HK = KH$ е подгрупа од G. Ако и $K \lhd G$, тогаш $KH \lhd G$ и $KH = [K \cup H]$.

Решение. Бидејќи $H \lhd G$ имаме

$$HK = \bigcup_{u \in K} Hu = \bigcup_{u \in K} uH = KH,$$

а потоа и $HK\,(HK)^{-1} = HKK^{-1}H^{-1} = HKH = HHK = HK$,

т.е. $HK = KH$ е подгрупа од G.

Ако и $K \lhd G$, тогаш имаме:

$(\forall x \in G)\ xHK = HxK = HKx$, т.е. $HK \lhd G$.

Јасно дека H, $K \subseteq HK$, т.е. $H \cup K \subseteq HK$. Ако L е друга подгрупа од G и $H \cup K \subseteq L$, тогаш имаме $HK \subseteq LL = L$, т.е. $[H \cup K] = HK$.

12.3. Ако H, K и M се подгрупи од G, при што $H \lhd G$, $K \lhd M$, тогаш $HK \lhd HM$.

Решение. Според 12.2, имаме $HK = KH$. Потоа, ако $hm \in HM$ ќе имаме

$HKhm = KHhm = KHm = HKm = hHmK = hmHK$,

т.е. $HK \lhd HM$.

12.4. Ако $\{H_i \mid i \in I\}$ е фамилија нормални подгрупи од групата G, тогаш и $H = \bigcap_i H_i$ е нормална подгрупа од G.

Решение. Јасно дека H е подгрупа од G. Ако $x \in G$, ќе имаме:

$$xH = x(\bigcap_i H_i) = \bigcap_i xH_i = \bigcap_i H_i x = (\bigcap_i H_i)x = Hx,$$

т.е. $H \lhd G$.

12.5. Секоја подгрупа H од G со идекс 2 е нормална подгрупа од G.

Решение. Нека H е подгрупа од G и $(G : H) = 2$. Ако $x \in G$, тогаш или $x \in H$, или $x \in xH$. Ако $x \in H$, тогаш јасно е дека $xH = Hx$. Ако $x \notin H$, тогаш од $H \cap xH = \varnothing = H \cap Hx$ и $G = H \cup xH = H \cup Hx$, следува $Hx = xH$, т.е $H \lhd G$.

12.6. Да се најдат сите нормални подгрупи од групата S_3.

Решение. Вистински подгрупи од S_3 (5.36) се:

$H = \{1, \rho_1, \rho_2\}$, $H_i = \{1, \sigma_i\}$, $i = 1,2,3$.

Подгрупата H е со индекс 2 во S_3, па значи $H \lhd G$. Подгрупата H_i, $i = 1, 2, 3$, не е нормална, зашто на пример, за H_3 имаме:

$\sigma_1^{-1}\sigma_3\sigma_1 = \sigma_1\sigma_3\sigma_1 = \rho_1\sigma_1 = \sigma_2$, а $\sigma_2 \notin H_3$.

12.7. Да се покаже дека групата

$K = \{(1), (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$

е нормална подгрупа од A_4, а $H = \{(1), (1\ 4)\ (2\ 3)\}$ е нормална во K, но H не е нормална во A_4.

Решение. Елементите на групата A_4 се: (1), (1 2) (3 4), (1 3) (2 4), (1 4) (2 3), (1 2 3), (1 2 4), (1 3 4), (2 3 4), (1 3 2), (1 4 2), (1 4 3) и (2 4 3).

За да покажеме дека K е нормална подгрупа од A_4, треба да покажеме дека $x^{-1}Kx = K$ за секој $x \in A_4 \setminus K$. Поради симетријата што постои меѓу 1, 2, 3 и 4, доволно е да провериме дека тоа равенство е точно, на пример, за $x = (1\ 2\ 3)$. Имаме $x^{-1} = (1\ 3\ 2)$, па

$$x^{-1}Kx = (1\ 3\ 2)\{(1), (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}(1\ 2\ 3) =$$
$$= \{(1), (1\ 3\ 2)\ (1\ 2)\ (3\ 4)\ (1\ 2\ 3), (1\ 3\ 2)\ (1\ 3)\ (2\ 4)\ (1\ 2\ 3),$$
$$(1\ 3\ 2)\ (1\ 4)\ (2\ 3)\ (1\ 2\ 3)\} =$$
$$= \{(1), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3), (1\ 2)\ (3\ 4)\} = K.$$

Подгрупата H е нормална во K, бидејќи е со индекс 2. Но, на пример $(1\ 2\ 3)^{-1}(1\ 4)\ (2\ 3)\ (1\ 2\ 3) = (1\ 2)\ (3\ 4) \notin H$, па значи H не е нормална во A_4.

12.8. Нека G е множеството од сите пермутации на $\mathbb{N}$ што го имаат својството:

$\alpha \in G \Leftrightarrow$ секој нетривијален циклус на α е конечен и такви циклуси има конечно многу.

(Со други зборови G се состои од оние пермутации α од $S_{\mathbb{N}}$ што имаат само конечно многу подвижни елементи.) Да се покаже дека:

а) G е нормална подгрупа од $S_{\mathbb{N}}$.

б) множеството P од сите парни пермутации од G е нормална подгрупа од G.

в) P е проста група.

Решение. а) Нека $\varphi \in S_{\mathbb{N}}$, $\alpha \in G$. Ако $n_1, \ldots, n_k$ се подвижните точки на α и ако $m \neq \varphi^{-1}(n_1), \ldots, \varphi^{-1}(n_k)$, тогаш $\varphi(m) \neq n_1, \ldots, n_k$, па

$\varphi^{-1}\alpha\varphi(m) = \varphi^{-1}\varphi(m) = m$, од каде што следува дека $\varphi^{-1}\alpha\varphi \in G$.

12.9. Да се покаже дека секоја подгрупа од кватернионската група K е нормална.

Решение. Вистинските подгрупи од кватернионската група K, (6.6) се:
$H = \{1, -1\}$, $K_1 = \{1, -1, i, -i\}$, $K_2 = \{1, -1, j, -j\}$, $K_3 = \{1, -1, k, -k\}$.
Подгрупите K_1, K_2, K_3 се со индекс 2, па значи тие се нормални. За подгрупата H имаме:
$(\forall x \in K)\ xH = \{x, -x\}$, $Hx = \{-x, x\}$,
т.е. $xH = Hx$. Значи, и H е нормална подгрупа од K.

12.10. Да се најдат нормалните подгрупи од:
а) диедралната група D_4.
б) групата D од 10.9.

Решение. а) Во 10.8, се најдени подгрупите од D_4. Подгрупите H_6, H_7 и H_8 се со индекс 2 во D_4, па значи тие се и нормални подгрупи од D_4. Подгрупата H_1 е исто така нормална подгрупа од D_4, а други нормални подгрупи нема.

До овој заклучок може лесно да се дојде, ако се искористи резултатот од 10.33, каде што се најдени класите конјугирани подгрупи од D_4.

б) Според 10.34 б), добиваме дека нормални подгрупи од D се:
K_n, $n \in \mathbb{N}$, $L_{n,s}$, $n \in \mathbb{N}$, $s = 0, 1, \ldots, n-1$.

12.11. Да се покаже дека множествата
$H = \{(0, b) \mid b \in \mathbb{Q}\}$ и $K = \{(a, 0) \mid a \in \mathbb{Z}\}$ се подгрупи од групата $G = \mathbb{Z} \times \mathbb{Q}$ од 6.4, и $H \lhd G$.
Да се најдат HK и KH. Дали $HK = KH$?

Решение. Операцијата во G е дефинирана со:
$(a, b) \circ (c, d) = (a + c, 2^c b + d)$,
при што $(0, 0)$ е единица во групата G, а $(a, b)^{-1} = (-a, -2^{-a}b)$.
За H имаме:
$(0, b_1) \circ (0, b_2)^{-1} = (0, b_1) \circ (0, -b_2) = (0, b_1 - b_2) \in H$ и
$(a, b) \circ (0, b_1) \circ (a, b)^{-1} = (a, b + b_1) \circ (-a, -2^{-a}b) = (0, 2^{-a} b_1) \in H$,
т.е. H е нормална подгрупа од G. За K имаме:
$(a_1, 0) \circ (a_2, 0)^{-1} = (a_1, 0) \circ (-a_2, 0) = (a_1 - a_2, 0) \in K$,
т.е. K е подгрупа од G. Бидејќи
$(1, 1) \circ (a, 0) \circ (1, 1)^{-1} = (1 + a, 2^a) \circ (-1, -2^{-1}) =$
$= (a, 2^{-1} \cdot 2^a - 2^{-1}) = (a, 2^{-1}(2^a - 1)) \notin K$,
следува дека подгрупата K не е нормална во G.
На крајот имаме $HK = KH = G$.

12.12 Да се покаже дека подмножеството $H = \{(0, z) \mid z \in \mathbb{Z}\}$ е нормална подгрупа од групата G во 6.3.

12.13. Во множеството $G = \mathbb{Z} \times \mathbb{Z} \times \{-1, 1\}$ е определена операција "o" со:

$$(a, b, \pm 1) \text{ o } (c, d, \varepsilon) = (a + c, b + d, \pm \varepsilon),$$

каде што $\varepsilon = \pm 1$. Да се докаже дека G(o) е група, а потоа да се најде $H = [(1, 0, 1)]$ и да се провери дали $H \lhd G$.

Одговор. $H = \{(n, 0, 1) \mid n \in \mathbb{Z}\}$; $H \lhd G$.

12.14. Нека G е која било група. Да се покаже дека подгрупата H од G, генерирана од сите квадрати во G, е нормална подгрупа од G.

Решение. Нека $h \in H$; тоа значи дека

$$h = u_1^2 u_2^2 \ldots u_n^2, \qquad u_i \in G, \qquad i = 1,2,\ldots,n.$$

Тогаш имаме:

$$(\forall x \in G) \quad x^{-1} hx = x^{-1}(u_1^2 \ldots u_n^2)x = (x^{-1}u_1^2 x)\ldots(x^{-1}u_n^2 x) =$$

$$= [(x^{-1}u_1 x)(x^{-1}u_1 x)]\ldots[(x^{-1}u_n x)(x^{-1}u_n x)] =$$

$$= (x^{-1}u_1 x)^2 \ldots (x^{-1}u_n x)^2 \in H,$$

т.е. $H \lhd G$.

12.15. Да се покаже дека центарот $C(G)$ од групата G е нормална подгрупа од G.

Решение. Да покажеме прво дека $C(G)$ е подгрупа од G. Ако c_1, c_2 се елементи од $C(G)$, тогаш за кои било $x \in G$ имаме $c_i x = x c_i$, $i = 1,2$, $x c_2^{-1} = c_2^{-1} x$. . Затоа имаме:

$$(c_1 c_2^{-1})x = c_1(c_2^{-1}x) = c_1(x c_2^{-1}) = (c_1 x)c_2^{-1} = (x c_1)c_2^{-1} = x(c_1 c_2^{-1}),$$

т.е. $c_1 c_2^{-1} \in C(G)$. Значи, $C(G)$ е подгрупа од G. Ако пак $c \in C(G)$, тогаш $x^{-1} c x = c$, па значи, за секој $x \in G$, $x^{-1} cx \in C(G)$, т.е. $C(G)$ е нормална подгрупа од G.

12.16. Нека H е конечна циклична подгрупа од G и нека $H \lhd G$. Ако K е вистинска подгрупа од H, тогаш $K \lhd G$.

Решение. Секоја подгрупа од циклична група е циклична. Да претпоставиме дека $K = [y]$ има ред m. Тогаш, за секој $x \in G$, имаме

$(x^{-1}yx)^m = x^{-1}y^m x = e$.

Ако и $(x^{-1}yx)^r = e$, тогаш добиваме $x^{-1}y^r x = e$, т.е. $y^r = e$.

Значи, $m \mid r$, па редот на елементот $x^{-1}yx$ е m.

Бидејќи $H \lhd G$, следува дека $x^{-1}yx \in H$, па $[x^{-1}yx]$ е подгрупа од H со ред m. Но, за секој $m < n$, $m \mid n$, постои единствена подгрупа од H со ред m, па значи $[x^{-1}yx] = K$, т.е. за секој $x \in G$, $x^{-1}yx \in K$, а тоа пак значи дека $K \lhd G$.

12.17. Ако H и K се две нормални подгрупи од групата G и ако $H \cap K = \{e\}$, тогаш секој елемент од H комутира со секој елемент од K.

Решение. Нека $h \in H$, $k \in K$. Елементот $hkh^{-1}k^{-1}$ припаѓа и на H и на K (зашто H и K се нормални), т.е. $hkh^{-1}k^{-1} \in H \cap K$. Но, $H \cap K = \{e\}$, па значи имаме $hkh^{-1}k^{-1} = e$, т.е. $hk = kh$.

12.18. Ако H е подгрупа на групата G, да се покаже дека $H \lhd N(H)$ и дека, ако H е нормална подгрупа во групата K тогаш $K \subseteq N(H)$. (Притоа, $N(H)$ е *нормализатороѿ* на H во G.)

Решение. Бидејќи $N(H) = \{x \mid x \in G, x^{-1}Hx = H\}$, јасно е дека $H \lhd N(H)$. Потоа, ако K е подгрупа од G и ако $H \lhd K$, тогаш имаме:

$(\forall k \in K)$ $k^{-1}Hk = H$, т.е. $k \in N(H)$,

а тоа значи дека $K \subseteq N(H)$.

12.19. Ако H е подгрупа од групата G, тогаш постои максимална нормална подгрупа во H.

Решение. Во подгрупата H постои барем една нормална подгрупа, на пример, центарот $C(H)$. Применувајќи ја лемата на Цорн, заклучуваме дека во H постои барем една максимална нормална подгрупа.

12.20. Да се покаже дека фактор–група од една циклична група е циклична.

Решение. Нека $G = [a]$ е циклична група, а $H = [b]$ е подгрупа од G. Групата G / H е циклична бидејќи е хомоморфна слика од G при природниот хомоморфизам.

12.21. Нека G е бесконечна циклична група. Да се покаже дека, за секој $n \in \mathbb{N}$, постои единствена подгрупа од G, со индекс n.

Решение. Нека $G = [x]$ е бесконечна циклична група и нека $H_n = [x^n]$, $n \in \mathbb{N}$. Тогаш $H_n = \{x^{nr} \mid r \in \mathbb{Z}\}$ и

$G / H_n = \{H_n, xH_n, \ldots, x^{n-1}H_n\}$.

Значи, редот на G / H_n е n, што преставува индексот на H_n во G.

Нека сега H е подгрупа од G со индекс n. Секоја подгрупа од циклична група е циклична, па постои $r \in \mathbb{N}$, така што $H = [x^r]$, т.е. имаме $H = H_r$. Но, H_r е со индекс r, па значи $r = n$, т.е. $H = H_n$.

12.22. Нека $C = C(G)$ е центарот на групата G. Ако групата G не е комутативна, да се покаже дека фактор–групата G / C не е циклична.

Решение. Да претпоставиме дека фактор–групата G / C е циклична со генератор Ca. Тогаш $G / C = \{Ca^i \mid a \in G, i \in \mathbb{Z}\}$. Ако $x, y \in G$, тогаш тие можат да се претстават во обликот $x = c_1 a$, $y = c_2 a^j$, за некои c_1, c_2 од C. Тогаш имаме:

$$xy = (c_1 a^i)(c_2 a^j) = c_1(a^i c_2) a^j = c_1(c_2 a^i) a^j = c_1 c_2 a^{i+j} =$$
$$= c_2 c_1 a^{j+i} = c_2 (c_1 a^j) a^i = (c_2 a^j)(c_1 a^i) = yx,$$

т.е. групата G е комутативна, спротивно на претпоставката.

12.23. Да се покаже дека фактор–групата $\mathbb{Q} / \mathbb{Z}$ на $\mathbb{Q}(+)$ во однос на $\mathbb{Z}(+)$, е периодична и дека за секој $n \in \mathbb{N}$, постои единствена подгрупа со ред n, којашто е циклична.

