Примерни задачи за пръстени по Алгебра 2

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

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

където p е фиксирано просто число;

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

където p е фиксирано просто число;

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

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

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:*

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

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

Отговор: (i) Не. (ii) Да.

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.

(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. Докажете, че такова подмножество $I = \{r(i_1) = a = 0_R, r(i_2), \ldots r(i_p)\}$ 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 $r(i_1), \ldots, r(i_p)$ в стълбовете с номера $i_1, \ldots, i_p$. Комутативността на събирането в пръстена R е еквивалентна на симетричността на матрицата за събиране. Затова $(I = \{r(i_1) = a = 0_R, r(i_2), \ldots, +) \leq (R, +)$ точно когато за всяко $1 \leq k \leq p$ стълбът с номер i_k от таблицата за събиране съдържа пермутация на $r(i_1), \ldots, r(i_p)$ в редовете с номера $i_1, \ldots, i_p$.

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

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

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 $M_{n,n}(\mathbb{Q})$.

Задача 7. *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.*

Задача 8. *Ако I и J са идеали в пръстен R, то множеството*

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

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.

Задача 9. *Ако I и J са идеали в пръстен R, то множеството*

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

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.

Задача 10. *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,

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

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 11. *Идеалите $I_1, \ldots, I_n$ в комутативен пръстен с единица R са взаимно прости, ако $I_a + I_b = R$ за всички $a \neq b$. Да се докаже, че идеалите $m_1\mathbb{Z}, \ldots, m_n\mathbb{Z}$ в пръстена $\mathbb{Z}$ на целите числа са взаимно прости тогава и само тогава, когато числата m_a и m_b са взаимно прости за всички $a \neq b$.*

Теорема 12. (Китайска теорема за остатъците) *Нека $I_1, \ldots, I_n$ са два по два взаимно прости идеала в комутативен пръстен с единица R и $c_1, \ldots, c_n \in R$. Тогава съществува $c \in R$, така че $c + I_j = c_j + I_j$ за $\forall 1 \leq j \leq n$.*

Доказателство: С индукция по $n \geq 2$, ако $I_1 + I_2 = R$, то съществуват $\alpha_1 \in I_1$ и $\alpha_2 \in I_2$ с $\alpha_1 + \alpha_2 = 1_R$. Непосредствено се проверява, че

$$c = c_1\alpha_2 + c_2\alpha_1 \in R$$

изпълнява условията $c + I_j = c_j + I_j$ за $\forall 1 \leq j \leq 2$.

В общия случай, от $I_1 + I_j = R$ за $\forall 2 \leq j \leq n$ следва съществуването на $\alpha_j \in I_1$ и $\beta_j \in I_j$ с $\alpha_j + \beta_j = 1_R$ за $\forall 2 \leq j \leq n$. Почленното умножение на тези равенства дава

$$1_R = (\alpha_2 + \beta_2)(\alpha_3 + \beta_3)\ldots(\alpha_n + \beta_n) = \alpha + \beta_2 \ldots \beta_n \in I_1 + I_2 \ldots I_n,$$

където $\alpha \in I_1$ е сумата на онези произведения, в които участва поне един множител $\alpha_j \in I_1$. Оттук $I_1 + I_2 \ldots I_n = R$. По индукционно предположение съществува $c' \in R$ с $c' + I_j = c_j + I_j$ за $\forall 2 \leq j \leq n$. Сега

$$c = c_1\beta_2 \ldots \beta_n + c'\alpha \in R$$

изпълнява равенствата $c + I_1 = c_1 + I_1$ и $c + I_2 \ldots I_n = c' + I_2 \ldots I_n$ за $\forall 2 \leq j \leq n$, откъдето и $c + I_j = c' + I_j = c_j + I_j$, съгласно $I_2 \ldots I_n \subseteq I_j$ за $\forall 2 \leq j \leq n$, Q.E.D.

