Пръстени.

Разглеждаме непразното множество $R \neq \varnothing$, което е затворено относно две бинарни операции – събиране

$$+ : R \times R \longrightarrow R$$

и умножение

$$\cdot : R \times R \longrightarrow R.$$

Казваме, че R е пръстен, ако са изпълнени аксиомите 1.-4. за абелева група спрямо събирането и в допълнение

5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ за $\forall a, b, c \in R$,

6) $(a + b) \cdot c = a \cdot c + b \cdot c$ и $c \cdot (a + b) = c \cdot a + c \cdot b$ за $\forall a, b, c \in R$.

Казваме, че елементите $a, \in R$ са делители на нулата, ако $a \neq 0$ и $b \neq 0$, но $ab = 0$. Пръстен, който не съдържа делители на нулата се нарича област.

Казваме, че R е пръстен с единица, ако съществува единичен елемент $1 \in R$, такъв че $1 \cdot a = a \cdot 1 = a$ за $\forall a \in R$.

Ако R е пръстен с единица 1, казваме, че елементът $a \in R$ е обратим, ако съществува елемент $a^{-1} \in R$, такъв че $aa^{-1} = a^{-1}a = 1$. Множеството $R^* = \{a \in R \mid \exists a^{-1} \in R : aa^{-1} = a^{-1}a = 1\}$ от обратимите елементи на R образува група спрямо операцията умножение, наречена мултипликативна група на пръстена R. Пръстен, в който всеки ненулев елемент е обратим, т.е. $R^* = R\backslash\{0\}$, се нарича тяло.

Казваме, че R е комутативен пръстен. ако $ab = ba$ за $\forall a, b \in R$. Комутативните тела наричаме полета.

Типични примери са пръстенът на целите числа $\mathbb{Z}$. Той е комутативен пръстен с единица, в който няма делители на нулата, т.е. е и област. $\mathbb{Z}$ обаче не е поле, т.к. единствено елементите 1 и -1 са обратими. Множествата $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ са пръстени относно обичайното събиране и умножение на числа. Освен това те са полета. За всяко $n \in \mathbb{N}$, множеството $\mathbb{Z}_n$ от остатъците при деление с n е пръстен. Ако F е произволно поле, множеството $F_{n\times n}$ е некомутативен пръстен с единица. $F_{n\times n}$ обаче не е област и не е тяло.

Забележка: всяка адитивно записана абелева група G може да бъде вложена в пръстен, чрез дефиниране на нулево умножение, т.е. $ab = 0$ за $\forall a, b \in G$.

Задача 1. *Покажете, че множеството*

$$M = \{a \mid a \in \mathbb{Z}\},$$

в което са въведени операция събиране $\oplus$ *по правилото*

$$a \oplus b = a + b - 1$$

и операция умножение $\odot$ *по правилото*

$$a \odot b = a + b - (ab),$$

е пръстен.

Решение. 1. Проверяваме асоциативността на $\oplus$. За произволни елементи $a, b, c \in M$ имаме, че

$$(a \oplus b) \oplus c = (a + b - 1) \oplus c = a + b - 1 + c - 1 = a + b + c - 2$$

и

$$a \oplus (b \oplus c) = a \oplus (b + c - 1) = a + b + c - 1 - 1 = a + b + c - 2,$$

което показва, че $\oplus$ притежава свойството асоциативност.

2. Търсим неутрален елемент $0_M \in M$. Той трябва да изпълнява условието

$$a \oplus 0_M = 0_M \oplus a = a$$

за $\forall a \in M$. Тогава имаме, че

$$a \oplus 0_M = a,$$

$$a + 0_M - 1 = a,$$

$$0_M = 1.$$

3. За всеки елемент $a \in M$ търсим противоположен елемент $-a \in M$. Той трябва да изпълнява условието

$$a \oplus (-a) = -a \oplus a = 0_M.$$

Тогава имаме, че

$$a \oplus (-a) = 0_M,$$
$$a + (-a) - 1 = 1,$$
$$-a = 2 - a.$$

4. Операцията $\oplus$ има свойството комутативност, защото за всеки два елемента $a, b \in M$ имаме, че

$$a \oplus b = a + b - 1 = b + a - 1 = b \oplus a.$$

5. Операцията $\odot$ е асоциативна съгласно

$$(a \odot b) \odot c = (a+b-ab) \odot c = a+b-ab+c-(a+b-ab)c = a+b+c-ab-ac-bc+abc$$

и

$$a \odot (b \odot c) = a \odot (b+c-bc) = a+b+c-bc-a(b+c-bc) = a+b+c-ab-ac-bc+abc$$

за произволни елементи $a, b, c \in M$.

6. Ще проверим дистрибутивния закон

$$(a \oplus b) \odot c = a \odot c \oplus b \odot c,$$

а проверката на другия е аналогична. И така, за произволни елементи $a, b, c \in M$ имаме, че

$$(a \oplus b) \odot c = (a+b-1) \odot c = (a+b-1)+c-(a+b-1)c = a+b+2c-ab-ac-1$$

и

$$a \odot c \oplus b \odot c = (a+c-ac) \oplus (b+c-bc) = a+c-ac+b+c-bc-1 = a+b+2c-ab-ac-1.$$

С това шестте аксиоми са изпълнени и следователно множеството M е пръстен относно дефинираните операции. $\square$

Задача 2. *Кои от множествата*

а) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$,

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

са полета?