Решение. Треба да покажеме дека секој елемент $\mathbb{Z} + x \in \mathbb{Q} / \mathbb{Z}$ е со конечен ред. Ако $x = m / n$, ќе имаме :

$$\underbrace{(\mathbb{Z}+x)+(\mathbb{Z}+x)+\ldots+(\mathbb{Z}+x)}_{n} = \mathbb{Z} + nx = \mathbb{Z} + n(m / n) = \mathbb{Z} + m = \mathbb{Z},$$

т.е. фактор–групата $\mathbb{Q} / \mathbb{Z}$ е периодична.

Нека сега n е даден природен број. Елементот $\mathbb{Z} + 1/n$ генерира циклична подгрупа од $\mathbb{Q} / \mathbb{Z}$, што значи дека за секој $n \in \mathbb{N}$ постои барем една циклична подгрупа со ред n. Нека H е која било подгрупа од $\mathbb{Q} / \mathbb{Z}$ со ред n, т.е. $H = \{\mathbb{Z}, \mathbb{Z} + x_2, \ldots, \mathbb{Z} + x_n\}$, каде што $x_i = p_i / q_i$, $i = 2, 3, \ldots, n$. Можеме да претпоставиме дека $0 < x_i < 1$, $q_2 = \ldots = q_n = q$ и $p_2 < p_3 < \ldots < p_n$. Ако ги поделиме p_i со $p_2 = p$, нека добиеме $p_i = s_i p + r_i$, $0 \le r_i < p$.

Бидејќи $(p_i / q) - (s_i p / q) = r_i / q$, добиваме дека $r_i / q \in \mathbb{Z}$, што е можно само за $r_i = 0$. Значи, p е фактор во p_i за секој i, па имаме:

$$H = \{\mathbb{Z}, \mathbb{Z} + p / q, \mathbb{Z} + s_3 p / q, \ldots, \mathbb{Z} + s_n p / q\}.$$

Бидејќи подгрупата H е со ред n, q е фактор во np. Ако $p > 1$, тогаш, поради $p < s_3 p < \ldots < s_n p$, би имале $s_n \ge n$, па и $s_n p / q \ge 1$, коешто е спротивно на претпоставката $x_i < 1$. Според тоа, имаме $p = 1$ и $q = n$, т.е. H е генерирана од елементот $\mathbb{Z}+1/n$.

12.24. Нека G е комутативна непериодична група. Да се покаже дека фактор–групата $G / T(G)$ е апериодична.

Решение. Нека $xT(G)$ е произволен елемент од $G / T(G)$, различен од $T(G)$. Тоа значи дека $x \notin T(G)$, т.е. x нема конечен ред. Ако би постоел $n \in \mathbb{N}$, со својството $(xT(G))^n = T(G)$, т.е. $x^n T(G) = T(G)$, тогаш $x^n \in T(G)$, што значи дека x^n има конечен ред. Но, тогаш и x ќе има конечен ред, спротивно на претпоставката дека $x \notin T(G)$. Значи, групата $G / T(G)$ е апериодична.

12.25. Нека G и H се групи, а $f : G \to H$ епиморфизам. Да се покаже дека f е изоморфизам ако и само ако $\mathrm{Ker} f = \{e\}$, каде што e е единицата во G.

Решение. Ако f е изоморфизам, тогаш е јасно дека $\mathrm{Ker} f = \{e\}$. Обратно, да претпоставиме дека за епиморфизмот $f : G \to H$, $\mathrm{Ker} f = \{e\}$. За да покажеме дека f е изоморфизам, доволно е да покажеме дека f е инјекција. Затоа, нека $f(x_1) = f(x_2)$. Тогаш имаме:

$$e' = f(x_1)\,(f(x_2))^{-1} = f(x_1)\,f(x_2^{-1}) = f(x_1 x_2^{-1}),$$

а бидејќи $\mathrm{Ker} f = \{e\}$, следува $x_1 x_2^{-1} = e$, т.е. $x_1 = x_2$, што значи дека f е инјекција.

12.26. Ако $f : G \to G'$ е хомоморфизам, а S е подгрупа од G, тогаш рестрикцијата $g = f_S$ е хомоморфизам и притоа $\mathrm{Ker} g = S \cap \mathrm{Ker} f$.

12.27. Нека G е група и a е фиксен елемент од G. Определуваме пресликување $f : \mathbb{Z} \to G$ со $f(m) = a^m$. Да се покаже дека:

а) f е хомоморфизам од $\mathbb{Z}(+)$ во G.

б) f е мономорфизам ако и само ако a има бесконечен ред.

Решение. а) Нека $m, n \in \mathbb{Z}$. Имаме $f(m + n) = a^{m+n} = a^m a^n = f(m) f(n)$, т.е. f е хомоморфизам.

б) Бидејќи условот $f(m) = f(n) \Rightarrow m = n$ е еквивалентен со условот

$a^m = a^n \Rightarrow m = n$ добивме дека f е мономорфизам ако и само ако a има бесконечен ред.

12.28. Нека f е хомоморфизам од G во G'. Ако $a \in G$ има конечен ред m, тогаш $f(a) = a'$ има конечен ред m' и притоа m' е делител на m.

Решение. Нека $a \in G$ има конечен ред m и нека $H = [a]$. Тогаш $f(H)$ е циклична подгрупа од G', генерирана со $f(a) = a'$. Бидејќи H има конечен ред, подгрупата $f(H)$ има исто така конечен ред m', што значи a' има конечен ред m'. Бидејќи

$a' = (f(a))^m = f(a^m) = f(e) = e'$, следува дека m' е делител на m.

12.29. Ако групата G е со конечен ред n и, ако $f : G \to H$ е хомоморфизам, да се покаже дека редот на $f(G)$ е фактор во n.

Решение. Од првата теорема за изоморфизам следува дека $f(G)$ е изоморфна со $G/\mathrm{Ker}f$. Ако m е редот на $f(G)$, тогаш $m = (G : \mathrm{Ker}f)$, па значи m е фактор во n.

12.30. Ако G е циклична група со ред n, а p е фактор во n, тогаш постои хомоморфизам f од G во подгрупата со ред p. Да се најде $\mathrm{Ker}f$.

Решение. Нека $G = [x]$, $n = pm$ и нека $H = [y]$ е подгрупа од G со ред p. Ако $f : G \to H$ е дефинирано со

$f(x^k) = y^k, \qquad 0 \le k \le n-1,$

тогаш, јасно е дека f е пресликување. Бидејќи $x^r x^s = x^{r+s-\varepsilon n}$, каде што $\varepsilon = 0$ за $r + s \le n-1$, а $\varepsilon = 1$ за $r + s \ge n$, ќе имаме:

$f(x^r x^s) = f(x^{r+s-\varepsilon n}) = y^{r+s-\varepsilon n} = y^r y^s y^{-\varepsilon n}$.

Но, редот на y е фактор во n, па $y^{-\varepsilon n} = 1$. Значи, имаме

$f(x^r x^s) = y^r y^s = f(x^r) f(x^s)$, т.е. f е хомоморфизам од G во H.

Потоа имаме:

$\mathrm{Ker}f = \{x^k \mid f(x^k) = e, 0 \le k \le n-1\} = \{x^k \mid y^k = e\}$

$= \{x^k \mid p \mid k\} = \{x^p, x^{2p}, \ldots, x^{(m-1)p}\} = [x^p]$.

12.31. Нека G е множеството пресликувања $f_{a,b} : \mathbb{R} \to \mathbb{R}$, дефинирани со: $(\forall x \in \mathbb{R})\ f_{a,b}(x) = ax + b, \quad a \neq 0$.

а) Да се покаже дека G е група.

б) Да се покаже дека преасликувањето $\varphi : G \to G$, дефинирано со $\varphi(f_{a,b}) = f_{a,0}$ е хомоморфизам.

в) Да се најде $\mathrm{Ker}\,\varphi$.

Решение. Бидејќи $(f_{a,b} f_{c,d}) = acx + ad + b = f_{ac,\,ad+b}(x)$, добиваме

$f_{a,b} f_{c,d} = f_{ac,\,ad+b}$.

Затоа :

$\varphi(f_{a,b} f_{c,d}) = \varphi(f_{ac,\,ad+b}) = f_{ac,0} = f_{a,0} f_{c,0} = \varphi(f_{a,b})\,\varphi(f_{c,d})$,

т.е. φ е хомоморфизам.

в) $\mathrm{Ker}\,\varphi = \{f_{1,b} \mid b \in \mathbb{R}\}$.

12.32. Ако групите G и G' се изоморфни, да се покаже дека и нивните центри $C(G)$ и $C(G')$ се изоморфни.

Решение. Нека $f: G \to G'$ е изоморфизам. Тогаш рестрикцијата g од f на $C(G)$ е мономорфизам од $C(G)$ во G', па за да покажеме дека $C(G)$ и $C(G')$ се изоморфни, доволно е да покажеме дека

$$g(C(G)) = C(G').$$

Нека $c \in C(G)$;

Ако $a' \in G'$, тогаш постои $a \in G$, таков што $f(a) = a'$ и:

$$g(c)\, a' = f(c) f(a) = f(ca) = f(ac) = f(a) f(c) = a' g(c),$$

што значи дека $g(c) \in C(G')$, т.е. $g(C(G)) \subseteq C(G')$.

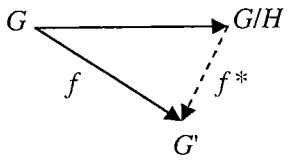
Ако пак $b' \in C(G')$, тогаш постои $b \in G$, таков што $f(b) = b'$ и ако $x \in G$ е произволен елемент, имаме:

$$f(xb) = f(x) f(b) = f(b) f(x) = f(bx).$$

Бидејќи f е инјекција имаме $xb = bx$, што значи $b \in C(G)$, т.е. $g(C(G))$ го содржи центарот $C(G')$.

Значи $g(C(G)) = C(G')$, т.е. $C(G)$ и $C(G')$ се изоморфни.

12.33. Ако f е хомоморфизам од групата G во групата G', а H нормална подгрупа од G со својството $H \subseteq \mathrm{Ker} f$, тогаш постои единствен хомоморфизам $f^*: G/H \to G'$, таков што дијаграмот:



е комутативен, т.е. $f = f^* h$, каде што $h : G \to G/H$ е природниот хомоморфизам.

Решение. Ако постои пресликување f^* што ги задоволува условите на задачата, тогаш мора да е

$$f^*(xH) = f(x). \qquad (1)$$

Бидејќи $H \subseteq K = \mathrm{Ker} f$, $xH = yH$ повлекува $xK = yK$, т.е. $xH = yH$, повлекува $x = y$. Значи, $f(x)$ зависи само од xH, а не од x, па според тоа f^* определено со (1) е пресликување.

Бидејќи

$$f^*(xHyH) = f^*(xyH) = f(xy) = f(x) f(y) = f^*(xH) f^*(yH),$$

f^* е хоморфизам.

Ако $g : G / H \to G'$ е хомоморфизам со својството $f = gh$, тогаш од $gh = f*h$, бидејќи h е епиморфизам, следува $g = f*$, т.е. $f*$ е единствен.

12.34. Нека G е група. Секој елемент $\tau_a \in \mathrm{Aut}G$, определен со
$(\forall x \in G)\ \tau_a(x) = a^{-1}xa$,
се вика *внатрешен автоморфизам* на G. Да се покаже дека:

а) Множеството V од сите внатрешни автоморфизми е нормална подгрупа од групата Aut G.

б) V е изоморфна со фактор–групата $G / C(G)$.

Решение. а) Бидејќи
$$b^{-1}(a^{-1}xa)\,b = (ab)^{-1}x(ab),\quad a(a^{-1}xa)\,a^{1} = x,$$
добиваме дека $\tau_a\tau_b = \tau_{ba}$ и $\tau_{a^{-1}} = \tau_a^{-1}$, од каде што следува дека V е подгрупа од Aut$G$.

Нека $\varphi \in \mathrm{Aut}G$. Тогаш $\varphi^{-1}\tau_a\varphi \in \mathrm{Aut}G$ и имаме
$$(\varphi^{-1}\tau_a\varphi)(x) = \varphi^{-1}(a^{-1}\varphi(x)\,a) = (\varphi^{-1}(a))^{-1}x(\varphi^{-1}(a)),$$
т.е. $\varphi^{-1}\tau_{a\varphi} = \tau_{\varphi^{-1}(a)} \in V$. Значи, $V \lhd \mathrm{Aut}G$.

б) Да го разгледаме пресликувањето $f : G \to V$, определено со $f(a) = \tau_{a^{-1}}$. Бидејќи
$$f(ab) = \tau_{(ab)^{-1}} = \tau_{b^{-1}a^{-1}} = \tau_{a^{-1}}\tau_{b^{-1}} = f(a)f(b),$$
следува дека f е хомоморфизам, а јасно е дека е и епиморфизам. Понатаму, од
$$\tau_a = 1_G \Leftrightarrow (\forall x \in G)\ ax = xa,$$
следува дека $\mathrm{Ker}f = C(G)$, па значи $G / C(G) \cong V$.

12.35. Ако групата G е некомутативна, тогаш групата V од сите внатрешни автоморфизми на G не е циклична.

Упатство. Види 12.22 и 12.34.

12.36. Нека H, K и L се нормални подгрупи од групата G, при што H и K се изоморфни како групи. Да се покаже дека:

а) G / H и G / K може да не бидат изоморфни.

б) H / L и K / L може да не бидат изоморфни.

Решение. Нека $G = \mathbb{Z}(+)$, $H = 2\mathbb{Z}$, $K = 3\mathbb{Z}$, $L = 6\mathbb{Z}$. Тогаш:

а) $G / H \cong \mathbb{Z}_2$, $\quad G / K \cong \mathbb{Z}_3$;

б) $H / L \cong \mathbb{Z}_3$; $\quad K / L \cong \mathbb{Z}_2$,

а $\mathbb{Z}_2$ и $\mathbb{Z}_3$ не се меѓусебно изоморфни.

12.37. Нека $f: G \to M$ е епиморфизам, а H е подгрупа од G. Да се покаже дека $f(H)$ е подгрупа од M и притоа, ако $H \lhd G$, тогаш $f(H) \lhd M$.

Решение. Јасно е дека $f(H)$ е подгрупа од M. Да претпоставиме дека $H \lhd G$. Ако y е произволен елемент од M, тогаш, бидејќи f е епиморфизам, постои $b \in G$, таков што $y = f(b)$. Тогаш имаме:

$y^{-1} f(a) y = (f(b))^{-1} f(a) f(b) = f(b^{-1} ab)$.

Но, H е нормална подгрупа од G, па ако $a \in H$, тогаш и $b^{-1} ab \in H$, т.е. ако $a \in H$, тогаш $y^{-1} f(a)\ y \in f(H)$, за секој $y \in M$, а тоа значи дека $f(H)$ е нормална подгрупа од M.

12.38. Нека $f: G \to M$ е епиморфизам, а K подгрупа од M. Да се покаже дека:

а) $H = f^{-1}(K)$ е подгрупа од G и $\mathrm{Ker} f \subseteq H$.

б) ако H_1 е подгрупа од G, со својството $\mathrm{Ker} f \subseteq H_1$ и $f(H_1) = K$, тогаш $H_1 = H$.

в) ако $K \lhd M$, тогаш и $H \lhd G$.

Решение. а) Бидејќи $f(e) = e' \in K$, следува дека $e \in H$, т.е. $H \neq \emptyset$. Потоа имаме:

$(\forall h_1, h_2 \in H)\ \ f(h_1 h_2^{-1}) = f(h_1) f(h_2^{-1}) = f(h_1)(f(h_2))^{-1} \in K$, т.е.

$h_1 h_2^{-1} \in H$, а тоа значи дека H е подгрупа од G.

Од $\mathrm{Ker} f = \{x \mid f(x) = e'\}$, а $e' \in K$, добиваме дека $\mathrm{Ker} f \subseteq H$.

б) Нека H_1 е подгрупа од G, при што $\mathrm{Ker} f \subseteq H_1$ и $f(H_1) = K$. Ако $h_1 \in H_1$, тогаш $f(h_1) \in K$, т.е. $h_1 \in H$. Значи, $H_1 \subseteq H$.