Следствие 13. *Ако R е комутативен пръстен с единица 1_R, а $I_1, \ldots, I_n$ са два по два взаимно прости идеала в R, то произведението им*

$$I_1 \ldots I_n = I_1 \cap \ldots \cap I_n$$

съвпада със сечението.

Доказателство: За произволни идеали I_j в пръстен R имаме $I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n$. С индукция по $n \geq 2$ ще проверим, че ако $I_1, \ldots, I_n$ са два по два взаимно прости идеала в комутативен пръстен с единица R, то

$$I_1 \cap \ldots \cap I_n \subseteq I_1 \ldots I_n,$$

откъдето $I_1 \cap \ldots \cap I_n = I_1 \ldots I_n$. Наистина, от $I_1 + I_2 = R$ следва съществуването на $\alpha_1 \in I_1$ и $\alpha_2 \in I_2$ с $\alpha_1 + \alpha_2 = 1_R$. Оттук, за произволен елемент $\gamma \in I_1 \cap I_2$ имаме

$$\gamma = \gamma.1_R = \alpha_1\gamma + \gamma\alpha_2 \in I_1I_2,$$

съгласно $\alpha_1 \in I_1$, $\gamma \in I_2$ и $\gamma \in I_1$, $\alpha_2 \in I_2$. В общия случай, доказахме че ако $I_1, \ldots, I_n$ са два по два взаимно прости идеала, то I_1 и произведението $I_2 \ldots I_n$ на останалите идеали са взаимно прости, $I_1 + I_2 \ldots I_n = R$. Оттук съществуват $\alpha_1 \in I_1$ и $\beta \in I_2 \ldots I_n = I_2 \cap \ldots \cap I_n$ с $\alpha_1 + \beta = 1_R$. За произволен елемент $\gamma \in I_1 \cap I_2 \cap \ldots \cap I_n = I_1 \cap (I_2 \ldots I_n)$ имаме

$$\gamma = \gamma.1_R = \alpha_1\gamma + \gamma\beta \in I_1(I_2 \ldots I_n),$$

съгласно $\alpha_1 \in I_1$, $\gamma \in I_2 \dots I_n$ и $\gamma \in I_1$, $\beta \in I_2 \dots I_n$. Оттук следва включването

$$I_1 \cap \ldots \cap I_n \subseteq I_1 \dots I_n$$

и съвпадението $I_1 \cap \ldots \cap I_n = I_1 \dots I_n$. Теоремата за хомоморфизмите на пръстени дава изоморфизма на пръстени

$$R/I_1 \dots I_n = R/\ker(\varphi) \simeq \mathrm{im}(\varphi) = (R/I_1) \times \ldots \times (R/I_n)\,,$$

Q.E.D.

Следствие 14. *Нека $m_1, \dots, m_n \in \mathbb{N} \setminus \{1\}$ са две по две взаимно прости естествени числа, c е цяло число. Тогава целите числа x, удовлетворяващи сравненията*

$$|x \equiv c(\mathrm{mod}\ \ m_j) \quad за \quad \forall 1 \leq j \leq n \tag{1}$$

образуват съседния клас $c + m_1 \dots m_n\mathbb{Z} \in \mathbb{Z}_{m_1 \dots m_n}$.

Доказателство: От $m_1 \dots m_n\mathbb{Z} \subset m_j\mathbb{Z}$ следва, че всяко

$$c' = c + m_1 \dots m_n z \in c + m_1 \dots m_n\mathbb{Z}$$

е решение на (1). Обратно, ако $c'' \equiv c(\mathrm{mod}\ \ m_j)$ за $\forall 1 \leq j \leq n$, то $c'' - c \in m_j\mathbb{Z}$ за $\forall 1 \leq j \leq n$. Следователно

$$c'' - c \in m_1\mathbb{Z} \cap \dots m_n\mathbb{Z} = (m_1\mathbb{Z}) \dots (m_n\mathbb{Z}) = m_1 \dots m_n\mathbb{Z}$$

и $c'' \in c + m_1 \dots m_n\mathbb{Z}$, Q.E.D.

