Примерни задачи за пръстени по Висша Алгебра 1

Задача 1. *Да се определи кои от следните числови множества образуват пръстени относно обичайните операции събиране и умножение на комплексни числа:*

$$\textit{(а)}\ R_1 = \left\{ \frac{a}{p^k} \,\middle|\, a \in \mathbb{Z},\ k \in \mathbb{N},\ p \textit{ не дели } a \right\},$$

където p е фиксирано просто число;

$$\textit{(б)}\ R_2 = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z},\ b \neq 0,\ (a,b) = 1,\ p \textit{ не дели } b \right\},$$

където p е фиксирано просто число;

$$\textit{(в)}\ R_3 = \{x + y\sqrt[3]{2} \,|\, x, y \in \mathbb{Q}\};$$

$$\textit{(г)}\ R_4 = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} \,|\, x, y, z \in \mathbb{Q}\}.$$

Решение: (а) Ако допуснем, че $(R_1, +)$ е подгрупа на $(\mathbb{C}, +)$, то неутралният елемент 0 на $(\mathbb{C}, +)$ принадлежи на R_1. Но от $0 = \frac{a}{p^k}$ следва $a = 0.p^k$ и $0 \in \mathbb{Z}$ се дели на p, така че $0 = \frac{0}{p^k} \notin R_1$. Следователно $(R_1, +)$ не е подгрупа на $(\mathbb{C}, +)$ и R_1 не е подпръстен на $\mathbb{C}$.

(б) Ако $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in R_2$, то след евентуално съкращение на общите множители на числителя и знаменателя на

$$\frac{a_1}{b_1} - \frac{a_2}{b_2} = \frac{a_1 b_2 - a_2 b_1}{b_1 b_2}$$

получаваме рационално число от R_2. Причина за това е, че $b_1 b_2$ не се дели на простото число p, ако b_1 и b_2 не се делят поотделно на p. Следователно $(R_2, +)$ е подгрупа на адитивната група $(\mathbb{C}, +)$ на полето $\mathbb{C}$ на комплексните числа.

За произволни $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in R_2$ произведението

$$\frac{a_1}{b_1}.\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2} \in R_2$$

след евентуално съкращение на общите множители на числителя и знаменателя. Отново използваме, че $b_1 b_2$ не се дели на p, ако b_1 и b_2 не се делят поотделно на p.

Следователно R_2 е подпръстен на $\mathbb{C}$, а оттам и пръстен относно обичайните операции събиране и умножение на комплексни числа.

(в) За произволни $x_1 + y_1\sqrt[3]{2}, x_2 + y_2\sqrt[3]{2} \in R_3$ са в сила $x_1 - x_2 \in \mathbb{Q}$, $y_1 - y_2 \in \mathbb{Q}$, защото $\mathbb{Q}$ е група относно обичайното събиране на комплексни числа. Следователно $(x_1 + y_1\sqrt[3]{2}) - (x_2 + y_2\sqrt[3]{2}) = (x_1 - x_2) + (y_1 - y_2)\sqrt[3]{2} \in R_3$ и $(R_3, +)$ е подгрупа на адитивната група $(\mathbb{C}, +)$ на полето $\mathbb{C}$ на комплексните числа.

Множеството R_3 не е затворено относно умножение на свои елементи, защото $\sqrt[3]{2} \in R_3$, но $\sqrt[3]{2}.\sqrt[3]{2} = \sqrt[3]{4} \notin R_3$. По-точно, допускането $\sqrt[3]{4} = a + b\sqrt[3]{2}$ за някои $a, b \in \mathbb{Q}$ води до

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

Ако $a + b^2 = 0$, то $ab = 2$, откъдето

$$0 = \frac{2}{b} + b^2 = \frac{2 + b^3}{b} \quad \text{и} \quad b^3 = -2.$$

Това противоречи на ирационалността на $\sqrt[3]{-2}$. При $a + b^2 \neq 0$ получаваме, че

$$\sqrt[3]{2} = \frac{2 - ab}{a + b^2} \in \mathbb{Q}$$

е рационално число, което също не е вярно.

Относно ирационалността на $\sqrt[3]{\pm 2}$, да предположим, че

$$\sqrt[3]{\pm 2} = \pm p_1^{a_1} \dots p_k^{a_k} q_1^{-b_1} \dots q_l^{-b_l} \in \mathbb{Q}$$

за различни прости $p_1, \dots, p_k, q_1, \dots, q_l$ и $a_i, b_j \in \mathbb{N}$. След повдигане в степен 3 и освобождаване от знаменателя получаваме

$$\pm 2 q_1^{3b_1} \dots q_l^{3b_l} = \pm p_1^{3a_1} \dots p_k^{3a_k}.$$

Без ограничение на общността ще считаме, че $p_1 < p_2 < \ldots < p_k$. Тогава $p_1 = 2$, защото $p_1^{3a_1} \dots p_k^{3a_k}$ е четно число. Но отдясно, степенният показател на 2 се дели на 3, докато отляво, степенният показател на 2 дава остатък 1 при деление на 3. Това противоречи на единствеността на разлагането на естествените числа $n > 1$ в произведение от прости множители и доказва ирационалността на $\sqrt[3]{\pm 2}$. В резултат, $\sqrt[3]{2}.\sqrt[3]{2} \notin R_3$ и R_3 не е пръстен относно обичайните операции събиране и умножение на комплексни числа.

(г) За произволни $x_i + y_i\sqrt[3]{2} + z_i\sqrt[3]{4} \in R_4$, $i = 1, 2$ е в сила

$$(x_1 + y_1\sqrt[3]{2} + z_1\sqrt[3]{4}) - (x_2 + y_2\sqrt[3]{2} + z_2\sqrt[3]{4}) = (x_1 - x_2) + (y_1 - y_2)\sqrt[3]{2} + (z_1 - z_2)\sqrt[3]{4} \in R_4,$$

защото $(\mathbb{Q}, +)$ е подгрупа на $(\mathbb{C}, +)$. Освен това,

$$(x_1 + y_1\sqrt[3]{2} + z_1\sqrt[3]{4})(x_2 + y_2\sqrt[3]{2} + z_2\sqrt[3]{4}) =$$

$$= (x_1x_2 + 2y_1z_2 + 2z_1y_2) + (x_1y_2 + y_1x_2 + 2z_1z_2)\sqrt[3]{2} + (x_1z_2 + y_1y_2 + z_1x_2)\sqrt[3]{4} \in R_4,$$

защото $x_i, y_i, z_i \in \mathbb{Q}$ и $\mathbb{Q}$ е подпръстен на $\mathbb{C}$. Следователно R_4 е пръстен относно обичайните операции събиране и умножение на комплексни числа.