Потоа, ако $h \in H$, тогаш $f(h) \in K$. Бидејќи f е епиморфизам, постои $h_1 \in H_1$, така што $f(h_1) = f(h)$, т.е. $f(hh_1^{-1}) = e'$. Од тоа следува дека $hh_1^{-1} \in \mathrm{Ker} f$, а бидејќи $\mathrm{Ker} f \subseteq H_1$, добиваме $hh_1^{-1} \in H_1$, т.е. $h \in H_1$. Значи, $H \subseteq H_1$.

Од сето тоа следува дека $H_1 = H$.

в) Нека $K \lhd M$. Тогаш имаме:

$(\forall h \in H)\ (\forall x \in G) f(x^{-1} hx) = (f(x))^{-1} f(h)\ f(x) \in K$,

т.е. $x^{-1} hx \in H$. Значи, $H \lhd G$.

12.39. Нека $H \lhd G$, а K е подгрупа од G / H. Да се покаже дека постои единствена подгрупа M од G, таква што $H \subseteq M$ и $K = M / H$.

Решение. Нека $f: G \to G / H$ е природниот епиморфизам, и нека ставиме $M = \{x \mid x \in G,\ f(x) \in K\}$. Бидејќи f е епиморфизам, според 12.38,

следува дека M е подгрупа од G и дека $\mathrm{Ker} f = H \subseteq M$. Јасно дека $M / H = f(M) = K$. Единствеността следува од 12.38 б).

12.40. Нека $H \lhd G$, така што G / H е циклична група со ред 6. Да се најдат сите подгрупи K_i од G / H, а потоа подгрупите M_i од G, за кои важи $M_i / H = K_i$.

Решение. Да ставиме $G / H = [\, xH \,]$. Вистински подгрупи од G / H се:
$K_1 = \{H, x^3H\}$, $K_2 = \{H, x^2H, x^4H\}$.

Според 12.39, ако $f : G \to G / H$ е природниот епиморфизам, добиваме:

$M_1 = \{x \mid x \in G, f(x) \in K_1\} = \{x \mid x \in G, f(x) \in H \text{ или } f(x) \in x^3H\} = H \cup x^3H$,
$M_2 = \{x \mid x \in G, f(x) \in K_2\} = H \cup x^2H \cup x^4H$.

12.41. Нека $f : G \to K$ е епиморфизам, а M нека е подгрупа од K со индекс $n < \infty$. Ако $H = f^{-1}(M)$, тогаш подгрупата H е исто така со индекс n во G.

Решение. Нека $a_1 M$, $a_2 M$,..., $a_n M$, $a_i \in K$, се различните леви комплекси на M во K. Бидејќи f е епиморфизам, постојат $g_i \in G$, т.ш. $f(g_i) = a_i$, $i = 1,\ldots, n$. Да ги формираме подмножествата

$$g_1 H,\ g_2 H,\ldots,\ g_n H \tag{1}$$

во G. Ако $g_i H = g_j H$, тогаш $g_i g_j^{-1} \in H$, па

$f(g_i g_j^{-1}) = f(g_i)\,(f(g_j))^{-1} = a_i a_j^{-1} \in K$, т.е. $a_i K = a_j K$.

Но, $a_i K \cap a_j K = \varnothing$ за $i \neq j$. За да покажеме дека е $(G : H) = n$, треба да покажеме дека секој елемент од G, припаѓа барем на едно од множествата (1).

Затоа, нека x е произволен елемент од G. Тогаш $f(x) \in K$, па $f(x) \in a_i M$, за некој $i = 1,\ldots, n$. Значи, постои $b \in M$, таков што $f(x) = a_i b$. Да ставиме $g = g_i^{-1} x$. Тогаш имаме

$f(g) = f(g_i^{-1} x) = a_i^{-1} a_i b = b$, т.е. $g = g_i^{-1} x = f^{-1}(b)$.

Значи, $g \in H$, т.е. $x \in g_i H$.

12.42. Нека H е подгрупа од G со индекс n. Ако $f : G \to K$ е епиморфизам и ако $\mathrm{Ker} f \subseteq H$, тогаш $f(H)$ е со индекс n во K.

Упатство. Слично како 12.41.

12.43. Нека $\mathbb{Q}^*$ е мултипликативна група на рационалните броеви ($\neq 0$) и нека $f : \mathbb{Q}^* \to \mathbb{Q}^*$ е пресликување дефинирано со:

$(\forall x \in \mathbb{Q}^*)\ f(x) = |x|$.

а) Да се покаже дека f е хомоморфизам.

б) Да се најде $\mathrm{Ker} f$.

в) Да се провери точноста на првата теорема за изоморфизам

Решение. а) Бидејќи

$f(xy) = |xy| = |x||y| = f(x)f(y)$,

следува дека f е хомоморфизам.

б) $\mathrm{Ker} f = \{x \mid f(x) = 1\} = \{x \mid |x| = 1\} = \{1, -1\}$.

в) Да го провериме само третиот дел од првата теорема за изоморфизам, т.е. да провериме дека постои единствен мономорфизам f^* од $\mathbb{Q}^* / \mathrm{Ker} f$ во $\mathbb{Q}^*$, таков што $f = f^* g$, каде што

$g : \mathbb{Q}^* \to \mathbb{Q}^* / \mathrm{Ker} f$ е природниот епиморфизам. Бидејќи

$\mathbb{Q}^* / \mathrm{Ker} f = \{\{-q, q\} \mid q \in \mathbb{Q}^*\}$,

имаме $g(x) = \{-x, x\}$, за секој $x \in \mathbb{Q}^*$,

$f^* : \mathbb{Q}^* / \mathrm{Ker} f \to \mathbb{Q}^*$, дефинирано со: $f^*(\{-x, x\}) = |x|$, е мономорфизам и притоа единствен со својството $f = f^* g$.

12.44. Нека G е подгрупа од S_n и нека $f : G \to \{-1, 1\}$ е пресликување, дефинирано со:

$$f(a) = \begin{cases} 1 \text{ ако } a \text{ е парна,} \\ -1 \text{ ако } a \text{ е непарна.} \end{cases}$$

Да се покаже дека f е хомоморфизам од G во групата $\{1, -1\}$ со два елемента. Што може да се заклучи користејќи ја првата теорема за изоморфизам?

Решение. Дека f е хомоморфизам, лесно се покажува. Ако H е множеството парни пермутации од G, тогаш $H = \mathrm{Ker} f$, па според првата теорема за изоморфизам, добиваме дека $H \lhd G$.

12.45. Нека G е конечна група со ред n, а $k > 1$ нека е природен број, таков што:

$(\forall x, y \in G)\ (xy)^k = x^k y^k$.

Ако $H = \{\forall x \mid x \in G, x^k = e\}$, $K = \{x^k \mid x \in G\}$, да се покаже дека H и K се нормални подгрупи во G и дека $(G : H)$ е редот на K.

Решение. Да покажеме дека H е нормална подгрупа од G. Бидејќи $e^k = e$, следува дека $H \neq \emptyset$. Потоа имаме:

$(xy^{-1})^k = x^k (y^{-1})^k = x^k (y^k)^{-1} = ee^{-1} = e$,

т.е. H е подгрупа од G. На крајот имаме:

$(\forall g \in G)\ (\forall x \in H)\ (g^{-1} x g)^k = g^{-1} x^k g = g^{-1} g = e$,

т.е. $H \lhd G$. Слично и за K.

Да покажеме дека $(G : H) = |K|$. Пресликувањето $f : G \to K$, дефинирано со $f(x) = x^k$ е сурјекција и притоа имаме

$f(xy) = (xy)^k = x^k y^k = f(x) f(y)$, т.е. е епиморфизам.

Јадрото $\mathrm{Ker} f$ ги содржи оние и само оние елементи од G за кои $x^k = e$, т.е. имаме $\mathrm{Ker} f = H$. Според првата теорема за изоморфизам, добиваме дека G / H е изоморфна со K, од каде што следува дека $|G / H| = (G : H) = |K|$.

12.46. Нека $\mathbb{Q}^*$ е мултипликативната група на рационалните броеви и нека $H = \{1, -1\}$, $K = [1 / 2]$. Да се најдат KH и KH / H и да се провери точноста на втората теорема за изоморфизам.

Решение. Имаме $K = \{1/2^r \mid r \in \mathbb{Z}\}$, па

$KH = \{x \mid x = kh,\ k \in K,\ h \in H\} = \{x \mid x = k$ или $x = -k,\ k \in K\} =$

$= \{x \mid x = \pm 1 / 2^r,\ r \in \mathbb{Z}\}$.

Да ја најдеме групата KH / H. Имаме:

$KH/H = \{x\{-1,1\} \mid x \in KH\} = \{\{1/2^r, -1/2^r\} \mid r \in \mathbb{Z}\} =$

$= \{(\frac{1}{2}\{-1,1\})^r \mid r \in \mathbb{Z}\} = \{(\frac{1}{2}H)^r \mid r \in \mathbb{Z}\}$.

За $r \neq 0$, $1/2^r \notin H$, па $KH / H = \left[\frac{1}{2}H\right]$ е бесконечна циклична група. Потоа, имаме $K \cap H = \{1\}$, $K / (K \cap H)$ е изоморфна со K. Но, K е бесконечна циклична група, па групите KH / H и $K/(K \cap H)$ се изоморфни, каде што изоморфизмот е f, определен со

$$f(\frac{1}{2^r}H) = \left\{1/2^r\right\}.$$

12.47. Ако H_1 и H_2 се две нормални подгрупи од групата G и, ако K е подгрупа од G, со својството $K \cap H_1 = K \cap H_2$, тогаш групите KH_1 / H_1 и KH_2 / H_2 се изоморфни.

Решение. Од втората теорема за изоморфизам следува дека

$KH_1 / H_1 \cong K / (K \cap H_1)$, $KH_2 / H_2 \cong K / (K \cap H_2)$.

Од друга страна, бидејќи $K \cap H_1 = K \cap H_2$, следува дека

$K / (K \cap H_1) = K / (K \cap H_2)$, па значи, $KH_1 / H_1 \cong KH_2 / H_2$.

12.48. Ако K_1 и K_2 се подгрупи од групата G и ако постои нормална подгрупа H во G, со својството $K_1 H = K_2 H$, тогаш групите $K_1 / (K_1 \cap H)$ и $K_2 / (K_2 \cap H)$ се изоморфни.

Упатство. Да се искористи втората теорема за изоморфизам.

12.49. Нека K и H се нормални подгрупи од групата G, а L подгрупа од G. Ако редовите на K и H се заемно прости со редот на L, тогаш групите LH / H и LK / K се изоморфни.

Упатство. Да се докаже прво дека $L \cap H = L \cap K$, а потоа да се искористи втората теорема за изоморфизам.

12.50. Нека $\tau = (12)$, а $H = [\tau]$. Да се покаже дека фактор–групата HA_n / A_n е со ред 2.

Решение. Според втората теорема за изоморфизам, имаме:

$$HA_n / A_n \cong H / (H \cap A_n). \qquad (1)$$

Бидејќи τ е непарна пермутација, $\tau \notin A_n$, а од $\tau^2 = (1)$, следува дека $H = \{1, \tau\}$. Значи, имаме $H \cap A_n = \{1\}$, па $H / (H \cap A_n)$ е изоморфна со H. Бидејќи H е со ред 2, според (1), добиваме дека и HA_n / A_n е со ред 2.

12.51. Нека $G = [a]$ е циклична група со ред 12 и нека $H = [a^6]$, $K = [a^2]$. Да се најдат групите G / H, K / H, $(G / H) / (K / H)$ и да се докаже дека $(G / H) / (K / H)$ и G / K се изоморфни.

Решение. Бидејќи $H = \{e, a^6\}$ елементите на G/H се:

$$A_1 = H,\ A_2 = Ha = \{a, a^7\},\ A_3 = Ha^2 = \{a^2, a^8\},\ A_4 = Ha^3 = \{a^3, a^9\},$$
$$A_5 = Ha^4 = \{a^4, a^{10}\},\ A_6 = Ha^5 = \{a^5, a^{11}\}.$$

Бидејќи $K = \{e, a^2, a^4, a^6, a^8, a^{10}\}$, имаме $K / H = \{A_1, A_3, A_5\}$, а, $(G / H) / (K / H) = \{\{A_1, A_3, A_5\}, \{A_2, A_4, A_6\}\} = \{B_1, B_2\}$ и притоа

$$B_2 B_2 = (K / H) A_2 (K / H) A_2 = (K / H) A_2 A_2 = (K / H) A_3 = B_1,$$

т.е. $(G / H) / (K / H) = [B_2]$ е циклична група со ред 2.

Елементите на G / K се:

$C_1 = \{e, a^2, a^4, a^6, a^8, a^{10}\}$ и $C_2 = \{a, a^3, a^5, a^7, a^9, a^{11}\}$, при што $C_2 C_2 = C_1$. Значи, $G / K = [C_2]$ е циклична група со ред 2.

Според тоа, добиваме дека групите $(G / H) / (K / H)$ и G / K, како циклични групи со ред 2, се изоморфни.

12.52. Нека $H, K \lhd G$, при што $H \subseteq K$. Ако G / K и K / H се конечни, да се покаже дека и G / H е конечна.

Упатство. Да се искористи третата теорема за изоморфизам.

12.53. Нека $H, K \lhd G$, при што $H \subseteq K$. Ако K / H е со ред 2, а G / K е циклична, да се покаже дека G / H е комутативна.

Решение. Бидејќи G / K е циклична, а според третата теорема за изоморфизам, групите G / K и $(G / H) / (K / H)$ се изоморфни, следува

дека и групата $(G / H) / (K / H)$ е циклична. Бидејќи K / H е со ред 2, да ставиме $K / H = \{H, kH\}$. Тогаш имаме:

$$(G / H) / (K / H) = \{gH\,(K / H) \mid g \in G\} = \{\{gH, (gH)\,(kH)\} \mid g \in G\}.$$

$$(G / H) / (K / H) = \{(K / H)\,gH \mid g \in G\} = \{\{gH, (kH)\,(gH)\} \mid g \in G\}.$$

Значи имаме $(kH)\,(gH) = (gH)\,(kH)$, т.е. $K / H = C(G / H)$. Според 12.22, следува дека групата G / H е комутативна.

§13. ТЕОРЕМИ НА СИЛОВ

13.1. Нека H е нормална подгрупа од G. Да се покаже дека, ако H и G/H се p–групи, тогаш и G е p-група.

Решение. Нека xH, $x \in G$ е произволен елемент од G / H. Можеме да претпоставиме дека $x \notin H$, зашто ако $x \in H$, тогаш поради тоа што H е p–група, редот на x е степен од p. Бидејќи G / H е p–група, постои $k \in \mathbb{N}$, таков што

$$H = (xH)^{p^k} = x^{p^k} H ,$$

од каде што следува дека $x^{p^k} \in H$, Но, и H е p–група, па постои некој $m \in \mathbb{N}$, таков што

$$(x^{p^k})^{p^m} = e, \text{ т.е. } x^{p^{k+m}} = e .$$

Значи, редот на секој елемент $x \in G$ е степен од p, т.е. G е p–група.

13.2. Нека G е p–група со ред p^n. Да се покаже дека за секој $k : 0 \le k \le n$, G содржи нормална подгрупа H_k со ред p^k.

Решение. Прво да претпоставиме дека G е комутативна. Доказот ќе го спроведеме со индукција по n.

За $n = 1$, тврдењето е точно, зашто самата група G и единичната се подгрупи.

Да претпоставиме дека тврдењето е точно за секој $m < n$, т.е. секоја комутативна група со ред p^m има подгрупа со ред p^k, каде што $0 \le k \le m$. Нека групата G има ред p^n. Според теоремата на Коши, постои $a \in G$ со ред p. Да ставиме

$$K = [a] = \{e, a, \ldots, a^{p-1}\}$$

и да ја разгледаме фактор–групата G / K. Таа е, исто така, комутативна и има ред p^{n-1}. Според индуктивната претпоставка, постои подгрупа H од G / K со ред p^k, за секој $k : 0 \le k \le n - 1$. Според 12.39, постои подгрупа H од G што ја содржи K и $H / K = \overline{H}$. Редот на H во G е $k + 1$, па значи во G постои подгрупа H_s, $s = k + 1$, за секој s: $0 \le s \le n$.