Задача 15. *Да се намерят всички цели решения на системите сравнения*

$$(i)\left|\begin{array}{llll} 2x & \equiv -1 & (\mathrm{mod} & 3) \\ 3x & \equiv -1 & (\mathrm{mod} & 5) \end{array}\right. ;(ii)\left|\begin{array}{llll} 5x & \equiv 1 & \mathrm{mod} & 6) \\ 5x & \equiv 6 & (\mathrm{mod} & 7) \end{array}\right. ;(iii)\left|\begin{array}{llll} 2x & \equiv 1 & (\mathrm{mod} & 3) \\ 3x & \equiv 4 & (\mathrm{mod} & 5) \\ 5x & \equiv -2 & (\mathrm{mod} & 7) \end{array}\right. .$$

Решение: (i) Първо решаваме всяко от сравненията в системата. От $2x-(-1) = 3y_1$ с $y_1 \in \mathbb{Z}$ изразяваме

$$x = \frac{3y_1 - 1}{2} = y_1 + \frac{y_1 - 1}{2}.$$

Полагаме

$$z_1 := \frac{y_1 - 1}{2} \in \mathbb{Z}$$

и получаваме $y_1 = 2z_1 + 1$, $x = 3z_1 + 1$. Следователно $2x \equiv -1(\mathrm{mod}\ \ 3)$ има единствено решение $x \equiv 1(\mathrm{mod}\ \ 3)$. Аналогично, представяме $3x + 1 = 5y_2$ с $y_2 \in \mathbb{Z}$ във вида

$$x = \frac{5y_2 - 1}{3} = 2y_2 + \frac{(-y_2 - 1)}{3}.$$

Ако

$$z_2 := \frac{-y_2 - 1}{3} \in \mathbb{Z},$$

то $y_2 = -3z_2 - 1$ и $x = -5z_2 - 2$. Оттук $3x \equiv -1 (\text{mod } 5)$ има решение $x \equiv -2 (\text{mod } 5)$. С това сведохме системата сравнения (i) към системата

$$\left| \begin{array}{lll} x & \equiv 1 & (\text{mod } 3) \\ x & \equiv -2 & (\text{mod } 5) \end{array} \right. . \tag{2}$$

За да намерим едно решение $c \in \mathbb{Z}$ на тази система ще използваме доказателството на Китайската теорема за остатъците. По-точно, съгласно $1 = 6 + (-5)$ с $6 \in 3\mathbb{Z}$, $(-5) \in 5\mathbb{Z}$, цялото число $c = 6(-2) + (-5).1 = -17$ е решение на (2). Съгласно взаимната простота на 3 и 5, всички решения на (i) са $-17 + 15\mathbb{Z} = 13 + 15\mathbb{Z}$.

(ii) Решаваме поотделно дадените сравнения и свеждаме системата (ii) към

$$\left| \begin{array}{lll} x & \equiv 5 & (\text{mod } 6) \\ x & \equiv 4 & (\text{mod } 7) \end{array} \right. . \tag{3}$$

Съгласно $1 = 7 + (-6)$ с $7 \in 7\mathbb{Z}$, $(-6) \in 6\mathbb{Z}$, цялото число $c = 7.5 + (-6).4 = 11$ е решение на системата (3). Понеже 6 и 7 са взаимно прости естествени числа, всички решения на (ii) образуват съседния клас $11 + 42\mathbb{Z} \in \mathbb{Z}_{42}$.