Задача 2. *Да се определи кои от следните подмножества на пръстена $M_{n,n}(F)$ на матриците от ред n с елементи от числово поле F образуват подпръстен:*

$$(i)\quad S_1 = \{A \in M_{n,n}(F) \;\mid\; A^t = A\};$$

$$(ii)\quad S_2 = \left\{ A = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & 0 & \dots & 0 \end{pmatrix} \;\Big|\; a_{i1} \in F \right\};$$

Решение: (i) Ако $A, B \in S_1$, то $(A-B)^t = A^t - B^t = A - B$. Оттук $A - B \in S_1$ и $(S_1, +)$ е подгрупа на $(M_{n,n}(F), +)$. Съществуват некомутиращи матрици $A, B \in M_{n,n}(F)$, $AB \neq BA$. За тях $(AB)^t = B^tA^t = BA \neq AB$, $AB \notin S_1$ и S_1 не е подпръстен на $M_{n,n}(F)$.

(ii) Ако $A, B \in S_2$, то $A - B \in S_2$, защото $(A-B)_{ij} = A_{ij} - B_{ij} = 0$ за $\forall 1 \leq i \leq n$, $\forall 2 \leq j \leq n$. Следователно $(S_2, +)$ е подгрупа на $(M_{n,n}(F), +)$. Освен това,

$$AB = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1} & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ b_{21} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ b_{n1} & 0 & \dots & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & 0 & \dots & 0 \\ a_{21}b_{11} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ a_{n1}b_{11} & 0 & \dots & 0 \end{pmatrix} \in S_2,$$

така че S_2 е подпръстен на $M_{n,n}(F)$.

Задача 3. *Нека R е комутативен пръстен с единица 1_R. Да се докаже, че:*

(i) идеалът I на R съвпада с R тогава и само тогава, когато I има непразно сечение $I \cap R^* \neq \emptyset$ с мултипликативната група R^* на R;

(ii) пръстенът R е поле тогава и само тогава, когато единствените идеали в R са нулевият $\{0_R\}$ и целият пръстен R.

Упътване: (i) Ако $I = R$, то $1_R \in I \cap R^*$. Обратно, произволен елемент $r_o \in I \cap R^*$ има обратен $r_o^{-1} \in R$, така че $1_R = r_o^{-1} r_o \in I$. Сега за всяко $r \in R$ имаме $r = r1_R \in I$ и $I = R$.

(ii) Нека R е поле, а $I \neq \{0_R\}$ е ненулев идеал. Тогава съществува $r \in I \setminus \{0_R\}$. Съгласно обратимостта на r в R получаваме, че $1_R = r^{-1}r \in I$, откъдето $I = R$ по (i). Обратно, ако единствените идеали на R са $\{0_R\}$ и R, то за произволен ненулев елемент r на R, главният идеал $\langle r \rangle = rR$, породен от r съдържа ненулев елемент r, така че $rR = R$. Оттук съществува $s \in R$ с $rs = 1_R$ и r е обратим в R. По този начин, всеки ненулев елемент на R е обратим относно умножението и R е поле.

Задача 4. *Дадена е таблицата за събиране и част от таблицата за умножение в*

пръстена $R = \{a, b, c, d, e, f\}$*:*

$+$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

$.$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	c	d	$\ldots$	f
c	a	c	$\ldots$	a	c	e
d	a	d	$\ldots$	d	$\ldots$	d
e	a	e	c	a	e	c
f	a	f	$\ldots$	d	c	b

(i) Да се попълни таблицата за умножение на R*.*
(ii) Да се намерят подпръстените на R*.*
(iii) Да се намерят всички идеали в R*.*

Упътване: (i) Ако ред (съответно, стълб) от таблицата за умножение съдържа единствен неизвестен елемент xy, представяме десния множител y (съответно, левия множител x) на този елемент като сума на два други елемента и прилагаме десния (съответно, левия) дистрибутивен закон за събиране и умножение.

Преди всичко, a е нулата на R, защото $a + x = x = x + a$ за $\forall x \in R$. Ако търсим be, използваме таблицата за събиране, за да запишем e като сума на две други събираеми. Всяко от представянията $e = b + d$, $e = c + c$ или $e = f + f$ върши работа, докато $e = a + e$ и $e = e + a$ не са от полза. Умножавайки отляво коя и да е от изброените три суми с b, пресмятаме съответно

$$be = b(b + d) = b^2 + bd = b + d = e,$$

$$be = b(c + c) = bc + bc = c + c = e \quad \text{или}$$

$$be = b(f + f) = bf + bf = f + f = e.$$

Аналогично, за да намерим c^2 използваме, например, представянето $c = b + b$ за десния множител и извеждаме

$$c^2 = c(b + b) = cb + cb = c + c = e.$$

За пресмятането на de можем да представим $d = b + c$ и да получим

$$de = (b + c)e = be + ce = e + c = a.$$

По-нататък, за намирането на dc можем да приложим $c = b + b$ и да изведем, че

$$dc = d(b + b) = db + db = d + d = a.$$

Накрая, можем да пресметнем

$$fc = f(b + b) = fb + fb = f + f = e.$$

(ii) Определете първо подгрупите $(I, +)$ на адитивната група $(R, +)$. За целта, проверете, че $a \in R$ е нулата на пръстена R. Търсим $I = \{r(i_1), \ldots, r(i_p)\} \subseteq R$ като

подмножество на R, съдържащо $a = 0_R$, чийто брой на елементите p дели броя на елементите $|R|$ на R. Твърдим, че такова подмножество $I = \{r(i_1) = a = 0_R, r(i_2), \dots r(i_p)\}$ е подгрупа на $(R, +)$ тогава и само тогава, когато за всяко $1 \leq j \leq p$ редът с номер i_j от таблицата за събиране съдържа пермутация на $r(i_1), \dots, r(i_p)$ в стълбовете с номера $i_1, \dots, i_p$. Комутативността на събирането в пръстена R е еквивалентна на симетричността на матрицата за събиране. Затова $(I = \{r(i_1) = a = 0_R, r(i_2), \dots, +) \leq (R, +)$ точно когато за всяко $1 \leq k \leq p$ стълбът с номер i_k от таблицата за събиране съдържа пермутация на $r(i_1), \dots, r(i_p)$ в редовете с номера $i_1, \dots, i_p$.

Наистина, ако $(I = \{i_1, \dots, i_p\}$ е подгрупа на $(R, +)$, то за всяко $1 \leq j \leq p$ елементите от реда с номер i_j и стълбовете с номера $i_1, \dots, i_p$ от таблицата за събиране се съдържат в множеството $\{r(i_1), \dots, r(i_p)\}$, защото $I = \{i_1, \dots, i_p\}$ е затворено относно събиране. Ако $r(i_j) + r(i_k) = r(i_j) + r(i_m)$ за някои $1 \leq k < m \leq p$, то $r(i_k) = r(i_m)$, така че гореспоменатите елементи са два по два различни и образуват пермутация на $i_1, \dots, i_p$. Обратно, ако за $\forall 1 \leq j \leq p$ редът с номер i_j от таблицата за събиране съдържа пермутация на $r(i_1), \dots, r(i_p)$ в стълбовете с номера $i_1, \dots, i_p$, то $I = \{i_1, \dots, i_p\}$ е затворено относно събиране. Ако в реда с номер i_j нулата $a = 0_R \in I$ на пръстена R се намира в стълба с номер i_k, то противоположният елемент $-r(i_j) = r(i_k) \in I$. Следователно I съдържа $-r(i_1), \dots, -r(i_p)$ и $(I, +)$ е подгрупа на $(R, +)$.