Нека сега G е некомутативна група; тогаш центарот $C(G)$ има ред p^m, $m<n$. Бидејќи $C(G)$ е комутативна, во неа постои нормална подгрупа H_k со ред p^k за секој $k : 0 \le k \le m$. H е нормална и во G. Значи, G содржи нормална подгрупа H_k со ред p^k за секој k: $0 \le k < m$, каде што p^m е редот на $C(G)$.

Ако $m < k \leq n$, фактор–групата $G / C(G)$ ќе има ред p^{n-m}, па во неа постои нормална подгрупа $\tilde{H}$ со ред p^{k-m}. Според 12.39, во G постои подгрупа H, така што $H/C(G) = \tilde{H}$ и нејзиниот ред е $p^m p^{k-m} = p^k$, што требаше да се докаже.

13.3. Нека G е група со ред $p^k m$, каде што p е прост број и $(p, m) = 1$. Да се покаже дека постои низа подгрупи $P_1 \subset P_2 \subset \ldots \subset P_k$, такви што P_i има ред p^i и P_i е нормална подгрупа во P_{i+1}.

Упатство. Да се искористи 13.2.

13.4. Центарот на секоја неединична конечна p–група е неединична подгрупа.

Решение. Нека $K_1, K_2, \ldots, K_{r+1}, \ldots, K_{r+s}$ се класите конјугирани елементи во G при што $K_1 = \{e\}$, $K_2 = \{a_2\}, \ldots, K_r = \{a_r\}$ се сите едноелементни класи, а преостанатите имаат повеќе од еден елемент. Бидејќи една класа конјугирани елементи се состои само од еден елемент, ако и само ако тој се содржи во центарот на G, имаме $C(G) = \{e, a_2, \ldots, a_r\}$. Ако $u \in K_{r+i}$, тогаш бројот на елементите во K_{r+i} е еднаков со индексот на нормализаторот $N(u)$ во G, па значи тој е делив со p. Нека n_i е бројот на елементите од K_{r+i}, а r бројот на елементите во $C(G)$. Тогаш за бројот на елементите во G имаме $n = r + n_1 + \ldots + n_s$ Бидејќи броевите n_i се поголеми од 1, тие се делат со p, а како индекси на подгрупите од G, тие се делители на $n = p^k$. Значи имаме

$p^k = r + p(m_1 + \ldots + m_s)$, при што $pm_i = n_i$,

од што следува дека и r се дели со p. Според тоа, $C(G)$ има барем p различни елементи.

13.5. Нека G е конечна p–група и нека $H \neq \{e\}$ е нормална подгрупа од G. Да се покаже дека $H \cap C(G)$ е неединична подгрупа од G.

Решение. Нека $h \in H$ и нека H_h е класата конјугирани елементи со h, а $N(h)$ нека е нормализаторот на h во G. Јасно е дека секој елемент од H_h е елемент и од H, т.е. $H_h \subseteq H$, бидејќи H е нормална подгрупа од G. Имајќи предвид дека две класи се или дисјунктни или еднакви, заклучуваме дека H може да се напише како дисјунктна унија од множества со облик H_h. Според 13.4, $C(G)$ има барем p елементи, а бидејќи H е p–група (како подгрупа од p–група), $C(H)$ има барем p елементи. Тоа значи дека постојат барем p класи H_h со по еден елемент и секој од тие елементи од

H му припаѓа и на $C(G)$. Според тоа, H и $C(G)$ имаат барем p заеднички елементи.

13.6. Да се покаже дека, ако простиот број p е фактор во редот на групата G и, ако постои единствена силова p–подгрупа P од G, тогаш P е нормална во G.

Решение. Нека P е силова p–подгрупа од G и нека a е елемент од G. Тогаш и $a^{-1}Pa$ е силова p–подгрупа од G, а бидејќи P е единствена, добиваме дека $a^{-1}Pa = P$. Значи, P е нормална подгрупа од G.

13.7. Да се најдат сите силови подгрупи од S_3 и S_4.

Решение. а) Групата S_3 е со ред $6 = 2 \cdot 3$. Значи, силовите подгрупи од S_3 се со ред 2 или со ред 3. Подгрупи од S_3 со ред 2 се $H_i = \{1, \sigma_i\}$, $i = 1, 2, 3$. Сите се максимални 2–подгрупи, па значи H_i се силови 2–подгрупи. Единствена 3–подгрупа од S_3 е $H = \{1, \rho_1, \rho_2\}$ којашто исто така е силова.

б) Редот на S_4 е $24 = 2^3 \cdot 3$. Ако бројот на силовите 2-подгрупи е r, тогаш $r = 1+2k$ и $r \mid 24$, од каде што добиваме $r = 1$ или $r = 3$. Ако пак, бројот на силовите 3–подгрупи е q, тогаш $q = 1+3m$ и $q \mid 24$, од каде што добиваме $q = 1$ или $q = 4$.

Бидејќи редот на A_4 е $12 = 2^2 \cdot 3$, следува дека силовите 3–подгрупи од A_4 се и силови 3–подгрупи и од S_4. Значи за да ги најдеме силовите 3–подгрупи од S_4, доволно е да ги најдеме силовите 3–подгрупи од A_4. Лесно се гледа дека ниедна силова 3–подгрупа од A_4 не содржи елемент од облик $(i\ j)\ (k\ m)$, зашто $((i\ j)\ (k\ m))^2 = 1$. Значи, ако P е силова 3–подгрупа од A_4, тогаш P може да содржи елемент од облик $(i\ j\ k)$. Така ги добиваме следниве силови 3–подгрупи од A_4 :

$P_1 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$, $P_2 = \{(1), (1\ 2\ 4), (1\ 4\ 2)\}$,
$P_3 = \{(1), (1\ 3\ 4), (1\ 4\ 3)\}$, $P_4 = \{(1), (2\ 3\ 4), (2\ 4\ 3)\}$.

За да ги најдеме силовите 2–подгрупи од S_4, доволно е да најдеме една, зашто другите се конјугирани со неа. Една силова 2–подгрупа од S_4 е:

$H_1 = \{(1), (1\ 2\ 3\ 4), (1\ 3)\ (2\ 4), (1\ 4\ 3\ 2), (1\ 4)\ (2\ 3), (1\ 2)\ (3\ 4), (1\ 3), (2\ 4)\}$

а другите две се:

$H_2 = \{(1), (1\ 2\ 4\ 3), (1\ 4)\ (3\ 2), (1\ 3\ 4\ 2), (1\ 3)\ (2\ 4), (1\ 2)\ (3\ 4), (2\ 3), (1\ 4)\}$

$H_3 = \{(1), (1\ 3\ 2\ 4), (1\ 2)(3\ 4), (1\ 4\ 2\ 3), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3), (1\ 2), (3\ 4)\}$.

13.8. Да се докаже дека секоја група со ред 15 е циклична.

Решение. Нека G е група со ред 15. Ако r е бројот на силовите 5-подгрупи, тогаш $r \equiv 1 (\mathrm{mod}\ 5)$ и $r \mid 15$. Можни се следниве случаи: $1+5k=1$, $1+5k=3$, $1+5k=5$ и $1+5k=15$. Само првата од овие четири равенки има решение и тоа е $k=0$. Значи, имаме $r=1$, т.е. постои само една силова 5–подгрупа H од G, којашто е циклична. Слично се добива дека постои единствена силова 3–подгрупа, којашто е циклична.

Затоа да ставиме $H=\{e, a, a^2, a^3, a^4\}$ и $K=\{e, b, b^2\}$. Елементот ab може да има ред 1, 3, 5 или 15. Ако $ab=e$, тогаш имаме $a=b^2 \in K$, што не е можно. Ако $(ab)^3=e$, тогаш $ab \in K$, па $ab=b$ или $ab=b^2$, од, каде што пак добиваме $a=e$ или $a=b$ што не е можно. Слично добиваме дека $(ab)^5 \neq$ е. Значи, имаме $(ab)^{15}=e$, т.е. $G=[ab]$ е циклична група.

13.9. Нека G е група со ред pq, каде што p и q се прости броеви и $p<q$. Ако H е подгрупа од G со ред q, да се покаже дека H е нормална во G.

Решение. Нека r е бројот на силовите q–подгрупи од G. Тогаш имаме $r \equiv 1 (\mathrm{mod}\ q)$ и $r \mid pq$. Од $r \mid pq$ добиваме $r=1$, или $r=p$ или $r=q$ или $r=pq$. Од $r=1+kq$ добиваме дека r не може да биде q ниту pq. Ако $r=p$ тогаш $p=1+kq$ но $p<q$, па $p=1$, што не е во согласност со условот. Значи, имаме $r=1$, т.е. постои единствена силова q-подгрупа H од G, па според 13.6, H е нормална во G.

13.10. Ако редот на групата G е pq, каде што p и q се прости броеви, $p<q$, и ако $q \neq 1+kp$ за секој $k \in \mathbb{N}$, тогаш групата G е циклична.

Решение. Според 13.9, во G постои единствена силова q–подгрупа H, којашто е нормална во G. Бројот на силовите p–подгрупи е $s=1+kp$. Можен е еден од следниве случаи: $1+kp=1$, $1+kp=p$, $1+kp=q$, или $1+kp=pq$. Случаите $1+kp=p$ и $1+kp=pq$ не се можни, па останува еден од случаите $1+kp=q$ и $1+kp=1$. Според условот на задачата, имаме $1+kp \neq q$ за секој $k \in \mathbb{N}$, па значи постои единствена силова p–подгрупа K од G, којашто е нормална во G.

Групите H и K се со прости редови, па значи тие се циклични. Затоа, нека $H=[h]$, $K=[k]$. Јасно дека $H \cap K=\{e\}$. Според 12.17, следува дека секој елемент од H комутира со секој елемент од K. Елементот hk може да има ред p, q или pq. Ако $(hk)^p=e$, тогаш,

бидејќи $hk = kh$, добиваме $e = (hk)^p = h^p k^p = h^p$ што не е можно, зашто $h^q = e$. Слично добиваме дека $(hk)^q \neq e$, па значи редот на елементот hk е pq, т.е. G е циклична група.

13.11. Ако во претходната задача $q = 1 + kp$, за некој $k \in \mathbb{N}$, тогаш групата G не мора да биде циклична.

Решение. Нека $G = S_3$. Редот на S_3 е $6 = 2 \cdot 3$, $3 = 1 + 2$ и S_3 не е циклична.

13.12. Да се покаже дека која било група со ред $p^2 q$, каде што p и q се различни прости броеви, содржи барем една нормална подгрупа.

Решение. Нека r е бројот на силовите p–подгрупи. Тогаш $r = 1 + kp$ и $r \mid p^2 q$. Бидејќи $(1 + kp, p^2) = 1$, добиваме $(1 + kp) \mid q$, т.е.

$$1 + kp = 1, \text{ или } 1 + kp = q. \tag{1}$$

Ако s е бројот на силовите q–подгрупи, тогаш $s = 1 + mq$ и $s \mid p^2 q$.

Бидејќи $(1 + mq, q) = 1$, добиваме $(1 + mq) \mid p^2$, т.е.

$$1 + mq = 1, \text{ или } 1 + mq = p \quad \text{или} \quad 1 + mq = p^2. \tag{2}$$

Простите броеви p и q се различни, па или $p < q$, или $q < p$. Ако $p < q$, тогаш од трите равенства во (2) е можно само равенството $1 + mq = 1$, т.е. постои единствена силова q–подгрупа. Ако пак $q < p$, тогаш од двете равенства во (1) е можно само равенството $1 + kp = 1$, т.е. постои единствена силова p–подгрупа.

Значи, во G постои или единствена силова p–подгрупа или единствена силова q–подгрупа, па според 13.6, во G постои барем една силова нормална подгрупа.

13.13. Ако редот на групата G е $2p$, каде што p е непарен прост број, тогаш G има една и само една подгрупа со ред p и, или G има точно p подгрупи со ред 2, или пак таа има само една подгрупа со ред 2.

Решение. Според 13.9, G има само една силова p–подгрупа, којашто е со ред p. Значи постои само една подгрупа од G со ред p. Бројот на силовите 2–подгрупи од G е $1 + 2k$ за некој цел број k, и притоа $1 + 2k = 1, 2, p$ или $2p$. Бидејќи 2 не го дели $1 + 2k$, ќе имаме $1 + 2k = 1$ или $1 + 2k = p$, па значи бројот на силовите 2-подгрупи е 1 или p.

13.14. Да се покаже дека, ако G е група со ред 200 тогаш во G постои барем една нормална силова подгрупа.

Решение. Бидејќи $200 = 2^3 \cdot 5^2$, да ги побараме силовите 2–подгрупи и силовите 5–подгрупи од G.

Нека r е бројот на силовите 5–подгрупи од G. Тогаш имаме $r = 1 + 5k$ и $r \mid 200$. Делителите на 200, $\neq 1$, се: 2, 4, 8, 5, 25, 10, 20, 40, 50, 100 и 200. Ни еден од овие броеви не е од облик $1+5k$, па значи постои единствена силова 5–подгрупа од G. Според 13.6, таа е нормална во G.

13.15. Во група со ред 50 постои барем една нормална подгрупа.

13.16. Ако G е група со ред 48, тогаш таа има барем една вистинска нормална подгрупа.

Решение. Бидејќи $48 = 2^4 \cdot 3$, групата G содржи силова 2-подгрупа, којашто е со ред 16. Ако бројот на силовите 2-подгрупи е r, тогаш $r = 1 + 2k$ и $r \mid 48$, од каде што добиваме $r = 1$ или $r = 3$. Ако $r = 1$, тогаш G има единствена силова 2–подгрупа, којашто, според 13.6, е нормална. Затоа, да претпоставиме дека $r = 3$. Нека H и K се две такви силови 2–подгрупи. Групата $H \cap K$ е вистинска подгрупа од H и нејзиниот ред n е фактор во 16. Можни се следниве случаи: $n = 2$, $n = 4$, или $n = 8$. Ако $n \leq 4$, тогаш имаме

$$|H||K|/n \geq 16 \cdot 16 / 4 = 64.$$

Но, редот на G е 48, па останува случајот $n = 8$. Значи, $H \cap K$ е со индекс 2 и во H и во K, па значи, таа е нормална и во H и во K. Нека $L = N(H \cap K)$. Тогаш имаме

$|L| \geq |HK| = |H|\,|K| / |H \cap K| = 32$.

Од ова следува дека $|L| = 48$, т.е. $L = G$. Но, секоја подгрупа е нормална во својот нормализатор, па значи $H \cap K$ е нормална во G.

§14. НОРМАЛНИ НИЗИ

14.1. За кои било елементи x, y од групата G важи равенството
$$xy = yx\,[x, y],$$
каде што $[x, y] = x^{-1} y^{-1} xy$ е *комутатор* на x и y.

Решение. $yx[x, y] = yx\,(x^{-1} y^{-1} xy) = yxx^{-1} y^{-1} xy = xy.$

14.2. Ако G е група тогаш
$(\forall x, y \in G)\ [x, y] = e \Leftrightarrow G$ е комутативна.

Решение. Нека x и y се произвилни елементи од групата G. Од $[x, y] = e$, добиваме $x^{-1} y^{-1} xy = e$, т.е. $xy = yx$. Значи, групата G е комутативна. Обратно е јасно.

14.3. Во симетричната група S_4, за елементите
$x = (1\ 2),\quad y = (1\ 2\ 3),\ z = (1\ 2\ 3\ 4),\ u = (1\ 3)\ (2\ 4),$
да се најдат комутаторите $[x, y]$, $[x, z]$, $[x, u]$, $[y, x]$, $[z, x]$ и $[u, x]$.