(iii) Поотделното решаване на всяко от дадените сравнения свежда системата (iii) към

$$\left| \begin{array}{lll} x & \equiv -1 & (\text{mod } 3) \\ x & \equiv 3 & (\text{mod } 5) \\ x & \equiv 1 & (\text{mod } 7) \end{array} \right. . \tag{4}$$

Първо решаваме системата сравнения

$$\left| \begin{array}{lll} x & \equiv -1 & (\text{mod } 3) \\ x & \equiv 3 & (\text{mod } 5) \end{array} \right. \tag{5}$$

като представяме $1 = 6 + (-5)$ с $6 \in 3\mathbb{Z}$, $(-5) \in 5\mathbb{Z}$ и намираме едно решение

$$c = (-1)(-5) + 6.3 = 23.$$

Всички решения на (5) образуват съседния клас $23 + 15\mathbb{Z} = 8 + 15\mathbb{Z}$.

Сега системата (4) е еквивалентна на системата

$$\left| \begin{array}{lll} x & \equiv 8 & (\text{mod } 15) \\ x & \equiv 1 & (\text{mod } 7) \end{array} \right. . \tag{6}$$

Представяме $1 = 15 + (-14)$ с $15 \in 15\mathbb{Z}$, $(-14) \in 7\mathbb{Z}$ и намираме едно решение

$$c = 15.1 + (-14).8 = -97.$$

Поради взаимната простота на 15 и 7, всички решения са

$$-97 + 15.7\mathbb{Z} = -97 + 105\mathbb{Z} = 8 + 105\mathbb{Z}.$$

Твърдение 16. *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 $1_R = (1_{R_1}, \ldots, 1_{R_n})$. В такъв случай, мултипликативната група

$$R^* = R_1^* \times \ldots \times R_n^*$$

на R е директно произведение на мултипликативните групи R_i^* на R_i.

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 $\forall 1 \leq i \leq n$.

Ако R и R_i имат единици, то мултипликативната група R^* на R се състои от онези $x = (x_1, \ldots, x_n) \in R = R_1 \times \ldots \times R_n$, за които съществува $y = (y_1, \ldots, y_n) \in R = R_1 \times \ldots \times R_n$ с

$$xy = yx = 1_R,$$

$$(x_1 y_1, \ldots, x_n y_n) = (y_1 x_1, \ldots, y_n x_n) = (1_{R_1}, \ldots, 1_{R_n}).$$

Последното е равносилно на $x_i y_i = y_i x_i = 1_{R_i}$ за $\forall 1 \leq i \leq n$, така че $x = (x_1, \ldots, x_n) \in R^*$ тогава и само тогава, когато $x_i \in R_i^*$ за $\forall 1 \leq i \leq n$. По този начин доказахме, че

$$R^* = R_1^* \times \ldots \times R_n^*.$$

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.

Следствие 17. *Ако $I_1, \ldots, I_n$ са два по два взаимно прости идеала в комутативен пръстен с единица R, то съществува изоморфизъм на пръстени*

$$R/I_1 \ldots I_n \simeq (R/I_1) \times \ldots \times (R/I_n).$$

Решение: Изображението

$$\varphi : R \longrightarrow (R/I_1) \times \ldots \times (R/I_n),$$

$$\varphi(r) = (r + I_1, \ldots, r + I_n) \quad \text{за} \quad \forall r \in R$$

е хомоморфизъм на пръстени съгласно

$$\varphi(r+s) = (r+s+I_1, \ldots, r+s+I_n) = (r+I_1, \ldots, r+I_n) + (s+I_1, \ldots, s+I_n) = \varphi(r) + \varphi(s)$$

и

$$\varphi(rs) = (rs + I_1, \ldots, rs + I_n) = (r + I_1, \ldots, r + I_n)(s + I_1, \ldots, s + I_n) = \varphi(r)\varphi(s)$$

за $\forall r, s \in R$. Съгласно Китайската теорема за остатъците, φ е епиморфизъм, т.е. $\mathrm{im}(\varphi) = (R/I_1) \times \ldots \times (R/I_n)$.