Подгрупа $(I, +)$ на $(R, +)$ е подпръстен точно когато в таблицата за умножение сечението на редовете и стълбовете , отговарящи на $i_1, \dots, i_p$ съдържа само $r(i_1), \dots, r(i_p)$.

Адитивната група $(R, +)$ от ред $|R| = 6$ има тривиални подгрупи $(\{a = 0_R\}, +)$, $(R, +)$ и евентуални нетривиални подгрупи от ред 2 или от ред 3. За произволно подмножество $\{a, x\} \subset R$ имаме $a + a = a$ и $a + x = x = x + a$, защото $a = 0_R$ е нулата на R. От това, че $x + a = x, x + x$ е пермутация на a, x, стигаме до извода, че $x + x = a$.

В конкретния, случай, съгласно $b + b = c$, $c + c = e$, $d + d = a$, $e + e = c$, $f + f = e$, единствената подгрупа $(\{a, x\}, +)$ на $(R, +)$ от ред 2 е $\{a, x\} = \{a, d\}$.

Нека $(G, +)$ е подгрупа на $(R, +)$ от ред 3. Тогава $G = \{a, x, y\}$ за различни $x, y \in \{b, c, d, e, f\}$. От $x \neq a = 0_R$ и $y \neq a = 0_R$ следва, че $x + y = a$. Понеже $x + a = x, x + x, x + y = a$ е пермутация на a, x, y, сумата $x + x = y$. Аналогично, от това, че $y + a = y, y + x = a, y + y$ е пермутация на a, x, y извеждаме равенството $y + y = x$.

В конкретния случай, подмножествата $\{x, y\} \subset \{b, c, d, e, f\}$ с $x + y = a$ са $\{x, y\} = \{b, f\}$ и $\{x, y\} = \{c, e\}$. Понеже $b+b = c \notin \{b, f\} \subset \{a, b, f\}$, подмножеството $\{a, b, f\} \subset R$ не е подгрупа на $(R, +)$. Съгласно $c+c = e$ и $e+e = c$, стигаме до извода, че $(\{a, c, e\}, +)$ е подгрупа на $(R, +)$. Това доказва, че единствената подгрупа $(\{a, x, y\}, +)$ на $(R, +)$ от ред 3 е $\{a, x, y\} = \{a, c, e\}$.

Сечението на първи и четвърти ред с първи и четвърти стълб от таблицата за умножение съдържа само елементите a или d. Следователно $\{a, d\}$ е подпръстен на R. Сечението на първи, трети и пети ред с първи, трети и пети стълб от таблицата за умножение съдържа само елементите a, c или e, така че $\{a, c, e\}$ е подпръстен на R.

(iii) Подгрупа $(I, +)$ на $(R, +)$ е идеал в R, ако целите редове и стълбове от таблицата за умножение на R , отговарящи на $i_1, \dots, i_p$, съдържат само елементите $r(i_1), \dots, r(i_p)$.

В случая, освен тривиалните идеали $\{a = 0_R\}$ и R, първи и четвърти ред, както и първи и четвърти стълб от таблицата за умножение са съставени изцяло от елементите a и d, така че $\{a, d\}$ е идеал в R. Аналогично, първи, трети и пети ред, както и първи, трети и пети стълб от таблицата за умножение съдържат само елементите a, c, e. Затова

$\{a, c, e\}$ е идеал в R.

Задача 5. *Да се докаже, че множеството*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

е комутативна област с мултипликативна група $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$. *Поле ли е* $\mathbb{Z}[i]$*?*

Упътване: Ако $z = a + bi \in \mathbb{Z}[i]^*$, то съществува $t = c + di \in \mathbb{Z}[i]$ с $tz = 1$. Оттук $|t|^2|z|^2 = 1$ с $|t|^2 = c^2 + d^2, |z|^2 = a^2 + b^2 \in \mathbb{Z}^{\geq 0}$. Следователно $a^2 + b^2 = c^2 + d^2 = 1$ и $z \in \{\pm 1, \pm i\}$. Включването $\{\pm 1, \pm i\} \subseteq \mathbb{Z}[i]^*$ се проверява непосредствено.

Областта $\mathbb{Z}[i]$ не е поле, защото има ненулеви елементи, които не са обратими относно умножението.

Задача 6. *Дадени са подмножествата*

$$R_1 = \left\{ \begin{pmatrix} 0 & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ 0 & 0 & \dots & a_{2,n-1} & a_{2,n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_{n-1,n} \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix} \;\middle|\; a_{i,j} \in \mathbb{Q} \right\} \quad и$$

$$R_2 = \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n-1} & a_{1,n} \\ 0 & a_{2,2} & \dots & a_{2,n-1} & a_{2,n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & 0 & \dots & 0 & a_{n,n} \end{pmatrix} \;\middle|\; a_{i,j} \in \mathbb{Q} \right\} \subset M_{n,n}(\mathbb{Q})$$

на пръстена $M_{n,n}(\mathbb{Q})$ *на матриците от* n*-ти ред с рационални елементи. Да се определи кои* R_i *са подпръстени и кои* R_i *са идеали.*

Решение: Матрица $M = (M_{i,j})_{i,j=1}^n \in M_{n,n}(\mathbb{Q})$ принадлежи на R_1 точно когато $M_{i,j} = 0$ за $\forall n \geq i \geq j \geq 1$. Ако $A, B \in R_1$, то $(A - B)_{i,j} = A_{i,j} - B_{i,j} = 0$ и $(AB)_{i,j} = \sum\limits_{s=1}^{n} A_{i,s}B_{s,j} = \sum\limits_{i<s<j} A_{i,s}B_{s,j} = 0$ за $\forall n \geq i \geq j \geq 1$. Следователно R_1 е подпръстен на $M_{n,n}(\mathbb{Q})$. За

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix} \in M_{n,n}(\mathbb{Q}) \quad \text{и} \quad A = \begin{pmatrix} 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix} \in R_1$$

имаме

$$CA = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \notin R_1,$$

така че R_1 не е идеал на $M_{n,n}(\mathbb{Q})$.

Аналогични разглеждания доказват, че подмножеството R_2 е подпръстен, но не и идеал в $M_{n,n}(\mathbb{Q})$.

Твърдение 7. *Декартовото произведение $R = R_1 \times \ldots \times R_n$ на пръстените $R_1, \ldots, R_n$ е пръстен относно покомпонентно определените операции събиране*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

и умножение

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n).$$

Пръстенът R има единица тогава и само тогава, когато всички множители R_i имат единици 1_{R_i} и $1_R = (1_{R_1}, \ldots, 1_{R_n})$.