Решение. Имаме:
$[x, y] = x^{-1} y^{-1} xy = (1\ 2)\ (1\ 3\ 2)\ (1\ 2)\ (1\ 2\ 3) = (1\ 3\ 2).$
$[y, x] = y^{-1} x^{-1} yx = (1\ 3\ 2)\ (1\ 2)\ (1\ 2\ 3)\ (1\ 2) = (1\ 2\ 3).$
Слично, добиваме и:
$[x, z] = (1\ 4\ 2)$, $[x, u] = (1\ 2)\ (3\ 4)$, $[z, x] = (1\ 2\ 4)$, $[u, x] = (1\ 2)\ (3\ 4).$

14.4. Во групата матрици,
$$G = \left\{ \begin{bmatrix} x & y \\ u & v \end{bmatrix} \;\middle|\; x, y, u, v \in \mathbb{Z},\ \begin{vmatrix} x & y \\ u & v \end{vmatrix} = \pm 1 \right\},$$
да се најдат комутаторите $[A, B]$, $[B, C]$, $[C, A]$, ако
$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \qquad B = \begin{bmatrix} 1 & 2 \\ -1 & -1 \end{bmatrix}, \qquad C = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Одговор. $[A, B] = \begin{bmatrix} 7 & 4 \\ -2 & -1 \end{bmatrix}$, $[B, C] = \begin{bmatrix} 5 & -3 \\ -3 & 2 \end{bmatrix}$, $[C, A] = \begin{bmatrix} 1 & 2 \\ 2 & 5 \end{bmatrix}$.

14.5. Во групата на несингуларни матрици од трет ред, да се најдат комутаторите $[X, Y]$, $[Y, Z]$, $[Z, X]$, каде што

$$X=\begin{bmatrix}1&0&0\\0&2&0\\0&0&3\end{bmatrix},\qquad Y=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix},\qquad Z=\begin{bmatrix}0&0&1\\0&2&0\\3&0&0\end{bmatrix}.$$

Решение. $\begin{bmatrix}1&-1&-1\\0&1&-\frac{1}{2}\\0&0&1\end{bmatrix}$, $\begin{bmatrix}-\frac{1}{2}&-1&0\\-\frac{3}{2}&-1&-1\\3&2&1\end{bmatrix}$, $\begin{bmatrix}\frac{1}{3}&0&0\\0&1&0\\0&0&3\end{bmatrix}$.

14.6. Во симетричната група S_n $(n \geq 5)$,за циклусите $\alpha = (l\ k\ j)$ и $\beta = (i\ j\ m)$ да се најде комутаторот $[\alpha, \beta]$, каде што i, j, k, l, m се меѓусебно различни броеви.

Одговор. $(i\ j\ k)$.

14.7. Кои елементи во кватернионската група K (6.6) се комутанти?

Одговор. $-1, 1$.

14.8. Да се најде комутантот (изводот) D_4' на диедралната група D_4.

Решение. Бидејќи $b_i^{-1} = b_i$ (види 10.8), а $b_i * b_j = a_{i-j}$, добиваме

$[b_i, b_j] = b_i * b_j * b_i * b_j = a_{i-j} * a_{i-j} = a_{2(i-j)}$, т.е. $[b_i, b_j]$ е a_0 или a_2. Елементите со облик a_i, a_j комутираат, па $[a_i, a_j] = a_0$. Значи, имаме $D_4' = H_1 = \{a_0, a_2\}$.

14.9. Да се најде комутантот K' на кватернионската група K (6.6).

Одговор. $K' = \{1, -1\}$.

14.10. Да се покаже дека комутантот на групата од сите квадратни матрици од втор ред е подгрупата матрици со детерминанта +1.

14.11. Да се најде комутантот на симетричната група S_n.

Решение. Бидејќи групата S_2 е комутативна, добиваме дека $S_2' = E$. Нека $n > 2$ и нека $\alpha, \beta \in S_n$. Ако α и β ги напишеме како производ од транспозиции, лесно се заклучува дека пермутацијата $[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$ е парна, а тоа значи дека $S_n' \subseteq A_n$.

За секој циклус $(i\ j\ k)$ со должина 3 имаме:
$(i\ j\ k) = (i\ k)\ (i\ j)\ (i\ k)\ (i\ j) = [(i\ k), (i\ j)]$.
Но, секоја парна пермутација може да се напише како производ од циклуси со должина 3, па значи имаме $A_n \subseteq S_n'$.
Од сето тоа следува дека $S_n' = A_n$.

14.12. Да се докаже дека групата од сите транслации во рамнина е комутант на групата од сите транслации и сите ротации во рамнината.

14.13. Нека за групата G комутантот G' се содржи во центарот $C(G)$. Да се покаже дека за кои било $x, y, z \in G$ се точни равенствата:

а) $[xy, z] = [x, z]\ [y, z]$;

б) $[x, yz] = [x, y]\ [x, z]$;

в) $[x^n, y] = [x, y^n] = [x, y]^n$;

г) $(xy)^n = x^n\ y^n\ [y, x]^{n\ (n-1)/2}$;

д) $[x, [y, z]]\ [y, [z, x]]\ [z, [x, y]] = e$.

14.14. Ако за групата G редот на комутантот G' е 2, тогаш $G' \subseteq C(G)$.

Решение. Нека G е група, таква што комутантот G' е со ред 2.
Затоа, нека $G' = \{e, a\}$. За да покажеме дека $G' \subseteq C(G)$, треба да покажеме дека $ax = xa$ за секој $x \in G$. Комутаторот $[a, x]$ може да биде e, или a. Ако $[a, x] = a$, тогаш имаме $a^{-1} x^{-1} ax = a$, т.е. $ax = x$ што не е можно. Значи, имаме $[a, x] = e$, т.е. $ax = xa$.

14.15. Да се определат сите композициони низи на:

а) цикличната група C_{12};

б) кватернионската група K ;

в) симетричната група S_n, $n = 2, 3, 4, 5$.

Решение. а) Подгрупи од $C_{12} = [a]$ се: E, $A_1 = [a^2]$, $A_2 = [a^3]$, $A_3 = [a^4]$, $A_4 = [a^6]$ и C_{12}. Подгрупите A_1 и A_2 се максимални во C_{12}; подгрупите A_3 и A_4 се максимални во A_1; подгрупата A_4 е максимална и во A_2. Според тоа, композиционите низи на C_{12} се:
$C_{12} \supset A_1 \supset A_3 \supset E$, $C_{12} \supset A_1 \supset A_4 \supset E$, $C_{12} \supset A_2 \supset A_4 \supset E$.
б) Подгрупи од кватернионската група K се: $H = \{1, -1\}$, $K_1 = \{1, -1, i, -i\}$, $K_2 = \{1, -1, j, -j\}$, $K_3 = \{1, -1, k, -k\}$ и сите се нормални подгрупи од K. Композиционите низи на K се:

$K \supset K_1 \supset H \supset E, \quad K \supset K_2 \supset H \supset E, \quad K \supset K_3 \supset H \supset E.$

в) Групата S_2 има само една композициона низа и тоа $S_2 \supset E$.

Групата S_3, исто така, има само една композициона низа $S_3 \supset A_3 \supset E$.

Групата S_4 има само една нормална подгрупа A_4.

Групата A_4 има само една нормална подгрупа (види 12.7) и тоа $K_4 = \{(1), (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$. Групата K_4 има три нормални подгрупи (види 11.20) и тоа:

$H_1 = \{(1), (1\ 2)(3\ 4)\}$, $H_2 = \{(1), (1\ 3)\ (2\ 4)\}$ и $H_3 = \{(1), (1\ 4)\ (2\ 3)\}$.

Според тоа, групата S_4 има три композициони низи и тоа:

$S_4 \supset A_4 \supset K_4 \supset H_i \supset E, \quad i = 1, 2, 3.$

Групата S_5 има само една композициона низа $S_5 \supset A_5 \supset E$.

14.16. Нека групата G има композициона низа и нека H е нормална подгрупа од G. Да се покаже дека H е член на некоја композициона низа.

Решение. Низата $G \supset H \supset E$ е нормална, па проширувајќи ја до композициона, а таква барем една постои, следува дека H е член на композициона низа.

14.17. Нека $f: G \to S$ е хомоморфизам од групата G во групата S и нека

$$S = S_0 \supseteq S_1 \supseteq \ldots \supseteq S_m \supseteq E, \tag{1}$$

е нормална низа во S. Ако $G_i = f^{-1}(S_i)$, $i = 1, \ldots, m$, да се покаже дека

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m \supseteq E \tag{2}$$

е нормална низа во G.

Упатство. Да се искористи 12.38.

14.18. За една нормална низа велиме дека е *циклична*, ако сите членови на соодветната факторна низа се циклични групи. Да се покаже дека, ако нормалната низа (1), од 14.17, е циклична, тогаш и нормалната низа (2) е циклична.

14.19. Нека G и S се две групи со својството да постојат две изоморфни низи:

$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_k \supseteq E, \quad S = S_0 \supseteq S_1 \supseteq \ldots \supseteq S_k \supseteq E.$

Дали групите G и S мора да се изоморфни?

Решение. Групите G и S не мора да се изоморфни. На пример, нека $G = K$ е кватернионската група, $S = D_4$ е диедралната група. Факторите на нормалната низа

$$K \supset K_1 \supset H \supset E, \tag{1}$$

$K_1 = \{1, -1, i, -i\}$, $H = \{1, -1\}$, се циклични групи со ред 2. Исто така, факторите на нормалната низа

$$D_4 \supset H_7 \supset H_1 \supset E, \tag{2}$$

$H_7 = \{a_0, a_2, b_0, b_2\}$, $H_1 = \{a_0, a_1\}$, се циклични групи со ред 2. Значи, нормалните низи (1) и (2) се изоморфни, но групите K и D_4 не се изоморфни.

14.20. Да се провери дали диедралната група D_4 е решлива.

Решение. Според 14.8, имаме $D_4' = H_1 = \{a_0, a_1\}$. Но H_1 е комутативна, па $H_1' = E$. Значи, имаме $D_4'' = E$, т.е. групата D_4 е решлива.

14.21. Дали групата K од кватерниони е решлива?

Решение. Според 14.9, имаме $K' = H = \{1, -1\}$. Но, H е комутативна, па $H' = K'' = E$. Значи, групата K е решлива.

14.22. Да се покаже дека симетричната група S_n, $n = 2, 3, 4$, е решлива.

Решение. Групата S_2 е комутативна, па значи и решлива. За групата S_3 имаме $S_3' = A_3$, $A_3' = E$, па значи и таа е решлива. За групата S_4 имаме $S'_4 = A_4$, $A'_4 = K_4 = \{(1), (1\ 2)\ (3\ 4), (1\ 3)\ (2\ 4), (1\ 4)\ (2\ 3)\}$, $K' = E$, па значи и S_4 е решлива.

14.23. Да се покаже дека симетричната група S_n, $n \geq 5$, не е решлива.

Решение. Според 14.11, имаме $S_n' = A_n$. Бидејќи A_n, $n \geq 5$, е проста група, а A'_n е нормална подгрупа од A_n, имаме $A'_n = E$ или $A'_n = A_n$. Но, A_n не е комутативна, па $A'_n \neq E$, т.е. $A'_n = A_n$. Значи, групата S_n, $n \geq 5$, не е решлива.

14.24. За кои n групата A_n е решлива?

Одговор. $n = 1, 2, 3, 4$.

14.25. За една нормална низа велиме дека е *абелова* ако факторите на таа низа се абелови. Да се покаже дека:

а) ако низата (1) од 14.17 е абелова, тогаш и низата (2) е абелова.

б) секоја абелова нормална низа од една конечна група има циклично проширување.

Решение. б) Доказот ќе го спроведеме, вршејќи индукција по редот на групата. Ако редот на групата G е 1, 2 или 3, тогаш G има само една нормална низа $G \supset E$, којашто е циклична. Да претпоста-

виме дека редот на групата G е n и дека тврдењето е точно за секоја група со ред m, $m = 1, 2,\ldots, n-1$. За да покажеме дека тврдењето е точно и за групата G со ред n, ќе разгледаме два случаја.

(i) Групата G е комутатива. Нормалната низа $G \supset E$ е абелова.

Ако $a \in G$, $a \neq e$, тогаш и низата $G \supset [a] \supset E$ е абелова, при што $[a]/E$ е циклична. Групата $G / [a]$ е со помал ред n, па значи низата $G / [a] \supset [a] / [a]$ има циклично проширување.

$G / [a] \supset G_1 / [a] \supset \ldots \supset G_r / [a] = [a] / [a]$.

Бидејќи групата $(G_i / [a]) / (G_{i+1} / [a])$ е изоморфна со групата G_i / G_{i+1}, низата

$G \supset G_1 \supset \ldots \supset G_r = [a] \supset E$

е циклична и е проширување на низата $G \supset E$.

(ii) Ако групата G е некомутативна, да ја разгледаме абеловата низа

$$G \supset A_1 \supset A_2 \supset \ldots \supset A_s = E. \qquad (1)$$

Бидејќи групата G / A_1 и A_1 се со помали редови од n, според индуктивната претпоставка, абеловите низи:

$G / A_1 \supset A_1 / A_1$; $\quad A_1 \supset A_2 \supset \ldots \supset A_s = E$

имаат циклични проширувања

$G / A_1 \supset G_1 / A_1 \supset \ldots \supset G_r / A_1 = A_1 / A_1$,

$A_1 \supset B_1 \supset B_2 \supset \ldots \supset B_m = E$.

Но, тогаш нормалната низа

$G \supset G_1 \supset \ldots \supset G_r \supset B_1 \supset B_2 \supset \ldots \supset B_m = E$

е циклично проширување на абеловата низа (1).

14.26. Да се покаже дека една конечна група е решлива ако и само ако за неа постои циклична нормална низа.

Решение. Нека конечната група G е решлива. Тогаш за G постои абелова нормална низа, којашто, (според 14.25 б) има циклично проширување. Значи, ако конечната група G е решлива, тогаш за неа постои циклична нормална низа.

Обратно, нека за конечната група G постои циклична нормална низа. Бидејќи секоја циклична нормална низа е и абелова, следува дека групата G е и решлива.

14.27. Нека за групата G постои нормална подгрупа H, таква што групите H и G / H се решливи. Да се покаже дека и групата G е решлива.

Решение. Нека за групата G постои нормална подгрупа H, таква што групите H и G / H се решливи. Бидејќи H е решлива, постои нормална низа

$$H = B_1 \supseteq \ldots \supseteq B_s = E,$$

така што групите B_i / B_{i+1} се комутативни. Исто така бидејќи групата G / H е решлива, постои нормална низа

$$G / H = A_1 / H \supseteq \ldots \supseteq A_r / H = H / H,$$

така што групите $(A_i / H) / (A_{i+1} / H)$ се комутативни. Но, групите A_i / A_{i+1} и $(A_i / H) / (A_{i+1} / H)$ се изоморфни, па значи нормалната низа

$$G = A_1 \supseteq \ldots \supseteq A_r = B_1 \supseteq \ldots \supseteq B_s = E$$

е абелова, т.е. групата G е решлива.

14.28. Да се покаже дека секоја конечна група со ред pq, каде што p и q се прости броеви, е решлива.

Решение. Нека G е група со ред pq. Ако p и q се различни прости броеви, на пример $p< q$, тогаш во G постои единствена силова q–подгрупа H од G, па таа е и нормална подгрупа од G (види 13.9). Бидејќи H е со прост ред, H е циклична група. Групата G / H е со ред p, па значи и таа е циклична. Значи групите H и G / H, како комутативни, се решливи па според 14.27, и групата G е решлива.

Ако пак $p = q$, т.е. групата G е со ред p^2, тогаш таа е комутативна, па значи и решлива.

14.29. Да се покаже дека секоја група со ред p^2q, каде што p и q се различни прости броеви, е решлива.

Решение. Според 13.12, во G постои барем една нормална подгрупа H и тоа, ако $p< q$, тогаш H е со ред q, а ако $p> q$, тогаш H е со ред p^2. Ако H е со ред q, тогаш G / H е со ред p^2, а ако H е со ред p^2, тогаш G / H е со ред q. Значи, во секој случај групите H и G / H се реш-ливи, па според 14.27, и групата G е решлива.

14.30. Да се покаже дека секоја конечна p–група е решлива.

Решение. Нека G е конечна p–група. Тогаш G е со ред p^n за некој $n \in \mathbb{N}$. Според 13.2, за секој $k : 0 \leq k \leq n$, постои нормална подгрупа H_k од G со ред p^k и притоа имаме

$$G = H_n \supset H_{n-1} \supset \ldots \supset H_1 \supset H_0 = E. \qquad (1)$$

Бидејќи групата H_{k+1} / H_k, $k = 0, 1,\ldots, n-1$, е со ред p, таа е циклична, па значи нормалната низа (1) е циклична. Според 14.26, добиваме дека групата G е решлива.