По определение, ядрото $\ker(\varphi) = I_1 \cap \ldots \cap I_n$. Вземайки предвид Следствие 13, получаваме, че $\ker(\varphi) = I_1 \ldots I_n$. Сега теоремата за хомоморфизмите на пръстени дава

$$R/I_1 \ldots I_n = R/\ker(\varphi) \simeq \mathrm{im}(\varphi) = (R/I_1) \times \ldots \times (R/I_n),$$

Q.E.D.

Следствие 18. *Ако* $n = p_1^{a_1} \dots p_k^{a_k}$ *е разлагането на естественото число* $n \geq 2$ *в произведение на прости множители* p_i *с естествени степенни показатели* a_i*, то пръстенът* $\mathbb{Z}_n$ *на остатъците при деление с* n *се разлага в директно произведение*

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{a_1}} \times \ldots \times \mathbb{Z}_{p_k^{a_k}}. \tag{7}$$

Следствие 18 се получава непосредствено от Следствие 17, вземайки предвид $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$, $\mathbb{Z}_{p_i^{a_i}} = \mathbb{Z}/\langle p_i^{a_i} \rangle$ за $\forall 1 \leq i \leq k$ и $\langle p_1^{a_1} \rangle \dots \langle p_k^{a_k} \rangle = \langle n \rangle$.

От разлагането (7) на $\mathbb{Z}_n$ в директно произведение на пръстени получаваме разлагането

$$\mathbb{Z}_n^* \simeq \mathbb{Z}_{p_1^{a_1}}^* \times \ldots \times \mathbb{Z}_{p_k^{a_k}}^*$$

на мултипликативната група $\mathbb{Z}_n^*$ на $\mathbb{Z}_n$ в директно произведение на мултипликативните групи $\mathbb{Z}_{p_i^{a_i}}^*$ на $\mathbb{Z}_{p_i^{a_i}}$. За нечетно просто p и произволно естествено m може да се докаже, че мултипликативната група $\mathbb{Z}_{p^m}^* \simeq (\mathbb{Z}_{p^{m-1}(p-1)}, +)$ е циклична. За произволно естествено $m \geq 3$ мултипликативната група $\mathbb{Z}_{2^m}^* \simeq (\mathbb{Z}_2, +) \times (\mathbb{Z}_{2^{m-2}}, +)$ е директно произведение на две циклични групи.

Задача 19. *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 20. *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 21. *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 $s_j + i_j \in S+I$, $1 \le j \le 2$ 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

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

Задача 21 твърди, че факторите по протежение на вертикалите са изоморфни.

Задача 22. *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 23. *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

$$\psi((a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})) = \psi((a_1+a_2)+(b_1+b_2)\sqrt{2}) = [(a_1+a_2)-3(b_1+b_2)](\text{mod } 7) =$$
$$= [(a_1 - 3b_1)(\text{mod } 7)] + [(a_2 - 3b_2)(\text{mod } 7)] = \psi(a_1 + b_1\sqrt{2}) + \psi(a_2 + b_2\sqrt{2}) \quad \text{и}$$
$$\psi((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) = \psi((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}) =$$
$$= [(a_1a_2 + 2b_1b_2) - 3(a_1b_2 + a_2b_1)](\text{mod } 7) = [(a_1a_2 + 9b_1b_2) - 3(a_1b_2 + a_2b_1)](\text{mod } 7) =$$
$$= [(a_1 - 3b_1)(a_2 - 3b_2)](\text{mod } 7) = [(a_1 - 3b_1)(\text{mod } 7)][(a_2 - 3b_2)(\text{mod } 7)] =$$
$$= \psi(a_1 + b_1\sqrt{2})\psi(a_2 + b_2\sqrt{2}).$$

Съгласно Теоремата за хомоморфизмите на пръстени,

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

Задача 24. *Да се докаже, че:*

(i) множеството

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

е пръстен относно обичайните операции събиране и умножение на матрици;