Пръстенът $R = R_1 \times \ldots \times R_n$ се нарича директно произведение на $R_1, \ldots, R_n$.

Директното произведение $R = R_1 \times \ldots \times R_n$ на R_i е комутативен пръстен тогава и само тогава, когато всички множители R_i са комутативни.

Доказателство: За произволни $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n), z = (z_1, \ldots, z_n)$ от $R = R_1 \times \ldots \times R_n$ е в сила асоциативният закон за събиране

$$(x+y)+z = ((x_1+y_1)+z_1, \ldots, (x_n+y_n)+z_n) = (x_1+(y_1+z_1), \ldots, x_n+(y_n+z_n)) = x+(y+z).$$

От комутативността на събирането в R_i за $\forall 1 \leq i \leq n$ получаваме комутативността на събирането

$$x + y = (x_1 + y_1, \ldots, x_n + y_n) = (y_1 + x_1, \ldots, y_n + x_n) = y + x$$

в R. Ако 0_{R_i} е нулевият елемент на R_i, то $0_R = (0_{R_1}, \ldots, 0_{R_n})$ е нула на R, съгласно

$$x + 0_R = (x_1 + 0_{R_1}, \ldots, x_n + 0_{R_n}) = (x_1, \ldots, x_n) = x \quad \text{за} \quad \forall x \in R = R_1 \times \ldots \times R_n.$$

Всеки елемент $x_i \in R_i$ има противоположен $-x_i \in R_i$, така че $x = (x_1, \ldots, x_n) \in R = R_1 \times \ldots \times R_n$ има противоположен $-x = (-x_1, \ldots, -x_n) \in R$, изпълняващ равенството

$$x + (-x) = (x_1 + (-x_1), \ldots, x_n + (-x_n)) = (0_{R_1}, \ldots, 0_{R_n}) = 0_R.$$

С това проверихме, че $R = R_1 \times \ldots \times R_n$ е абелева група относно покомпоненнтното събиране.

Покомпонентното умножение в $R = R_1 \times \ldots \times R_n$ е асоциативно, съгласно асоциативността на умножението в R_i за $\forall 1 \leq i \leq n$. По-точно,

$$(xy)z = ((x_1y_1)z_1, \ldots, (x_ny_n)z_n) = (x_1(y_1z_1), \ldots, x_n(y_nz_n)) = x(yz) \quad \text{за} \quad \forall x, y, z \in R.$$

Дистрибутивните закони за събиране и умножение в R са директно следствие от дистрибутивните закони за събиране и умножение в R_i,

$$(x + y)z = ((x_1 + y_1)z_1, \ldots, (x_n + y_n)z_n) = (x_1z_1 + y_1z_1, \ldots, x_nz_n + y_nz_n) =$$

$$= (x_1z_1, \ldots, x_nz_n) + (y_1z_1, \ldots, y_nz_n) = xz + yz \quad \text{за} \quad \forall x, y, z \in R,$$

$$x(y + z) = (x_1(y_1 + z_1), \ldots, x_n(y_n + z_n)) = (x_1y_1 + x_1z_1, \ldots, x_ny_n + x_nz_n) =$$

$$= (x_1y_1, \ldots, x_ny_n) + (x_1z_1, \ldots, x_nz_n) = xy + xz \quad \text{за} \quad \forall x, y, z \in R.$$

Следователно $R = R_1 \times \ldots \times R_n$ е пръстен относно покомпонентно определените събиране и умножение.

Елементът $1_R = (e_1, \ldots, e_n) \in R = R_1 \times \ldots \times R_n$ е единица в R точно когато

$$1_R x = x = x 1_R \quad \text{за} \quad \forall x \in R = R_1 \times \ldots \times R_n,$$

$$(e_1 x_1, \ldots, e_n x_n) = (x_1, \ldots, x_n) = (x_1 e_1, \ldots, x_n e_n) \quad \text{за} \quad \forall x \in R = R_1 \times \ldots \times R_n.$$

Последното е еквивалентно на $e_i x_i = x_i = x_i e_i$ за $\forall x_i \in R_i$, така че $1_R = (e_1, \ldots, e_n)$ е единица в $R = R_1 \times \ldots \times R_n$ тогава и само тогава, когато $e_i = 1_{R_i}$ са единиците на R_i за $\forall 1 \leq i \leq n$.

Пръстенът R е комутативен, ако

$$xy = yx \quad \text{за} \quad \forall x, y \in R,$$

$$(x_1 y_1, \ldots, x_n y_n) = (y_1 x_1, \ldots, y_n x_n) \quad \text{за} \quad \forall x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in R.$$

Последното е в сила тогава и само тогава, когато $x_i y_i = y_i x_i$ за $\forall x_i, y_i \in R_i$. Това доказва, че R е комутативен пръстен точно тогава, когато всички множители R_i са комутативни пръстени, Q.E.D.

Задача 8. *Да разгледаме директното произведение $\mathbb{Z}_3 \times \mathbb{Z}_3$ на пръстена $\mathbb{Z}_3$ на остатъците при деление на 3 със себе си и подмножествата*

$$R_1 = \{(a, \overline{0}) \mid a \in \mathbb{Z}_3\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3,$$

$$R_2 = \{(\overline{1}, a) \mid a \in \mathbb{Z}_3\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3,$$

$$R_3 = \{(a, a) \mid a \in \mathbb{Z}_3\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3,$$

$$R_4 = \{(a, -a) \mid a \in \mathbb{Z}_3\} \subset \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Да се определи кои R_i са подпръстени и кои R_i са идеали в $\mathbb{Z}_3 \times \mathbb{Z}_3$.

Решение: (i) Подмножеството $R_1 \subset \mathbb{Z}_3 \times \mathbb{Z}_3$ е подгрупа на $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$, съгласно

$$(a, \overline{0}) - (b, \overline{0}) = (a - b, \overline{0}) \in R_1 \quad \text{за} \quad \forall (a, \overline{0}), (b, \overline{0}) \in R_1.$$

За произволни $(a, \overline{0}) \in R_1$ и $(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_3$ са в сила равенствата

$$(a, \overline{0})(x, y) = (x, y)(a, \overline{0}) = (ax, \overline{0}) \in R_1,$$

така че R_1 е идеал на $\mathbb{Z}_3 \times \mathbb{Z}_3$.

(ii) Подмножеството $R_2 \subset \mathbb{Z}_3 \times \mathbb{Z}_3$ не е подгрупа на адитивната група $(\mathbb{Z}_3 \times \mathbb{Z}_3, +)$, защото

$$(\overline{1}, a) - (\overline{1}, b) = (\overline{0}, a - b) \notin R_2 \quad \text{за} \quad \forall (\overline{1}, a), (\overline{1}, b) \in R_2.$$

Следователно R_2 не е нито подпръстен, нито идеал на $\mathbb{Z}_3 \times \mathbb{Z}_3$.