14.31. Да се покаже дека секоја група со ред 275 е решлива.

14.32. Да се покаже дека секоја група со ред 100 е решлива.

14.33. Во множеството $G = \{a_i \mid i \in \mathbb{Z}\}$, определена е операција "$*$" со:

$$a_i * a_j = \begin{cases} a_{i+j} & \text{ако } i \text{ е парен,} \\ a_{i-j} & \text{ако } i \text{ е непарен.} \end{cases}$$

Да се покаже дека $G(*)$ е група, а потоа дека таа група е решлива.

14.34. Ако A, B, C, D се подгрупи од групата G, тогаш
$A \subseteq C, B \subseteq D \Rightarrow [A, B] \subseteq [C, D]$.

14.35. Да се покаже дека секоја подгрупа, а и секоја фактор–група од една нилпотентна група е нилпотентна.

Решение. Нека групата G е нилпотентна и H подгрупа од G. Бидејќи групата G е нилпотентна, постои природен број k, така што во низата

$G_0 = G, G_1, G_2, \ldots, G_n, \ldots,$

$G_k = E$, каде што $G_{n+1} = [G_n, G]$. Да ја формираме низата

$H_0 = H, H_1, H_2, \ldots, H_n, \ldots,$

каде што $H_{n+1} = [H_n, H]$. Бидејќи H е подгрупа од G, имаме $H_1 = [H, H] \subseteq [G, G] = G_1$.

Понатаму, од $H_1 \subseteq G_1$, добиваме $H_2 = [H_1, H] \subseteq [G_1, G] = G_2$.

Продолжувајќи така добиваме дека $H_k \subseteq G_k$, т.е. $H_k = E$. Значи, подгрупата H е нилпотентна.

За да покажеме дека фактор–групата G / H е нилпотентна, доволно е да покажеме дека секоја хомоморфна слика од нилпотентна група е нилпотентна. Затоа, нека групата G е нилпотентна и нека $f: G \to \overline{G}$ е епиморфизам. Бидејќи групата G е нилпотентна, постои нормална низа

$G = A_0 \supset A_1 \supset \ldots \supset A_s = E,$

таква што $[A_i, G] \subseteq A_{i+1}$. Да ставиме $f(A_i) = \overline{A}_i$, $i = 0,1, \ldots, s$. На тој начин ја добиваме нормалната низа

$\overline{G} = \overline{A}_0 \supset \overline{A}_1 \supset \ldots \supset \overline{A}_s = \overline{E}$.

Ако $\overline{a}_i \in \overline{A_i}$, $\overline{x} \in \overline{G}$, тогаш постојат елементи $a_i \in A_i$ и $x \in G$, такви што $f(a_i) = \overline{a}_i$, $f(x) = \overline{x}$. Бидејќи $[a_i, x] \in A_{i+1}$, имаме

$$[\overline{a}_i, \overline{x}] = f([a_i, x]) \in \overline{A}_{i+1}, \text{ т.е. } [\overline{A_i}, \overline{G}] \subseteq A_{i+1}.$$

Значи, групата $\overline{G}$ исто така е нилпотентна.

14.36. Дали групата S_n, $n \geq 2$, е нилпотентна ?

Решение. Бидејќи групата S_n, $n \geq 5$, не е решлива, а секоја нилпотентна група е решлива, следува дека групата S_n, $n \geq 5$, не е нилпотентна. Групата S_2 е комутативна, па значи и нилпотентна. За групата S_3 имаме $S_3' = A_3$. Бидејќи $\rho_1^{-1}\sigma_1^{-1}\rho_1\sigma_1 = \rho_2\sigma_1\rho_1\sigma_1 = \rho_1 \in [A_3, S_3]$, следува дека $[A_3, S_3] = A_3$. Според тоа, групата S_3 не е нилпотентна. Покажувајќи, на ист начин, дека $[A_4, S_4] = A_4$, заклучуваме дека и S_4 не е нилпотентна.

14.37. Нека комутантот G' на групата G се содржи во центарот $C(G)$. Да се покаже дека групата G е нилпотентна.

Решение. Нека комутантот G' на групата G се содржи во центарот $C(G)$. Тогаш елементите на G' комутираат со секој елемент од G, па $G_2 = [G', G] = \{a^{-1}b^{-1}ab \mid a \in G', b \in G\} = \{b^{-1}a^{-1}ab \mid a \in G', b \in G\} = E$, т.е. групата G е нилпотентна.

14.38. Нека H е подгрупа од центарот $C(G)$ на групата G. Ако G / H е нилпотентна, тогаш и G е нилпотентна.

Решение. Бидејќи G / H е нилпотентна, постои природен број k, така што $(G / H)_k = [(G / H)_{k-1}, G / H] = H$. Но, тоа значи дека $G_k = [G_{k-1}, G] \subseteq H$, па бидејќи H, како подгрупа од $C(G)$, е комутативна, имаме $G_{k+1} = [G_k, G] \subseteq [H, G] = E$. Значи, групата G е нилпотентна.

14.39. Да се покаже дека секоја конечна p–група е нилпотентна.

Решение. Нека G е конечна p–група, на пример, со ред p^n. Доказот ќе го спроведеме со индукција по n. За $n = 1$, групата G е комутативна, па значи и нилпотентна. Да препоставиме дека секоја p–група се ред p^m, $m = 1, \ldots, n-1$, е нилпотентна. Центарот $C(G)$, според 13. 4, е неединична подгрупа од G, и фактор–групата $G / C(G)$ е p–група со ред p^k, $k < n$. Според индуктивната претпоставка $G / C(G)$ е нилпотентна, па според 14.38, и групата G е нилпотентна.

14.40. Да се докаже дека кватернионската група K (6.6) е нилпотентна.

14.41. Да се докаже дека диедралната група D_4 е нилпотентна.

14.42. За кои n, диедралната група D_n е нилпотентна?

Одговор. За $n = 2^k$.

§ 15. ВНАТРЕШНИ ДИРЕКТНИ ПРОИЗВОДИ

15.1. Нека G е мултипликативната група на ненултите комплексни броеви,

$H = \{x \mid x \in G,\ |x| = 1\}$ и $K = \mathbb{R}^+$.

Да се покаже дека $G = H \otimes K$.

Решение. Ако $z \in G$, тогаш $|z| \in K$, $\frac{z}{|z|} \in H$ и имаме $z = |z| \frac{z}{|z|}$. Бидејќи $H \cap K = \{1\}$, следува дека $G = H \otimes K$.

15.2. Нека G е група. Да се покаже дека:

а) $G = E \otimes G \quad (E = \{e\})$;

б) $G = A \otimes B \otimes C = A \otimes B \Rightarrow C = E = \{e\}$.

Решение. а) Имаме $x = ex$ за секој $x \in G$ и $E \cap G = \{e\}$, па значи $G = E \otimes G$.

б) Нека $G = A \otimes B \otimes C = A \otimes B$. Од $G = A \otimes B \otimes C$ следува дека $G = ABC$ и $C \cap AB = \{e\}$, а од $G = A \otimes B$ следува $G = AB$, па значи имаме $C \cap G = \{e\}$, т.е. $C = \{e\}$.

15.3. За една подгрупа H од G велиме дека е *директен фактор* на G, ако постои подгрупа K од G, таква што $G = K \otimes H$. Да се определат сите директни фактори на групите: C_4, C_6, C_8, C_{10} и S_4.

Решение. Бидејќи за секоја група G имаме $G = E \otimes G$, при што $E = \{e\}$, следува дека E и G се директни фактори за секоја група G. Затоа, ќе ги бараме само оние директни фактори што претставуваат нетривијални подгрупи.

Групата $C_4 = [a]$, има само една нетривијална подгрупа $H = [a^2]$, па значи C_4 нема директни фактори, различни од E и C_4.

Групата $C_6 = [a]$, има две нетривијални подгрупи $H = \{e, a^2, a^4\}$ и $K = \{e, a^3\}$ и имаме $HK = G$, $H \cap K = \{e\}$. Значи, директни фактори, различни од E и G, се H и K.

Групата $C_8 = [a]$ има две нетривијални подгрупи, $K = \{e, a^4\}$ и $H = \{e, a^2, a^4, a^6\}$. Бидејќи $K \subset H$, следува дека C_8 нема директни фактори, различни од E и C_8.

За групата C_{10} директни фактори се $H = \{e, a^2, a^4, a^6, a^8\}$ и $K = \{e, a^5\}$, а групата S_4 нема дирекни фактори, различни од E и S_4.

15.4. За една група G велиме дека е *неразложлива*, ако од $G = H \otimes K$ следува $H = E$ или $K = E$. Која од групите C_{21}, C_{p^n} (p–прост број), $\mathbb{Z}(+)$ и $\mathbb{Q}(+)$ е неразложлива?

Решение. Ако $C_{21}=[a]$, тогаш $C_3=\{e, a^7, a^{14}\}$ и $C_7=\{e, a^3, a^6, a^9, a^{12}, a^{15}, a^{18}\}$ се подгрупи од C_{21} при што $C_7C_3 = C_{21}$ и $C_7 \cap C_3 = \{e\}$. Значи, имаме $C_{21} = C_3 \otimes C_7$, т.е. C_{21} е разложлива.

Ако $C_{p^n} = [a]$, тогаш секоја нејзина подгрупа е циклична, па затоа нека $[a^{p^r}]$ и $[a^{p^s}]$ се кои било две подгрупи. Можеме да претпоставиме дека $r < s$. Тогаш имаме:

$$a^{p^s} = (a^{p^r})^{ps-r} \in [a^{p^r}],$$

т.е. $[a^{p^r}] \bigcap [a^{p^s}] \neq \{e\}$. Значи, групата C_{p^n} е неразложлива.

Подгрупите од групата $\mathbb{Z}(+)$, се од облик $m\mathbb{Z}$, па ако $m\mathbb{Z}$ и $n\mathbb{Z}$ се две подгрупи од $\mathbb{Z}(+)$, тогаш $m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z} \neq \{0\}$, т.е. групата $\mathbb{Z}(+)$ е неразложлива.

Да покажеме уште и дека $\mathbb{Q}(+)$ е неразложлива група. За таа цел да претпоставиме дека A и B се две подгрупи од $\mathbb{Q}(+)$, при што секоја од нив има и ненулти елементи.

Ако $\frac{m}{n} \in A$, $\frac{r}{s} \in B$ и $\frac{m}{n}\frac{r}{s} \neq 0$, тогаш $(nr)\frac{m}{n} = (sm)\frac{r}{s} \in A \cap B$, од што и следува заклучокот дека $\mathbb{Q}(+)$ е неразложлива група, бидејќи во пресекот $A \cap B$ на кои било две ненулти подгрупи постои ненулти елемент.

15.5. Нека $G = H \otimes K$, а S е нормална подгрупа од G. Да се покаже дека еден од следниве услови е исполнет:

(i) S е комутативна;

(ii) $S \cap (H \cup K) \neq \{e\}$.

Решение. Ќе покажеме дека, ако не е исполнет условот (ii), т.е. ако $S \cap (H \cup K) = \{e\}$, тогаш подгрупата S е комутативна.

Од $S \cap (H \cup K) = (S \cap H) \cup (S \cap K) = \{e\}$, следува $S \cap H = \{e\}$ и $S \cap K = \{e\}$. Но, според 12.17, добиваме дека секој елемент од S комутира со секој елемент од K.

Ако $x, y \in S$, тогаш од $G = H \otimes K$, следува $x = h_1 k_1$ и $y = h_2 k_2$, па имаме:

$$xy = h_1 k_1 y = h_1 y k_1 = y h_1 k_1 = yx,$$

т.е. подгрупата S е комутативна.

15.6. Нека $G = \{e, a, a^2, a^3\} \times \{e, b, b^2, b^3\}$. Да се најдат сите хомоморфизми од G во цикличната група $C_8 = \{e, c, c^2, \ldots, c^7\}$.

Решение. Можеме да претпоставиме дека

$$G = \{e, a, a^2, a^3, b, b^2, b^3, ab, ab^2, ab^3, a^2b, a^2b^2, a^2b^3, a^3b, a^3b^2, a^3b^3\}$$

каде што $a^4 = b^4 = e$. Нека $f = G \to C_8$ е еден хомоморфизам, при што $f(a) = c^r$, $f(b) = c^s$. Ако се има предвид дека a и b имаат ред 4, добиваме дека редовите на c^r, c^s се делители на 4 (види 12.28). Според тоа, можни се следниве случаи: $r = 0, 2, 4, 6$ и $s = 0, 2, 4, 6$, т.е. r, s се парни. Да ставиме $r = 2m$, $s = 2n$. Тогаш имаме:

$$f(a^i b^j) = c^{2im} c^{2nj} = (c^2)^{im+jn}. \qquad (1)$$

Обратно, ако f се определи со (1), добиваме хомоморфизам. Бидејќи постојат 16 елементи $(m, n) \in \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$ заклучуваме дека постојат 16 хомоморфизми од G во C_8. Тие хомоморфизми се:

$$f_{00}(a^i b^j) = e, \quad f_{01}(a^i b^j) = c^{2j}, \quad f_{02}(a^i b^j) = c^{4j}, \ldots$$

и, воопшто, $f_{mn}(a^i b^j) = (c^2)^{im+jn}$, $(m,n) \in \{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$.

15.7. Да се даде пример на група $G = A \otimes B$ и нормална подгрупа H, така што $H \neq (H \cap A) \otimes (H \cap B)$.

Решение. Ако G е групата од 15.6, тогаш, ставајќи

$$A = \{e, a, a^2, e^3\}, \qquad B = \{e, b, b^2, b^3\}, \qquad H = \{e, a^2b^2\},$$

добиваме $G = A \otimes B$, $H \cap A = \{e\} = H \cap B$, $H \neq (H \cap A) \otimes (H \cap B)$.

15.8. Нека $G = A \otimes B \otimes C \otimes D \otimes F$ и $H = AB$, $K = CDF$. Да се покаже дека $G = H \otimes K$ и да се обопшти овој резултат.

Решение. Од $G = A \otimes B \otimes C \otimes D \otimes F$ следува дека кој било елемент $x \in G$ може на единствен начин да се претстави како производ $x = abcdf$, $a \in A, \ldots, f \in F$. Да ставиме $ab = h$, $cdf = k$. Тогаш x е претставен на единствен начин како производ $x = hk$, па според тоа G е директен производ од H и K.

Нека $G = A_1 \otimes \ldots \otimes A_n$. Ако ставиме

$H = A_1 \otimes \ldots \otimes A_m$, $K = A_{m+1} \otimes \ldots \otimes A_n$, тогаш $G = H \otimes K$.

15.9. Нека H и K се две подгрупи од G, такви што

$$(\forall h \in H, \ k \in K) \quad hk = kh. \qquad (1)$$

Да се покаже дека:

а) $KH = K \otimes H \Leftrightarrow |KH| = |K|\,|H|$.

б) $(|K|, |H|) = 1 \Rightarrow KH = K \otimes H$.

Решение. Да забележиме прво дека од (1) следува $KH = HK$, па значи KH е подгрупа од G и притоа $H \lhd KH$, $K \lhd KH$.

а) Нека $KH = K \otimes H$; тоа значи дека $K \cap H = \{e\}$, па од

$$|KH| = \frac{|K||H|}{|K \cap H|}, \tag{2}$$

следува $|KH| = |K||H|$.

Обратно, ако $|KH| = |K||H|$, тогаш од (2) следува дека $|K \cap H| = 1$, т.е. $K \cap H = \{e\}$, што значи $KH = K \otimes H$.

б) Нека $|K|$ и $|H|$ се заемно прости, т.е. $(|K|, |H|) = 1$.

За да покажеме дека $KH = K \otimes H$, доволно е да покажеме дека $K \cap H = \{e\}$.

Ако $x \in K \cap H$, тогаш редот на x е фактор во $|K|$ и $|H|$, а бидејќи $(|K|, |H|) = 1$ следува дека редот на x е 1, т.е. $x = e$.