(ii) за произволно просто число p подмножествата

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

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

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

$$\varphi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = c(\mathrm{mod}\ \ p)$$

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

$$x = \begin{pmatrix} a_1 & b_1 \\ 0 & pc_1 \end{pmatrix} + J \quad \text{и} \quad y = \begin{pmatrix} pa_2 & b_2 \\ 0 & c_2 \end{pmatrix} + J \in R/J$$

имат нулево произведение

$$xy = \begin{pmatrix} pa_1a_2 & a_1b_2 + b_1c_2 \\ 0 & pc_1c_2 \end{pmatrix} + J = J,$$

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

Задача 25. *Нека*

$$\mathbb{Z}_{2\times 2} = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \;\middle|\; a_{ij} \in \mathbb{Z} \right\}$$

е пръстенът на 2×2*-матриците с целочислени елементи, а*

$$(\mathbb{Z}_2)_{2\times 2} = \left\{ \begin{pmatrix} a_{11} + 2\mathbb{Z} & a_{12} + 2\mathbb{Z} \\ a_{21} + 2\mathbb{Z} & a_{22} + 2\mathbb{Z} \end{pmatrix} \;\middle|\; a_{ij} + 2\mathbb{Z} \in \mathbb{Z}_2 \right\}$$

е пръстенът на 2×2*-матриците с елементи от полето* $\mathbb{Z}_2$ *на остатъците при деление с* 2*. Да се докаже, че подмножеството* $I = \{\, 2X \mid X \in \mathbb{Z}_{2\times 2} \,\}$ *е идеал на* $\mathbb{Z}_{2\times 2}$ *с фактор-пръстен* $\mathbb{Z}_{2\times 2}/I \simeq (\mathbb{Z}_2)_{2\times 2}$*, изоморфен на пръстена* $(\mathbb{Z}_2)_{2\times 2}$*.*

Задача 26. *Да се докаже, че всяко крайно поле* F *с характеристика* p *има* p^n *елемента за някое естествено* n*.*

Задача 27. *Нека* F *е поле с проста характеристика* p*,* a *и* b *са елементи на* F*,* a n *е естествено число. Да се докаже, че:*

(i) $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$*.*

(ii) изображението $\Phi_{p^n} : F \to F$*,* $\Phi_{p^n}(a) = a^{p^n}$ *е хомоморфизъм на пръстени.*

(iii) ако F *е крайно поле с* p^m *елемента, то* $\Phi_{p^n} : F \to F$*,* $\Phi_{p^n}(a) = a^{p^n}$ *е изоморфизъм на пръстени.*

Упътване: (i) Докажете, че биномните коефициенти $\binom{p}{i}$ с $1 \le i \le p-1$ се делят на p, за да изведете $(a \pm b)^p = a^p \pm b^p$. Продължете с индукция по $n \in \mathbb{N}$.

(ii) За съгласуваността на Φ_{p^n} със събирането използвайте (i).

(iii) Ако $\Phi_{p^n}(a) = \Phi_{p^n}(b)$, то $0 = a^{p^n} - b^{p^n} = (a-b)^{p^n}$, откъдето $a = b$. Това доказва взаимната еднозначност на действието на Φ_{p^n} върху полето F с p^m елемента.

Задача 28. *Да се докаже, че ако* F *е поле с проста характеристика* $\mathrm{char}F = p$*, то за произволни елементи* $x, y \in F$ *е в сила*

$$(x+y)^{p-1} = \sum_{i=0}^{p-1} (-1)^i x^i y^{p-1-i}.$$

Упътване: От $(x-1)^{p-1} = x^{p-1} + x^{p-2} + \ldots + x + 1$ изведете $\binom{p-1}{i} = (-1)^i$ за всички $0 \leq i \leq p-1$.