(iii) От

$$(a, a) - (b, b) = (a - b, a - b) \in R_3 \quad \text{за} \quad \forall (a, a), (b, b) \in R_3$$

следва, че $(R_3,+)$ е подгрупа на $(\mathbb{Z}_3\times\mathbb{Z}_3,+)$. За произволни $(\varepsilon,\varepsilon)\in R_3$ и $(\eta,-\eta)\in\mathbb{Z}_3\times\mathbb{Z}_3$ с $\varepsilon,\eta\in\{\pm\overline{1}\}=\mathbb{Z}_3^*$ имаме

$$(\varepsilon,\varepsilon)(\eta,-\eta)=(\eta,-\eta)(\varepsilon,\varepsilon)=(\varepsilon\eta,-\varepsilon\eta)\notin R_3,$$

така че R_3 не е идеал на $\mathbb{Z}_3\times\mathbb{Z}_3$. Съгласно

$$(a,a)(b,b)=(ab,ab)\in R_3\quad\text{за}\quad\forall(a,a),(b,b)\in R_3,$$

стигаме до извода, че R_3 е подпръстен на $\mathbb{Z}_3\times\mathbb{Z}_3$.

(iv) За $\forall(a,-a),(b,-b)\in R_4$ е в сила

$$(a,-a)-(b,-b)=(a-b,-(a-b))\in R_4,$$

така че $(R_4,+)$ е подгрупа на $(\mathbb{Z}_3\times\mathbb{Z}_3,+)$. От

$$(\varepsilon,-\varepsilon)(\eta,-\eta)=(\eta,-\eta)(\varepsilon,-\varepsilon)=(\varepsilon\eta,\varepsilon\eta)\notin R_4\quad\text{за}\quad\forall\varepsilon,\eta\in\{\pm\overline{1}\}=\mathbb{Z}_3^*$$

следва, че R_4 не е подпръстен на $\mathbb{Z}_3\times\mathbb{Z}_3$.

Задача 9. *Да се докаже, че ако I_α са идеали в пръстен R за всички $\alpha\in A$, то сечението $\cap_{\alpha\in A}I_\alpha$ е идеал в R.*

Решение: Ако $x,y\in\cap_{\alpha\in A}I_\alpha$, то $x,y\in I_\alpha$ за $\forall\alpha\in A$ и $x-y\in I_\alpha$ за $\forall\alpha\in A$, защото $(I_\alpha,+)$ са подгрупи на $(R,+)$. Следователно $x-y\in\cap_{\alpha\in A}I_\alpha$ и $(\cap_{\alpha\in A}I_\alpha,+)$ е подгрупа на $(R,+)$.

За произволни $x\in\cap_{\alpha\in A}I_\alpha$ и $r\in R$ имаме $rx,xr\in I_\alpha$ за $\forall\alpha\in I_\alpha$, защото идеалите I_α в R издържат леви и десни умножения с $r\in R$. Това доказва, че $\cap_{\alpha\in A}I_\alpha\trianglelefteq R$.

Задача 10. *Ако I и J са идеали в пръстен R, то множеството*

$$I+J=\{\alpha+\beta\ \mid\ \alpha\in I,\quad\beta\in J\}$$

се нарича сума на I и J. Да се докаже, че сумата $I+J$ на идеали I и J в пръстен R е идеал в R.

Решение: Ако $x_1+y_1,x_2+y_2\in I+J$ с $x_i\in I$, $y_i\in J$, то

$$(x_1+y_1)-(x_2-y_2)=(x_1-x_2)+(y_1-y_2)\in I+J,$$

защото $x_1-x_2\in I$, $y_1-y_2\in J$ за $(I,+)\leq(R,+)$, $(J,+)\leq(R,+)$. Следователно $(I+J,+)$ е подгрупа на $(R,+)$.

Ако $x+y\in I+J$ с $x\in I$, $y\in J$, и $r\in R$, то $r(x+y)=rx+ry\in I+J$, защото $rx\in I\trianglelefteq R$, $ry\in J\trianglelefteq R$. Аналогично, $(x+y)r=xr+yr\in I+J$, съгласно $xr\in I\trianglelefteq R$, $yr\in J\triangleleft R$ и $I+J$ е идеал в R.

Задача 11. *Ако I и J са идеали в пръстен R, то множеството*

$$IJ=\left\{\sum_{i=1}^{n}\alpha_i\beta_i\ \ \middle|\ \ \alpha_i\in I,\quad\beta_i\in J\right\}$$

се нарича произведение на идеалите I и J. Да се докаже, че произведението IJ на идеали I и J в пръстен R е идеал в R.

Решение: Ако $\sum\limits_{i=1}^{n} \alpha_i\beta_i, \sum\limits_{j=1}^{m} \alpha'_j\beta'_j \in IJ$ с $\alpha_i, \alpha'_j \in I$, $\beta_i, \beta'_j \in J$, то

$$\sum_{i=1}^{n} \alpha_i\beta_i - \sum_{j=1}^{m} \alpha'_j\beta'_j = \sum_{i=1}^{n} \alpha_i\beta_i + \sum_{j=1}^{m} [-(\alpha'_j\beta'_j)] = \sum_{i=1}^{n} \alpha_i\beta_i + \sum_{j=1}^{m} (-\alpha'_j)\beta'_j \in IJ,$$

защото $-\alpha'_j \in (I, +) \leq (R, +)$. Следователно $(IJ, +) \leq (R, +)$.

За $\forall \sum\limits_{i=1}^{n} \alpha_i\beta_i \in IJ$ с $\alpha_i \in I$, $\beta_i \in J$ и $\forall r \in R$ имаме

$$r\left(\sum_{i=1}^{n} \alpha_i\beta_i\right) = \sum_{i=1}^{n} (r\alpha_i)\beta_i \in IJ, \quad \left(\sum_{i=1}^{n} \alpha_i\beta_i\right) r = \sum_{i=1}^{n} \alpha_i(\beta_i r) \in IJ,$$

съгласно $r\alpha_i \in I \trianglelefteq R$, $\beta_i r \in J \trianglelefteq R$. Следователно IJ е идеал в R.

Задача 12. *За произволни естествени числа $m, n \in \mathbb{Z}$ с най-голям общ делител $d = (m, n)$ и най-малко общо кратно $\mu = [m, n]$ е в сила:*
(i) $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$;
(ii) $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$;
(iii) $m\mathbb{Z} \cap n\mathbb{Z} = \mu\mathbb{Z}$.

Решение: (i) По определение,

$$(m\mathbb{Z})(n\mathbb{Z}) = \left\{ \sum_{i=1}^{k} (mx_i)(ny_i) = mn\left(\sum_{i=1}^{k} x_i y_i\right) \;\middle|\; k \in \mathbb{N}, \quad x_i, y_i \in \mathbb{Z} \right\} \subseteq mn\mathbb{Z}.$$

Обратно, за $\forall z \in \mathbb{Z}$ имаме $mnz = (m.1)(n.z) \in (m\mathbb{Z})(n\mathbb{Z})$, така че $mn\mathbb{Z} \subseteq (m\mathbb{Z})(n\mathbb{Z})$ и $(m\mathbb{Z})(n\mathbb{Z}) = mn\mathbb{Z}$.