15.10. Да се покаже дека групите $C_n \times C_n$ и C_{n^2} не се изоморфни за кој било природен број $n > 1$.

Решение. Во $C_n \times C_n$ редот на секој елемент е делител на n, додека во C_{n^2} има елемент со ред n^2.

15.11. Ако C_m и C_n се циклични групи со ред m и n соодветно при што $(m, n) = 1$, тогаш групата $C_m \times C_n$ е изоморфна со цикличната група C_{mn}, којашто има ред mn.

Решение. Ако a е генератор на C_m, а b на C_n, тогаш елементот $(a, b) \in C_m \times C_n$ има ред mn, па значи $C_m \times C_n$ е циклична група со ред mn. Но, циклични групи со ист ред се изоморфни, па следува дека $C_m \times C_n$ е изоморфна со C_{mn}.

15.12. Да се покаже дека за кој било прост број p постојат само две неизоморфни групи со ред p^2.

Решение. Знаеме дека секоја група со ред p^2 е абелова. Според претходната задача, групите C_{p^2} и $C_p \times C_p$ се со ред p^2 и тие не се изоморфни. Значи, постојат барем две неизоморфни групи со ред p^2.

Нека G е која било група со ред p^2; G има подгрупа H со ред p, па таа е циклична. Ако $a \in H$, тогаш редот на a е или p, или p^2. Ако редот на a е p^2, тогаш $G = [a] = C_{p^2}$. Ако пак редот на a е p,

тогаш $[a] \cap H = \{e\}$. Подгрупите H и $[a]$ се нормални во G и $|[a]| \cdot |H| = |G|$. Одовде следува дека $G \cong [a] \times H = C_P \times C_P$.

Значи, $G = C_{p^2}$ или $G = C_P \times C_P$.

15.13. Да се покаже дека постојат само три комутативни групи со ред 8.

Решение. Јасно е дека постојат барем три неизоморфни групи со ред 8 и тоа C_8, $C_2 \times C_4$ и $C_2 \times K_4$, каде што C_n е циклична група со ред n, а K_4 е клајновата група со ред 4. Ако G е комутативна група со ред 8, ќе покажеме дека G е изоморфна со една од групите C_8, $C_2 \times C_4$, $C_2 \times K_4$.

Ако во G постои елемент со ред 8, тогаш G е циклична, па G е изоморфна со C_8.

Да препоставиме дека во G нема елемент со ред 8, но има елемент a со ред 4. Нека $H = [a]$. Во $G \setminus H$ постои барем еден елемент b со ред 2.

Навистина, ако $c \in G \setminus H$, тогаш редот на c е 2 или 4. Ако редот на c е 4, тогаш c^2 има ред 2, и $c^2 \in H$, зашто $(G : H) = 2$. Значи, $c^2 = a^2$, па имаме $ac \in G \setminus H$ и $(ac)^2 = a^2 c^2 = a^2 a^2 = e$, т.е. ac има ред 2. Ставајќи $K = [b]$, добиваме $G = K \otimes H$, а бидејќи $K \cong C_2$, $H \cong C_4$, добиваме дека $G \cong C_2 \times C_4$.

Ако во G нема елементи со ред 8 и елементи со ред 4, тогаш секој елемент $x \in G$, $x \neq e$, има ред 2. Нека a, b, c се три различни елементи и различни од e. Ако $A = [a]$, $B = [b]$, $C = [c]$, тогаш $BC \cong K_4$, $A \cong C_2$. Бидејќи $G = A \otimes BC$, добиваме дека $G \cong C_2 \times K_4$.

15.14. Да се покаже дека постојат само две некомутативни групи со ред 8.

Решение. Јасно е дека постојат барем две некомутативни групи со ред 8 и тоа диедралната D_4 (види 6.5) и кватернионската (6.6).

Нека G е некомутативна група со ред 8. Во G не постои елемент со ред 8, зашто, во тој случај G би била циклична, па според тоа и комутативна. Исто така, не е можно секој елемент од G да има ред 2, зашто и во тој случај G би била комутативна. Значи, групата G има елемент a со ред 4; нека $H = [a]$, $a^4 = e$. Подгрупата H е со индекс 2 во G, па значи H е нормална подгрупа во G и притоа $G = H \cup bH$ за некој $b \in G$, $b \notin H$. Елементот $b^2 \in H$, зашто ако $b^2 \notin H$, тогаш комплексите H, bH и b^2H би биле различни, спротивно на $(G : H) = 2$.

Според тоа, за елементот b^2 можен е еден од следниве случаи: $b^2 = e$, $b^2 = a$, $b^2 = a^2$, $b^2 = a^3$.

Ако би било $b^2 = a$, или $b^2 = a^3$, тогаш би добиле $G = [b]$, што не е можно. Значи, можно е или $b^2 = e$, или $b^2 = a^2$.

(i) Нека $b^2 = e$ и $K = [b]$. Тогаш $H \cap K = \{e\}$ и $G = HK$.

Од $H \lhd G$, имаме $b^{-1} ab \in H$, а од $a^4 = e$ добиваме $(b^{-1} ab)^4 = e$, т.е. $b^{-1} ab = a$, или $b^{-1} ab = a^3$. Ако $b^{-1} ab = a$, добиваме $ab = ba$, т.е. G е комутативна. Значи, $b^{-1} ab = a^3$, т.е. $ba = a^3 b$ и $ab = ba^3$. Елементите e, a, a^2, a^3, b, ab, a^2b, a^3b се сите различни и равенствата $a^4 = a$, $b^2 = e$, $ba = a^3b$,
ни овозможуваат да ја формираме следната шема:

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	e	a^3	a^2	a
ab	ab	b	a^3b	a^2b	a	e	a^3	a^2
a^2b	a^2b	ab	b	a^3b	a^2	a	e	a^3
a^3b	a^3b	a^2b	ab	b	a^3	a^2	a	e

шема 1.

Ако во оваа шема ставиме a_i наместо a^i и b_i наместо $a^i b$, тогаш таа поминува во шемата на диедралната група D_4. Значи, групата дефинирана со оваа шема е изоморфна со D_4.

(ii) Нека $b^2 = a^2$. Како и во претходниот случај, добиваме $b^{-1}ab = a^3$, т.е. $ab = ba^3$. Елементите e, a, a^2, a^3, b, ab, a^2b, a^3b се сите различни меѓусебно и равенствата

$a^4 = e$, $b^2 = a^2$, $ab = ba^3$,

ни овозможуваат да ја формираме шемата 2, дадена подолу. Ако во таа шема ставиме $f(x)$ наместо x, каде што:

$f(e) = 1$, $f(a) = i$, $f(a^2) = -1$, $f(a^3) = -i$,
$f(b) = j$, $f(ab) = k$, $f(a^2 b) = -j$, $f(a^3 b) = -k$,

тогаш шемата 2 поминува во шемата на кватернионската група K (види 6.6).

Значи, со шемата 2 е дефинирана група и таа е изоморфна со кватернионската група K.

Од сето тоа следува дека постојат само две некомутативни групи со ред 8 и тоа се диедралната D_4 и кватернионската K.

	e	a	a^2	a^3	b	ab	a^2b	a^3b
e	e	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	e	ab	a^2b	a^3b	b
a^2	a^2	a^3	e	a	a^2b	a^3b	b	ab
a^3	a^3	e	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	e	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	e
a^2b	a^2b	ab	b	a^3b	e	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	e	a^3	a^2

шема 2.

15.15. Да се покаже дека постојат само две комутативни неизоморфни групи со ред 12 и тоа: C_{12} и $C_3 \times K_4$, каде што K_4 е *клајноваша ӷрӯпа* (т.е. нецикличната група со ред 4).

15.16. Да се најдат сите некомутативни меѓусебно неизоморфни групи со ред 12.

Решение. Постојат само три некомутативни меѓусебно неизоморфни групи со ред 12. Тоа се: диедралната D_6, алтернативната A_4 и групата G, генерирана од матриците.

$$A = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \qquad B = \begin{bmatrix} \varepsilon & 0 \\ 0 & \varepsilon^2 \end{bmatrix}, \qquad i^2 = -1, \quad \varepsilon^3 = 1.$$

15.17. Ако p е прост број тогаш постојат само две меѓусебно неизоморфни групи со ред $2p$; тоа се: C_{2p} и D_p.

Решение. Нека p е прост број и нека G е група со ред $2p$.

Според 13.13, G има точно една подгрупа K со ред p и, или точно една подгрупа H со ред 2, или точно p подгрупи со ред 2.

(i) Нека G има само една подгрупа H со ред 2. Бидејќи H е единствената силова 2–подгрупа, а K единствената силова p-подгрупа, добиваме дека $H \lhd G$ и $K \lhd G$. Јасно дека $H \cap K = \{e\}$, како и $|H|\,|K| = 2p = |G|$. Според 12.17 и 15.9, добиваме дека $G = H \otimes K$. Групите H и K се циклични, па бидејќи $(2, p) = 1$, следува дека и групата G е циклична (види 15.11), т.е. $G = C_{2p}$.

(ii) Нека G има точно p подгрупи со ред 2. Ако $K = [a]$, $a^p = e$, тогаш од $b \notin K$ следува $b^2 = e$. Јасно е дека $G = K \cup Kb$, па

$G = \{e, a, \ldots, a^{p-1}, b, ab, \ldots, a^{p-1}b\}$

Бидејќи $a^i b \notin K$ за $i = 0, 1, \ldots, p-1$, следува дека $(a^i b)^2 = e$, па $a^i b = (a^i b)^{-1} = b^{-1}(a^i)^{-1} = ba^{p-i}$.

Ако D_p е диедрална група со ред $2p$ (види 6.5.), нека $f: D_p \to G$ е дефинирано со

$f(a_i) = a^i$, $f(b_i) = a^i b$, $i = 0, 1, \ldots, p-1$.

Лесно се покажува дека f е изоморфизам.

Од сето тоа следува дека постојат само две меѓусебно неизоморфни групи со ред $2p$, p прост број, и тоа едната C_{2p}, а другата D_p.

15.18. Да се најдат сите меѓусебно неизоморфни групи со ред 14.

Решение. Бидејќи $14 = 2 \cdot 7$, според 15.17, добиваме дека постојат само две: C_{14} и D_7.

15.19. Да се најдат барем 7 неизоморфни групи со ред 16.

Одговор. C_{16}, $C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times K_4$, $K_4 \times K_4$, $D_4 \times C_2$ и D_8 каде што K_4 е клајновата група (т.е. нецикличната група со ред 4).

15.20. Да се покаже дека $D_6 \cong D_3 \times C_2$, каде што D_m е диедрална (види 6.5.), а C_2 цикличната група со ред 2.

Решение. Пресликувањето $f: D_6 \to D_3 \times C_2$, дефинирано со:

$a_i \to (a_m, c^i)$, $b_i \to (b_m, c^i)$, $i = 0, 1, \ldots 5$, $m \equiv i \pmod 3$ е изоморфизам.

15.21. Нека G е комутативна група. Ако p е прост број, да се покаже дека

а) $S(p) = \{x \mid x \in G,\ x^{p^n} = e, n \in \mathbb{N}^0\}$ е подгрупа од G.

б) $G = \prod_p^* S(p) \Leftrightarrow G$ е периодична група.

Решение. а) Ако $x, y \in S(p)$, т.е. $x^{p^n} = e$, $y^{p^m} = e$, тогаш

$$(xy)^{p^{m+n}} = x^{p^{m+n}} . y^{p^{m+n}} = (x^{p^n})^{p^m} (y^{p^m})^{p^n} = e^{p^m} \cdot e^{p^n} = e,$$

што значи $xy \in S(p)$. Потоа, од $x^{p^n} = e$ следува

$$(x^{-1})^{p^n} = (x^{p^n})^{-1} = e,$$

т.е. $x \in S(p)$. Значи, $S(p)$ е подгрупа од G.

б) Ако $G = \prod_p^* S(p)$, тогаш кој било елемент $x \in G$ може да се претстави на единствен начин како производ $x = x_1 \dots x_k$, при што $x_i \in S(p_i)$, т.е. $x_i^{p_i^{n_i}} = e$, $i = 1, \dots, k$. Ставајќи $n = p_1^{n_1} \dots p_k^{n_k}$, добиваме дека $x^n = e$, т.е. групата G е периодична.

Обратно, нека G е периодична, и нека $x \in G$ има ред $n = p_1^{n_1} \dots p_k^{n_k}$,

Тогаш, постојат еднозначно определени елементи $x_1, \dots, x_k$ од G, такви што $x = x_1 x_2 \dots x_k$ и x_i има ред $p_i^{n_i}$. Значи, $x_i \in S(p_i)$. Од ова следува заклучокот дека $G = \prod_p^* S(p)$.

15.22. Нека G е конечна група со својството: секоја силова подгрупа е нормална во G. Да се покаже дека G е внатрешен директен производ од своите силови подгрупи.

Решение. Нека $| G | = n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Бидејќи секоја силова подгрупа е нормална, постои само една силова p_i–подгрупа ($i = 1, \dots, m$) во G и таа е со ред $p_i^{\alpha_i}$. Значи, постојат точно m силови подгрупи: $S_1, S_2, \dots, S_m$.

Да забележиме дека $S_i \cap S_j = \{e\}$ за $i \neq j$, од каде што следува дека секој елемент од S_i комутира со секој елемент од S_j (види 12.17).

Но тогаш $S_1 \cdot S_2 \dots \cdot S_m$ е подгрупа од G со ред n, па значи имаме $G = S_1 \cdot S_2 \dots S_m$. Бидејќи од $a_1 a_2 \dots a_m = e$, $a_i \in S_i$, следува дека $a_i = e$, $i = 1, \dots, m$, добиваме дека $S_i \cap S_1 \dots S_{i-1} S_{i+1} \dots S_m = \{e\}$. Од сето тоа следува дека $G = S_1 \otimes \dots \otimes S_m$.

15.23. Нека G е конечна комутативна група со ред $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, каде што $p_1, p_2, \dots, p_k$ се различни прости броеви. Да се покаже дека групата G е циклична ако и само ако постојат циклични подгрупи $H_1, H_2, \dots, H_k$, такви што $G = H_1 \otimes H_2 \otimes \dots \otimes H_k$, при што H_i има ред $p_i^{\alpha_i}$.

Решение. Да претпоставиме дека постојат циклични подгрупи H_1, $H_2, \dots, H_k$ т.ш. $G = H_1 \otimes H_2 \otimes \dots \otimes H_k$, при што H_i има ред $p_i^{\alpha_i}$.

Според 15.11, бидејќи $(p_i^{\alpha_i}, p_j^{\alpha}) = 1$ за $i \neq j$, следува дека $H_1 \times H_2 \times \times \ldots \times H_k$ е циклична група со ред n, па значи и G е циклична.

Обратно, нека групата G е циклична. Тогаш постојат елементи $a_1, a_2, \ldots, a_k$, такви што a_i има ред $p_i^{\alpha_i}$, $i = 1, 2, \ldots, k$.

Ако ставиме $H_i = [a_i]$, $i = 1, 2, \ldots, k$, тогаш, според 15.11. $H_1 \times H_2 \times \ldots \times H_k$ е циклична група со ред n, па е изоморфна со G. Оттука следува дека $G = H_1 \otimes H_2 \otimes \ldots \otimes H_k$.

15.24. Да се покаже дека, ако H и K се решливи подгрупи од G и ако $G = H \otimes K$, тогаш, и групата G е рашлива.

Решение. Бидејќи G / H е изоморфна со K, според 14.27, следува дека групата G е решлива.

§16. КОНЕЧНИ КОМУТАТИВНИ ГРУПИ

16.1. Да се определи бројот на неизоморфните комутативни групи со ред:

а) 100; б) 143;

в) p^2q^3, каде што p и q се различни прости броеви.

Решение. а) Бидејќи $100 = 2^2 5^2$, имаме :

$M = \{(2; 2), (2; 1, 1), (1, 1; 2), (1, 1; 1, 1;)\}$,

што значи дека постојат четири неизоморфни комутативни групи со ред 100

б) Бидејќи $143 = 11 \cdot 13$, имаме $M = \{(1; 1)\}$, т.е. само една.

в) Шест.