Задача 29. *Да се докаже, че:*

(i) множеството $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ *е подполе на полето* $\mathbb{R}$ *на реалните числа;*

(ii) полето $\mathbb{Q}(\sqrt{2})$ *е двумерно линейно пространство над простото си подполе.*

Задача 30. *Нека* m *и* n *са естествени числа, а* $\mathbb{Z}_n^*$ *е мултипликативната група на пръстена* $\mathbb{Z}_n$ *от остатъци при деление с* n*. Да се докаже, че:*

(i) $\Phi_m : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$, $\Phi_m(x + n\mathbb{Z}) = x^m + n\mathbb{Z}$ *е хомоморфизъм на мултипликативната група* $\mathbb{Z}_n^*$ *на* $\mathbb{Z}_n$ *в себе си;*

(ii) ако редът $\varphi(n)$ *на* $\mathbb{Z}_n^*$ *е взаимно прост с* m*, то* $\Phi_m : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ *е изоморфизъм на групи.*

Упътване: (ii) Изображението Φ_m на крайни множества е взаимно-еднозначно точно когато образът $\mathrm{im}\Phi \simeq \mathbb{Z}_n^* / \ker \Phi$ е изоморфен на праобраза $\mathbb{Z}_n^*$ или $\ker \Phi_m = \{1 + n\mathbb{Z}\}$. Условието $(a + n\mathbb{Z})^m \neq 1 + n\mathbb{Z}$ за $\forall a + n\mathbb{Z} \in \mathbb{Z}_n^* \setminus \{1 + n\mathbb{Z}\}$ следва от това, че редът δ на $a + n\mathbb{Z} \in \mathbb{Z}_n^*$ дели реда $\varphi(n)$ на $\mathbb{Z}_n^*$, а $\varphi(n)$ и m са взаимно прости по предположение.

Задача 31. *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 32. *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

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

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

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

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

има цели решения

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

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

(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 $(2) \neq I$.

Определение 33. *Идеалът $M \neq R$ в комутативен пръстен с единица R се нарича максимален, ако единственият идеал $M \subsetneq I \lhd R$ е $I = R$.*

Задача 34. *Да се докаже, че всеки собствен идеал $I \neq R$ в комутативен пръстен с единица R се съдържа в максимален идеал M.*

Упътване: Нека Σ_I е множеството на собствените идеали на R, съдържащи I, а $\{J_\alpha\}_{\alpha \in A}$ е линейно наредено подмножество на Σ_I. По определение, това означава, че за произволни $\alpha \neq \beta$ от A е изпълнено $J_\alpha \subseteq J_\beta$ или $J_\beta \subseteq J_\alpha$. Тогава $J = \cup_{\alpha \in A} J_\alpha \neq R$ е точна горна граница на $\{J_\alpha\}_{\alpha \in A}$, т.е. $J \in \Sigma_I$ и $J \supseteq J_\alpha$ за $\forall \alpha \in A$. Съгласно Лемата на Цорн, оттук следва съществуването на максимален елемент $M \in \Sigma_I$, който е максимален собствен идеал в R, съдържащ I.

Определение 35. *Идеалът P в комутативния пръстен с единица R се нарича прост, ако от $ab \in P$ за $a, b \in R$ следва $a \in P$ или $b \in P$.*

Задача 36. *В комутативен пръстен с единица R да се докаже, че:*

(i) идеалът $M \neq R$ е максимален тогава и само тогава, когато фактор-пръстенът R/M е поле;

(ii) идеалът P е прост тогава и само тогава, когато фактор-пръстенът R/P е област.

В частност, всеки максимален идеал е прост.

В пръстена $\mathbb{Z}$ на целите числа, максималните идеали са (p) за прости $p \in \mathbb{N}$, а единственият прост идеал, който не е максимален е нулевият $\{0\}$.

Упътване: (i) Ако идеалът M е максимален, то за $\forall r + M \neq M$ идеалът $rR + M = R$ съвпада с целия пръстен. Следователно съществуват $s \in R$ и $m \in M$, така че $rs + m = 1$ и $(r + M)(s + M) = rs + M = 1 - m + M = 1 + M$.