(ii) От една страна, $m, n \in d\mathbb{Z}$, защото d дели m и n. Идеалът $d\mathbb{Z}$ е затворен относно умножение с цели числа, така че $m\mathbb{Z} \subseteq d\mathbb{Z}$ и $n\mathbb{Z} \subseteq d\mathbb{Z}$. Следователно $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$, защото $(d\mathbb{Z}, +)$ е подгрупа на $(\mathbb{Z}, +)$. За обратното включване $d\mathbb{Z} \subseteq m\mathbb{Z}+n\mathbb{Z}$ използваме тъждеството на Безу $d = mu + nv$ с цели $u, v \in \mathbb{Z}$. По-точно, от $mu \in m\mathbb{Z}$ и $nv \in n\mathbb{Z}$ следва $d = mu + nv \in m\mathbb{Z} + n\mathbb{Z}$. Сумата $m\mathbb{Z} + n\mathbb{Z}$ на идеалите $m\mathbb{Z}$, $n\mathbb{Z}$ е идеал в $\mathbb{Z}$, така че $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$ и $d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}$.

(iii) Ако $\alpha \in m\mathbb{Z} \cap n\mathbb{Z}$, то m и n делят α, така че α е общо кратно на m и n. Оттук, най-малкото общо кратно μ на m и n дели α и $\alpha \in \mu\mathbb{Z}$. Това доказва вкрючването $m\mathbb{Z} \cap n\mathbb{Z} \subseteq \mu\mathbb{Z}$. Обратно, общото кратно μ на m и n се дели както на m, така и на n. Следователно $\mu \in m\mathbb{Z}$ и $\mu \in n\mathbb{Z}$, откъдето $\mu \in m\mathbb{Z} \cap n\mathbb{Z}$. Сечението $m\mathbb{Z} \cap n\mathbb{Z}$ на идеалите $m\mathbb{Z}$ и $n\mathbb{Z}$ е идеал в $\mathbb{Z}$, така че $\mu\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$ и $\mu\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$.

Задача 13. *Нека R е пръстен, а $I \subset J$ са идеали в R. Да се докаже, че I е идеал в J, J/I е идеал в R/I и*

$$(R/I) \,/\, (J/I) \simeq R/J.$$

Упътване: Разгледайте изображението

$$\varphi : R/I \longrightarrow R/J,$$

$$\varphi(r+I) = r+J \quad \text{за} \quad \forall r \in R.$$

Проверете, че φ е коректно определено, т.е. от $r+I = r_1+I$ следва $r+J = r_1+J$. Обяснете защо I е идеал във всеки подпръстен S на R, съдържащ I. Докажете, че φ е епиморфизъм на пръстени и приложете Теоремата за хомоморфизмите на пръстени.

Задача 14. *Нека I е идеал в пръстен R, а S е подпръстен на R. Да се докаже, че $S+I$ е подпръстен на R, I е идеал в $S+I$, $S \cap I$ е идеал в S и*

$$S/(S \cap I) \simeq (S+I)/I.$$

Упътване: Проверете, че $(S+I,+)$ е подгрупа на $(R,+)$. За произволни $s_j + i_j \in S+I$, $1 \leq j \leq 2$ имаме $(s_1+i_1)(s_2+i_2) = s_1s_2 + (s_1i_2 + s_2i_1 + i_1i_2) \in S+I$ с $s_1s_2 \in S$, $s_1i_2 + s_2i_1 + i_1i_2 \in I$. Следователно $S+I$ е подпръстен на R, съдържащ идеала I. Докажете, че изображението

$$\psi : S \longrightarrow (S+I)/I,$$

$$\psi(s) = s+I \quad \text{за} \quad \forall s \in S$$

е епиморфизъм на пръстени и приложете Теоремата за хомоморфизмите на пръстени.

Да разгледаме диаграмата от влагания

$$\begin{array}{ccc} S & \longrightarrow & S+I \\ \uparrow & & \uparrow \\ S \cap I & \longrightarrow & I \end{array} .$$

Задача 14 твърди, че факторите по протежение на вертикалите са изоморфни.

Задача 15. *Нека R е пръстенът $R = \{a+b\sqrt{3} \mid a,b \in \mathbb{Z}\}$, а I е главният идеал на R, породен от $3+2\sqrt{3}$. Да се докаже, че*

$$I = \{a+b\sqrt{3} \in R \mid a \equiv 0(mod\ 3)\}$$

и фактор-пръстенът $R/I \cong \mathbb{Z}_3$ е изморфен на пръстена $\mathbb{Z}_3$ от остатъци при деление с 3.

Решение: За произволни $x,y \in \mathbb{Z}$ имаме

$$(3+2\sqrt{3})(x+y\sqrt{3}) = (3x+6y) + (2x+3y)\sqrt{3} \quad \text{с} \quad 3x+6y \equiv 0(\text{mod } 3).$$

Следователно $I \subseteq \{a+b\sqrt{3} \in R \mid a \equiv 0(\text{mod } 3)\}$.

Обратно, ако $a,b \in \mathbb{Z}$, $a \equiv 0(\text{mod } 3)$, то системата

$$\left| \begin{array}{lll} 3x & +6y & = a \\ 2x & +3y & = b \end{array} \right.$$

има целочислено решение $x = -a+2b, y = 2\frac{a}{3} - b \in \mathbb{Z}$. В резултат получаваме включването $\{a+b\sqrt{3} \in R \mid a \equiv 0(\text{mod } 3)\} \subseteq I$ и съвпадението $I = \{a+b\sqrt{3} \in R \mid a \equiv 0(\text{mod } 3)\}$.

Изображението

$$\varphi : R \longrightarrow \mathbb{Z}_3,$$
$$\varphi(a + b\sqrt{3}) = a(\text{mod } 3)$$

е хомоморфизъм на пръстени, съгласно

$$\varphi((a_1 + b_1\sqrt{3}) + (a_2 + b_2\sqrt{3})) = \varphi((a_1 + a_2) + (b_1 + b_2)\sqrt{3}) = (a_1 + a_2)(\text{mod } 3) =$$

$$= a_1(\text{mod } 3) + a_2(\text{mod } 3) = \varphi(a_1 + b_1\sqrt{3}) + \varphi(a_2 + b_2\sqrt{3}) \quad \text{и}$$

$$\varphi((a_1+b_1\sqrt{3})(a_2+b_2\sqrt{3})) = \varphi((a_1a_2+3b_1b_2)+(a_1b_2+a_2b_1)\sqrt{3}) = (a_1a_2+3b_1b_2)(\text{mod } 3) =$$

$$= a_1a_2(\text{mod } 3) = [a_1(\text{mod } 3)][a_2(\text{mod } 3)] = \varphi(a_1 + b_1\sqrt{3})\varphi(a_2 + b_2\sqrt{3}).$$

Съгласно Теоремата за хомоморфизмите на пръстени,

$$R/I \simeq R/\ker(\varphi) \simeq \text{im}(\varphi) = \mathbb{Z}_3.$$

Задача 16. *Нека R е пръстенът $R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, а I е главният идеал на R, породен от $3 + \sqrt{2}$. Да се докаже, че*

$$I = \{a + b\sqrt{2} \in R \mid a - 3b \equiv 0 \ (mod\ 7)\}$$

и фактор-пръстенът $R/I \cong \mathbb{Z}_7$ е изморфен на пръстена $\mathbb{Z}_7$ от остатъци при деление със 7.