16.2. Да се напишат шемите на неизоморфните комутативни групи со ред 12.

Решение. Бидејќи $12 = 2^2 \cdot 3$, можеме да ги формираме низите (2; 1) и (1, 1; 1), па значи постојат две неизоморфни комутативни групи со ред 12: едната е цикличната C_{12}, а другата $K_4 \times C_3$, каде што K_4 е клајновата група. Шемите на овие групи лесно се формираат.

16.3. Да се најде бројот на неизоморфните абелови групи со ред 17640.

Решение. Бидејќи $17640 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$, лесно добиваме дека бараниот број е 12.

16.4. Каков треба да биде природниот број n за да бидат изоморфни сите комутативни групи со ред n?

Одговор. Бројот n треба да има облик: $n = p_1 \cdot p_2 \ldots p_k$, каде што p_i се прости броеви.

16.5. Нека $G = A \oplus B$ и нека A_1, B_1 се подгрупи во G, при што $A_1 \subseteq A$, $B_1 \subseteq B$ и $A_1 + B_1 = H$. Да се покаже дека $G / H = A / A_1 \oplus B / B_1$.

Решение. Нека $K = A / A_1 \oplus B / B_1$ и нека $f : A \to A / A_1$, $g : B \to B / B_1$ се природните хомоморфизми. Бидејќи секој $x \in G$ може да се претстави на единствен начин во обликот $x = a + b$, $a \in A$, $b \in B$, можеме да дефинираме пресликување $h : G \to K$ со:

$h(a + b) = f(a) + g(b)$,

коешто е епиморфизам бидејќи f и g се епиморфизми. Јасно е дека

$\text{Ker } h \supseteq \text{Ker } f = A_1$, $\text{Ker } h \supseteq \text{Ker } g = B_1$,

па значи $\text{Ker } h \supseteq A_1 + B_1$.

Ако $y \in \text{Ker} h$, тогаш $y = a + b$ за некои $a \in A$ и $b \in B$, па

$h(y) = (a+A_1) + (b+B_1)$ ќе биде неутралниот елемент во K само ако $a \in A_1$ и $b \in B_1$. Значи

$y \in A_1 + B_1$, т.е. $\text{Ker } h \subseteq A_1 + B_1$, па $\text{Ker} h = A_1 + B_1 = H$.

Бидејќи h е епиморфизам, добиваме

$G / \text{Ker } h \cong K$.

16.6. Нека G е комутативна група со ред n. Да се покаже дека G може да се претстави како директен производ, $G = G_1 \otimes \ldots \otimes G_k$, од конечно многу циклични групи, каде што $1 < n_{i+1} = |G_{i+1}|$ е делител на $n_i = |G_i|$ и дека низата $n_1, n_2, \ldots, n_k$ е инваријантна за групата G.

Решение. Нека $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, и нека G е претставена како директен производ

$$G = S_{11} \times S_{12} \times \ldots \times S_{1m_1} \times S_{21} \times \ldots \times S_{2m_2} \times \ldots \times S_{r1} \times \ldots \times S_{rm_r},$$

каде што S_{im_i} е циклична група со ред $p_i^{\beta i}, \beta_i \geq \beta_{i+1}$. За попросто, ќе претпоставиме дека $m_1 = m_2 = \ldots = m_r = m$. (Ако е, на пример, $m_1 < m_2$, ќе ставиме $S_{1m_1+1} = \ldots = S_{1m_2} = \{e\}$.)

Потоа, ако ставиме

$G_i = S_{1i} \cdot S_{2i} \ldots \cdot S_{ri}$

добиваме дека $G = G_1 \times G_2 \times \ldots \times G_m$, и притоа $|G_{i+1}|$ е делител на $|G_i|$. Групите G_i се циклични, бидејќи се директни производи на циклични групи со заемно прости редови.

Дека $n_1, n_2, \ldots, n_k$ е инваријантна за групата G е јасно.

16.7. Нека G е нециклична конечна абелова група. Да се покаже дека постои прост број p, таков што во G постои подгрупа H од тип (p, p), т.е. H е директен производ на циклични групи со ред p.

Решение. Не можат сите силови подгрупи да се циклични, бидејќи тогаш и G би била циклична. Нека $S(p)$ е нециклична p–подгрупа од G. Тогаш $S(p)$ е директен производ на циклични p–групи:

$S(p) = S_1(p) \times S_2(p) \times \ldots \times S_r(p)$.

Ако a_1 е елемент со ред p во $S_1(p)$, а a_2 со ред p во $S_2(p)$, тогаш $[a_1] \times [a_2]$ е подгрупа со тип (p, p).

16.8. Ако G е абелова група со инваријанта (p^3, p^2), каде што p е прост број, да се најде бројот на подгрупите со ред p^2.

Решение. Да ја претставиме G како производ на циклични p–групи: $G = A \times B$, $|A| = p^3$, $|B| = p^2$. Во A имаме само една подгрупа C со ред p^2 и само една подгрупа D со ред p; во B има само една подгрупа F со ред p. Тогаш, со ред p^2 се само следниве подгрупи од G: B, C, $D \times F$.

16.9. Да се докаже дека секоја конечногенерирана торзиона група е конечна.

Решение. Ако групата G е конечногенерирана, тогаш таа е директна сума од конечен број циклични групи. Ако G е торзиона, тогаш таа е директна сума од конечен број конечни циклични групи. Според тоа, G е конечна.

16.10. Нека $G = \oplus\sum_{i=1}^{\infty} G_i$, каде што G_i е циклична група со ред 2 за $i = 1, 2, \ldots$. Да се докаже дека G не е конечногенерирана.

Решение. Ако $a \in G$, $a \neq 0$, тогаш

$a = a_{i_1} + \ldots + a_{i_n}$, $a_{i_k} \in G_{i_k}$ и $2a = 2a_{i_1} + \ldots + 2a_{i_n} = 0$

(зашто $2a_{i_k} = 0$), што значи секој елемент $a \in G$ има конечен ред, па според тоа, групата G е торзиона. Кога G би била конечногенерирана, тогаш, според 16.9, таа би била конечна. Но, G е бесконечна, па значи таа не е конечногенерирана.

16.11. Нека G е p–група, таква што $G = [a] \oplus B$ и b е елемент од B чијшто ред не е поголем од редот на a. Да се покаже дека $G = [a + b] \oplus B$.

Решение. Ако $x \in G$, тогаш $x = ma + y$, каде што $y \in G$, па

$x = ma + mb + (y - mb) \in [a + b] + G$, од што следува дека $[a + b] + B = G$.

Треба да покажеме уште дека $[a + b] \cap B = \{0\}$. Затоа, нека $x \in [a + b] \cap B$. Тогаш, за некој цел број број m, имаме

$x = m(a + b) = b_1 \in B$, од каде што $ma = b_1 - mb$.

Бидејќи $[a] \cap B = \{0\}$ имаме $ma = 0$, па значи m е делив со некој степен од p – редот на a. Бидејќи редот на b не е поголем од редот на a, имаме и $mb = 0$. Според тоа $b_1 = 0$, т.е. $x = 0$. Значи: $[a + b] \cap B = \{0\}$, кое заедно со $[a + b] + B = G$ го дава резултатот.

16.12. Нека G е конечна p–група. Ако $a \in G$ е елемент со ред p, да се покаже дека a се појавува како елемент на цикличен директен суманд од G.

Решение. Бидејќи G е директна сума од циклични групи, да ставиме

$G = [c_1] \oplus [c_2] \oplus \ldots \oplus [c_n]$.

Ако $a = 0$, тврдењето е јасно.

Затоа, да претпоставиме дека $a \neq 0$. Не губејќи од општоста, ќе ставиме

$$a = m_1 p^{\alpha_1} c_1 + \ldots + m_k p^{\alpha_k} c_k,$$

а каде што $(m_i, p) = 1$, $m_1 p^{\alpha_1} c_1 \neq 0$ и $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n$. Ако ставиме $m_1 c_1 = c_1'$, тогаш имаме $[c_1'] = [c_1]$, па a можеме да го напишеме во обликот $a = p^{\alpha_1}(c_1' + b)$, каде што $b \in [\{c_2, \ldots, c_n\}]$. Бидејќи a е со ред p и $p^{\alpha_1} c_1' \neq 0$, редот на b не е поголем од редот на c_1' па според 16.11, ставајќи $c = c_1' + b$, добиваме

$G = [c] \oplus [\{c_2, \ldots, c_n\}]$, при што $a \in [c]$.

16.13. Нека G е конечна p-група и нека $H = [a]$ има ред p. Да се покаже дека G / H е изоморфна со некоја подгрупа од G.

Решение. Според 16.12, $G = [c] \oplus B$ при што $a \in [c]$. Тогаш, според 16.5, имаме $G / H \cong ([c] / H) \oplus B$. Но, поради $[pc] = [c] / H$, имаме $[\{pc, B\}] \cong G / H$.

16.14. Нека H е подгрупа од една конечна абелова група G. Да се покаже дека постои подгрупа K во G, така што $G / H \cong K$.

Решение. Доказот ќе го спроведеме со индукција по $|G|$. Да претпоставиме дека тврдењето е точно за сите групи со ред помал од r. Нека $|G| = r$ и нека H е подгрупа од G. Ако $H = \{0\}$, тогаш е јасно дека $G / H \cong G$, т.е. таква подгрупа K е самата G.

Нека H има ред прост број p. Да ставиме:

$G_p = \{x \mid x \in G, x$ има ред што е степен од $p\}$. (G_p е подгрупа, наречена *p–компонента* на G). Тогаш $H \subseteq G_p$ и $G = G_p \oplus F$. Според 16.5, имаме $G / H \cong (G_p / H) \oplus F$. Според 16.13, постои подгрупа L од G_p, таква што $G_p / H \cong L$, па значи $G/H \cong L \oplus F$ при што $L \oplus F = K$ е подгрупа од G.

Нека редот на H не е прост. Ако p е прост број што е делител на $|H|$, постои елемент $a \in H$ со ред p. Ставајќи $A = [a]$, добиваме

$(G / A) / (H / A) \cong G / H$. Бидејќи $| G / A | < | G | = r$, G / A има подгрупа $B / A \cong G / H$. Јасно е дека $B \neq G$, зашто во спротивно би имале $B = A$ што не е точно. Значи имаме $|B| < |G|$, па според индуктивната претпоставка, постои подгрупа K таква што $K \cong B / A \cong G / H$, со што тврдењето е докажано.

16.15. Нека G е конечна абелова група со ред mn, $(m, n) = 1$. Да се покаже дека постои подгрупа H со ред m и подгрупа K со ред n, така што $G = K \oplus H$.

Решение. Нека $mn = p_1^{\alpha_1} \ldots p_r^{\alpha_r} q_1^{\beta_1} \ldots q_s^{\beta_s}$. Тогаш имаме:

$G = S(p_1) \oplus \ldots \oplus S(p_r) \oplus S(q_1) \oplus \ldots \oplus S(q_s)$.

Ставајќи $H = S(p_1) \oplus \ldots \oplus S(p_r)$, $K = S(q_1) \oplus \ldots \oplus S(q_s)$, добиваме $G = H \oplus K$, при што H има ред m, а K има ред n.

16.16. Нека G се разложува во директен производ од C_2, C_3, C_5 и две бесконечни циклични групи. Да се најде:

а) периодичниот дел $T(G)$ на G;

б) бројот на периодичните подгрупи;

в) фактор–групата $G / T(G)$.

г) хомоморфната слика на G при хомоморфизмот f, за кој $\mathrm{Ker} f = C_5$.

Решение. а) $T(G) = C_{30}$. б) 8

в) Директниот производ од двете бесконечни циклични групи.

г) Директниот производ на C_2, C_3 и двете бесконечни циклични групи.

16.17. Нека G е конечно генерирана абелова група. Да се докаже дека рангот на G е еднаков со рангот на $G / T(G)$.

16.18. Да се најде бројот на неизоморфните комутативни групи со ранг 4 и $| T(G) | = 72$.

Решение. Бидејќи $72 = 2 \cdot 31$, според 15.17, $T(G) = C_{72}$.

Имајќи предвид дека $G = T(G) \oplus G^*$, каде што G^* е периодичниот дел, следува дека постои само една комутативна група со ранг 4 и $T(G) = 72$.

16.19. Ако $\lambda(n)$ е бројот на неизоморфните групи со ред n, да се најде $\lambda(n)$ за $n = 1, \ldots, 15$.

Решение.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\lambda(n)$	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1

(За 6, 10 и 14 види 15.17; за 8 и 12 види 15.13 – 15.16; за 15 види 13.8.)

16.20. Да се најдат сите абелови p–групи, коишто содржат точно p^2+p+1 подгрупа со ред p.

Решение. Нека $G = [a_1] \oplus [a_2] \oplus \ldots \oplus [a_k]$, каде што a_i има ред p^{α_i}. Ако $x = m_1a_1 + m_2a_2 + \ldots + m_ka_k$, тогаш

$$px = 0 \Leftrightarrow pm_1a_1 = pm_2a_2 = \ldots = pm_ka_k = 0.$$

Значи, $m_ia_i = 0$ или m_ia_i има ред p. Во $A_k = [a_k]$ има $p-1$ елементи со ред p, бидејќи има само една подгрупа со ред p. Ако се има предвид тоа што $x = x_1 + x_2 + \ldots + x_k$, x_k има ред p или $x_k = 0$, добиваме дека со ред p има $p \cdot p \ldots p - 1 = p^k - 1$ елементи (се одзема 1, бидејќи не може да биде $x = 0 + \ldots + 0$). Две подгрупи со ред p имаат заеднички елемент само 0, од што следува дека постојат

$$(p^k - 1) : (p - 1) = p^{k-1} + p^{k-2} + \ldots + 1$$

подгрупи со ред p. За да биде $p^{k-1} + \ldots + p + 1 = p^2 + p + 1$, треба да е $k - 1 = 2$, т.е. $k = 3$. Значи, G има облик $(p^\alpha, p^\beta, p^\gamma)$. Такви групи има бесконечно многу.

ПОКАЗАТЕЛ НА ПОИМИ

ПОЧЕСТО УПОТРЕБУВАНИ ОЗНАКИ

$\mathbb{N}$ – множеството на природните броеви

$\mathbb{Z}$ – множеството на целите броеви

$\mathbb{Q}$ – множеството на рационалните броеви; $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$

$\mathbb{R}$ – множеството на реалните броеви; $\mathbb{R}^* = \mathbb{R}\setminus\{0\}$

$\mathbb{C}$ – множеството на комплексните броеви

$\mathbb{P}(M)$ – партитивното множество на множеството M

kM – кардиналниот број на множеството M

$\mathcal{T}(M)$ – множеството трансформации на множеството M

S_M – групата пермутации на множеството M

S_n – симетричната група пермутации на множеството со n елементи

D_n – диедралната група со $2n$ елементи

C_n – циклична група со ред n

$[a]$ – циклична група генерирана од елементот a

$[A]$ – подалгебра генерирана од множеството A

$|G|$ – ред на групата G; кардинален број на множеството G

$H \lhd G$ – H нормална подгрупа од групата G

Aut G – множеството автоморфизми на G

End G – множеството ендоморфизми на G

$C(G)$ – центарот на групата G

$N(S)$ – нормализатор на подмножеството S од дадена група

$T(G)$ – периодичен дел (торзија) на групата G

(a,b) – подреден пар; интервал; најголем заеднички делител (НЗД)

$[a,b]$ – комутатор; сегмент; најмал заеднички содржател (НЗС)

ПРИРОДНО МАТЕМАТИЧКИ ФАКУЛТЕТ - СКОПЈЕ
Гази баба б.б. Поштенски фах 162, Скопје, Р. Македонија.

***

За издавачот

Д е к а н
Д-р Костадин Тренчевски, ред. проф.

***

Компјутерска обработка на текстот
Олгица Андова
Симона Самарџиска

***

Технички уредник
Кристина Органџиева

***

Коректура
Симона Самарџиска

Ракописот е предаден во печат во месец мај 2006 година. Печатењето е завршено во месец мај 2006 година. Обем 239 страници. Тираж 250 примероци. Книгата е отпечатена во печатницата "Алфа 94" – Скопје.