Обратно, ако R/M е поле, да допуснем, че съществува идеал $M \subsetneq J \subsetneq R$. Тогава за $\forall j \in J \setminus M$ ненулевият елемент $j + M \in R/M$ е обратим в R/M. С други думи, съществува $s + M \in R/M$ с $(j + M)(s + M) = js + M = 1 + M$. Оттук $1 = js + m$ за някое $m \in M$ и $1 \in J$, противно на допускането $J \neq R$.

Задача 37. *Нека R е комутативен пръстен с единица, а P е прост идеал в R. Да се докаже, че не съществуват идеали $P \subsetneq I \trianglelefteq R$ и $P \subsetneq J \trianglelefteq R$ с $P = I \cap J$.*

Упътване: При допускане на противното съществуват елементи $\alpha \in I \setminus P$ и $\beta \in J \setminus P$ с произведение $\gamma = \alpha\beta \in IJ \subseteq I \cap J = P$. Това противоречи на простотата на P.

Задача 38. *Нека $\varphi : R \to S$ е хомоморфизъм на комутативни пръстени с единица, а P е прост идеал в S. Да се докаже, че праобразът $\varphi^{-1}(P)$ е прост идеал в R.*

Забележка 39. *Съществуват максимални идеали, чиито праобрази под действие на хомоморфизми на пръстени са прости, но не максимални. Например, нулевият идеал е максимален в полето $\mathbb{Q}$ на рационалните числа. Под действие на тъждественото влагане $\mathbb{Z} \hookrightarrow \mathbb{Q}$ на целите числа той се издърпва до нулевия идеал на $\mathbb{Z}$, който е прост, но не е максимален.*

Задача 40. *Нека p е просто число, а*

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

е пръстенът от Задача 1 (б). Да се докаже, че:

(i) допълнението $R \setminus R^* = pR$ на мултипликативната група R^* на R съвпада с главния идеал $pR = \{p\alpha | \alpha \in R\}$, породен от p;

(ii) pR е единственият максимален идеал на R.

Упътване: (ii) Идеалът pR е максимален, защото произволен идеал $I \supsetneq pR$ съдържа елемент на R^* и $I = R$. Ако M е максимален идеал на R, то $M \neq R$, така че $M \cap R^* = \emptyset$ и $M \subseteq R \setminus R^* = pR$. От максималността на M следва, че $M = pR$.

Задача 41. *Нека R е множеството от всички реални функции, определени в интервала $[-2, 2]$. Да се докаже, че:*

(i) R е комутативен пръстен с единица относно поточково определените операции събиране и умножение на функции

$$(f + g)(x) = f(x) + g(x) \quad \text{и} \quad (fg)(x) = f(x)g(x) \quad \text{за } \forall x \in [-2, 2];$$

(ii) подмножеството $M = \{f \in R \mid f(1) = 0\} \subset R$ е максимален идеал в R с фактор-пръстен $R/M \simeq \mathbb{R}$;

(iii) подмножеството $N = \{f \in R \mid f(1) = f(0) = 0\} \subset M$ *е максимален идеал на подпръстена* M *на* R *с фактор-пръстен* $M/N \simeq \mathbb{R}$.

(iv) идеалът N *на* R *не е прост.*

Упътване: (ii) Приложете Теоремата за хомоморфизмите на пръстени към изображението

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

$$\varphi(f) = f(1) \quad \text{за} \quad \forall f \in R.$$

(iii) Приложете Теоремата за хомоморфизмите на пръстени към изображението

$$\psi : M \longrightarrow \mathbb{R},$$

$$\psi(f) = f(0) \quad \text{за} \quad \forall f \in M.$$

(iv) Използвайте, че $x(x-1) \in N$, но $x \notin N$ и $x - 1 \notin N$.