Решение: Главният идеал $I = (3 + \sqrt{2})$ се състои от числата

$$(3 + \sqrt{2})(x + y\sqrt{2}) = (3x + 2y) + (x + 3y)\sqrt{2} \quad \text{за произволни} \quad x, y \in \mathbb{Z}.$$

Съгласно $(3x+2y)-3(x+3y) = -7y \equiv 0(\text{mod } 7)$, идеалът I се съдържа в множеството $\{a + b\sqrt{2} \in R \mid a - 3b \equiv 0(\text{mod } 7)\}$.

Обратно, за произволни $a, b \in \mathbb{Z}$, с $a - 3b \equiv 0(\text{mod } 7)$, системата уравнения

$$\left| \begin{array}{lll} 3x & +2y & = a \\ x & +3y & = b \end{array} \right.$$

има целочислено решение

$$x = \frac{3a - 2b}{7} = b + \frac{3(a - 3b)}{7}, y = \frac{-a + 3b}{7} \in \mathbb{Z},$$

откъдето $\{a+b\sqrt{2} \in R \mid a-3b \equiv 0(\text{mod } 7)\} \subseteq I$ и $I = \{a+b\sqrt{2} \in R \mid a-3b \equiv 0(\text{mod } 7)\}$.

Изображението

$$\psi : R \longrightarrow \mathbb{Z}_7,$$
$$\psi(a + b\sqrt{2}) = a - 3b(\text{mod } 7)$$

е хомоморфизъм на пръстени, съгласно

$$\psi((a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})) = \psi((a_1+a_2)+(b_1+b_2)\sqrt{2}) = [(a_1+a_2)-3(b_1+b_2)](\text{mod } 7) =$$

$$= [(a_1 - 3b_1)(\mathrm{mod}\ \ 7)] + [(a_2 - 3b_2)(\mathrm{mod}\ \ 7)] = \psi(a_1 + b_1\sqrt{2}) + \psi(a_2 + b_2\sqrt{2}) \quad \text{и}$$

$$\psi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = \psi((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}) =$$

$$= [(a_1a_2 + 2b_1b_2) - 3(a_1b_2 + a_2b_1)](\mathrm{mod}\ \ 7) = [(a_1a_2 + 9b_1b_2) - 3(a_1b_2 + a_2b_1)](\mathrm{mod}\ \ 7) =$$

$$= [(a_1 - 3b_1)(a_2 - 3b_2)](\mathrm{mod}\ \ 7) = [(a_1 - 3b_1)(\mathrm{mod}\ \ 7)][(a_2 - 3b_2)(\mathrm{mod}\ \ 7)] =$$

$$= \psi(a_1 + b_1\sqrt{2})\psi(a_2 + b_2\sqrt{2}).$$

Съгласно Теоремата за хомоморфизмите на пръстени,

$$R/I = R/\ker(\psi) \simeq \mathrm{im}(\psi) = \mathbb{Z}_7.$$

Задача 17. *Да се докаже, че:*

(i) множеството

$$R = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \,\middle|\, a, b, c \in \mathbb{Z} \right\}.$$

е пръстен относно обичайните операции събиране и умножение на матрици;

(ii) за произволно просто число p подмножествата

$$I = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \in R \,\middle|\, p \ \textit{дели}\ c \right\}, \quad J = \left\{ \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) \in R \,\middle|\, p \ \textit{дели}\ a \ \textit{и}\ c \right\}$$

са идеали в R, R/I е поле и R/J не е поле.

Упътване: (i) Събирането на матрици е поелементно, така че акисомите за абелева група $(R, +)$ се свеждат до аксиомите за абелева група $(\mathbb{Z}, +)$. Проверете непосредствено асициативния закон за умножение на целочислени матрици и дискрибутивния закон за събиране и умножение на целочислени матрици.

(ii) Докажете, че изображението

$$\varphi : R \longrightarrow \mathbb{Z}_p,$$

$$\varphi \left(\begin{array}{cc} a & b \\ 0 & c \end{array} \right) = c(\mathrm{mod}\ \ p)$$

е епиморфизъм на пръстени с ядро I и приложете Теоремата за хомоморфизмите на пръстени.

За да проверим, че R/J не е поле избираме произволни $a_1, a_2, c_1, c_2 \in \mathbb{Z}$, взаимно прости p. Тогава ненулевите елементи

$$x = \left(\begin{array}{cc} a_1 & b_1 \\ 0 & pc_1 \end{array} \right) + J \quad \text{и} \quad y = \left(\begin{array}{cc} pa_2 & b_2 \\ 0 & c_2 \end{array} \right) + J \in R/J$$

имат нулево произведение

$$xy = \left(\begin{array}{cc} pa_1a_2 & a_1b_2 + b_1c_2 \\ 0 & pc_1c_2 \end{array} \right) + J = J,$$

така че фактор-пръстенът R/J има делители на нулата и не е поле.

Задача 18. *Дадено е множеството от матрици*

$$\mathbb{H} = \left\{ \begin{pmatrix} x & y \\ -\overline{y} & \overline{x} \end{pmatrix} \;\mid\; x, y \in \mathbb{C} \right\} \subset \mathbb{C}_{2\times 2}.$$

Да се докаже, че:

(i) $\mathbb{H}$ *е некомутативно тяло относно обичайните операции събиране и умножение на матрици, което се нарича тяло на кватернионите;*

(ii) $\mathbb{H}$ *е линейно пространство над* $\mathbb{R}$ *с базис*

$$E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix};$$

(iii) матриците $\pm E_2, \pm I, \pm J, \pm K$ *образуват подгрупа на общата линейна група* $Gl_2(\mathbb{C}) = \{X \in \mathbb{C}_{2\times 2} \;\mid\; \det(A) \neq 0\}$*, наречена група на кватернионите* $\mathbb{Q}_8$ *със съотношения*

$$I^2 = J^2 = K^2 = -E_2, \quad IJ = -JI = K, \quad JK = -KJ = I, \quad KI = -IK = J.$$

Упътване: Използвайти изброените съотношения, за да обосновете, че подмножеството $\mathbb{Q}_8 = \{\pm E_2, \pm I, \pm J, \pm K\} \subset Gl_2(\mathbb{C})$ е затворено относно умножение и обръщане.

Задача 19. *В пръстена* $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \;\mid\; a, b \in \mathbb{Z}\}$ *е даден идеалът*

$$I = (1 + \sqrt{-5}, 1 - \sqrt{-5}) = \{(1 + \sqrt{-5})\alpha + (1 - \sqrt{-5})\beta \;\mid\; \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]\},$$

породен от $1 + \sqrt{-5}$ *и* $1 - \sqrt{-5}$*. Да се докаже, че:*

(i) $I = \{a + b\sqrt{-5} \;\mid\; a \equiv b (\mathrm{mod}\ 2)\}$*;*

(ii) $2\mathbb{Z}[\sqrt{-5}] = (2) \subsetneq I \subsetneq (1) = \mathbb{Z}[\sqrt{-5}]$*;*

(iii) числото 2 *от идеала* I *не принадлежи на нито един главен идеал* $(a_o + b_o\sqrt{-5})$*, различен от* (1) *и* (2)*, така че идеалът* I *не е главен.*

Упътване: (i) За произволни цели x, y, z, t имаме

$$(1 + \sqrt{-5})(x + y\sqrt{-5}) + (1 - \sqrt{-5})(z + t\sqrt{-5}) = (x - 5y + z + 5t) + (x + y - z + t)\sqrt{-5} \quad \text{с}$$

$$x - 5y + z + 5t \equiv x + y - z + t (\mathrm{mod}\ 2).$$

Това доказва $I \subseteq \{a + b\sqrt{-5} \;\mid\; a \equiv b (\mathrm{mod}\ 2)\}$. Обратно, ако $a, b \in \mathbb{Z}$, $a \equiv b (\mathrm{mod}\ 2)$, то за произволни $y, t \in \mathbb{Z}$ системата уравнения

$$\left| \begin{array}{cccc|c} x & -5y & +z & +5t & = a \\ x & +y & -z & +t & = b \end{array} \right.$$

има цели решения

$$x = \frac{a+b}{2} + 2y - 3t, \quad z = \frac{a-b}{2} + 3y - 2t.$$

Следователно $\{a + b\sqrt{-5} \;\mid\; a \equiv b (\mathrm{mod}\ 2)\} \subseteq I$.

(ii) От $1+\sqrt{-5}, 1-\sqrt{-5} \in I$ следва, че $2 = (1+\sqrt{-5})+(1-\sqrt{-5}) \in I$ и $(2) \subseteq I \lhd \mathbb{Z}[\sqrt{-5}]$. Допускането $(2) = I$ води до $1 + \sqrt{-5} = 2(x + y\sqrt{-5})$ за някакви цели $x, y \in \mathbb{Z}$. Оттук $x = y = \frac{1}{2}$, което е противоречие, доказващо $(2) \subsetneq I$.

По определение $I \subseteq \mathbb{Z}[\sqrt{-5}]$. Съгласно (i), $1 \notin I$, така че $I \subsetneq \mathbb{Z}[\sqrt{-5}]$.

(iii) От предположението $(a_o + b_o\sqrt{-5})(x + y\sqrt{-5}) = 2$ за $x, y \in \mathbb{Z}$ следва, че

$$(a_o^2 + 5b_o^2)(x^2 + 5y^2) = |a_o + b_o\sqrt{-5}|^2|x + y\sqrt{-5}|^2 = 4$$

с $a_o^2 + 5b_o^2, x^2 + 5y^2 \in \mathbb{N}$. Ако $a_o^2 + 5b_o^2 = 1$, то $a_o = \pm 1$, $b_o = 0$ и $(a_o + b_o\sqrt{-5}) = (\pm 1) = (1)$. Уравнението $a_o^2 + 5b_o^2 = 2$ няма решение в цели числа a_o, b_o. Ако $a_o^2 + 5b_o^2 = 4$, то $x^2 + 5y^2 = 1$, откъдето $x + \sqrt{-5}y = \pm 1$ и $a_o + b_o\sqrt{-5} = \pm 2$, което противоречи на $(2) \neq I$.

Задача 20. *Да се намерят последните две цифри на естествените числа (i)* 9^{2012}*; (ii)* 7^{2013}*; (iii)* 11^{2014}.

Решение: (i) Естественото число 100 е взаимно просто с 9. Следователно е изпълнена теоремата на Ойлер $9^{\varphi(100)} \equiv 1(\text{mod } 100)$. Функцията на Ойлер

$$\varphi(100) = \varphi(2^2.5^2) = \varphi(2^2)\varphi(5^2) = 2.5.4 = 40,$$

така че $9^{40} \equiv 1(\text{mod } 100)$. След деление с частно и остатък $2012 = 40.50 + 12$ и получаваме

$$9^{2012} = (9^{40})^{50}.9^{12}(\text{mod } 100) = 9^{12}(\text{mod } 100).$$

Последователно пресмятаме, че $9^3 \equiv 29(\text{mod } 100)$, откъдето

$$9^6 = (9^3)^2 \equiv 29^2 \equiv 41(\text{mod } 100)$$

и $9^{12} = (9^6)^2 \equiv 41^2(\text{mod } 100) \equiv 81(\text{mod } 100)$. Окончателно получаваме, че

$$9^{2012} \equiv 9^{12}(\text{mod } 100) \equiv 81(\text{mod } 100).$$

Отговор: (ii) $7^{2013} \equiv 7(\text{mod } 100)$; (iii) $11^{2014} \equiv 41(\text{mod } 100)$.

Задача 21. *Да се намери остатъкът на:*

(i) 23^{57} *при деление с* 28*;*

(ii) 5^{67} *при деление с* 36*;*

(iii) 33^{55} *при деление с* 40.

Решение: (i) Естествените числа 23 и 28 са взаимно прости. Следователно е в сила теоремата на Ойлер $23^{\varphi(28)} \equiv 1(\text{mod } 28)$. Функцията на Ойлер

$$\varphi(28) = \varphi(2^2.7) = \varphi(2^2)\varphi(7) = 2.6 = 12.$$

Делим 57 на 12 с частно и остътък и получаваме $57 = 12.4 + 9$. Оттук

$$23^{57} = (23^{12})^4.23^9 \equiv 23^9(\text{mod } 28) \equiv (-5)^9(\text{mod } 28) = -5^9(\text{mod } 28).$$

Пресмятаме последователно $5^3 \equiv 13(\text{mod } 28)$, $5^6 = (5^3)^2 \equiv 13^2(\text{mod } 28) \equiv 1(\text{mod } 28)$. Оттук следва, че $5^9 \equiv 13(\text{mod } 28)$ и

$$23^{57} \equiv -5^9(\text{mod } 28) \equiv -13(\text{mod } 28) \equiv 15(\text{mod } 28).$$

Отговор: (ii) $\varphi(36) = 12$, $5^{67} \equiv 5(\text{mod } 36)$; (iii) $\varphi(40) = 16$, $33^{55} \equiv 17(\text{mod } 40)$.