Решение. По познатия вече начин докажете, че и двете множества са комутативни пръстени спрямо стандратните събиране и умножение на числа. Сега...

а) Пръстенът $\mathbb{Z}[\sqrt{2}]$ е пръстен с единица. Наистина, ако $1 = x + y\sqrt{2}$ е такъв елемент, че

$$(a + b\sqrt{2}).1 = a + b\sqrt{2}$$

за всеки елемент $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, то имаме, че

$$(a + b\sqrt{2})(x + y\sqrt{2}) = a + b\sqrt{2},$$

$$ax + 2by + (ay + bx)\sqrt{2} = a + b\sqrt{2}.$$

Последното е изпълнено, точно когато x и y са целочислени решения на системата

$$\left| \begin{array}{lll} ax & +2by & = a, \\ bx & +ay & = b \end{array} \right.$$

За $\forall a, b \in \mathbb{Z}$. Това е възможно само при $x = 1, y = 0$. Очевидно елементът $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Освен това $\mathbb{Z}[\sqrt{2}]$ е област, защото ако $a_1 + b_1\sqrt{2} \neq 0$ и $a_2 + b_2\sqrt{2} \neq 0$, то

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2} \neq 0$$

поради причината, че $(a_1, a_2) \neq (0, 0)$ и $(b_1, b_2) \neq (0, 0)$ едновременно. Ще покажем, че $\mathbb{Z}[\sqrt{2}]$ не е тяло, откъдето ще следва и че не е поле. Нека $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ е произволен ненулев елемент. Да видим дали във всички случаи той е обратим. Нека да допуснем, че съществува обратен елемент $u + v\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, такъв че

$$(a + b\sqrt{2})(u + v\sqrt{2}) = 1.$$

Това означава, че

$$au + 2bv + (av + bu)\sqrt{2} = 1$$

или еквивалентно, че системата

$$\left| \begin{array}{lll} au & +2bv & = 1, \\ bu & +av & = 0 \end{array} \right.$$

има целочислено решение (u, v) за произволни неедновременно нулеви цели числа $a, b \in \mathbb{Z}$. Но това би означавало, че

$$u = -\frac{a}{2b^2 - a^2}, v = \frac{b}{2b^2 - a^2} \in \mathbb{Z},$$

а това няма как да е изпълнено за всяка целочислена двойка $(a, b) \neq (0, 0)$. Противоречието доказва, че не може да бъде намерет обратен елемент за произволен ненулев елемент от $\mathbb{Z}[\sqrt{2}]$ и пръстенът не е тяло.

б) Докажете, че $\mathbb{Q}(\sqrt{2})$ също е комутативна област с единица. При търсенето на обратен елемент $u + v\sqrt{2}$ за произволен ненулев елемент от $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ условието

$$u = -\frac{a}{2b^2 - a^2}, v = \frac{b}{2b^2 - a^2} \in \mathbb{Q}$$

вече не е противоречиво и следователно всеки ненулев елемент е обратим. С това $\mathbb{Q}(\sqrt{2})$ е поле. $\square$

Задача 3. *Опишете пръстена* $\mathbb{Z}_5$ *и решете в него системата*

$$\left| \begin{array}{llll} x & +\overline{2}y & +\overline{3}z & = \overline{4}, \\ \overline{2}x & -y & & = \overline{1}, \\ \overline{3}x & -y & +z & = \overline{2}. \end{array} \right.$$

Решение. Използваме таблици на Кейли за описанието на всяка една от операциите.

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{0}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$

$\overline{3}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Решаваме системата по метода на Гаус, използвайки таблиците. Умножаваме второто уравнение по $\overline{3}$, а третото по $\overline{2}$, за да получим

$$\left|\begin{array}{llll} x & +\overline{2}y & +\overline{3}z & =\overline{4}, \\ x & -\overline{3}y & & =\overline{3}, \\ x & -\overline{2}y & +\overline{2}z & =\overline{4}. \end{array}\right.$$

Сега от воторото уравнение изваждаме първото и това ни дава

$$-\overline{3}z = -\overline{1},$$

което е еквивалентно на

$$\overline{2}z = \overline{4}.$$

Умножавайки това уравнение с $\overline{3}$ получаваме

$$z = \overline{2}.$$

Замествайки тази информация в останалите две уравнения получаваме системата

$$\left|\begin{array}{lll} x & +\overline{2}y & =\overline{3}, \\ x & -\overline{2}y & =\overline{0}. \end{array}\right.$$

Тяхното почленно събиране ни дава уравнението

$$\overline{2}x = \overline{3},$$

чието решение е

$$x = \overline{4}.$$

Накрая, например от второто уравнение получаваме, че

$$\overline{2}y = \overline{4},$$

което ни дава, че

$$y = \overline{2}.$$

Следователно решението на системата е $(x, y, z) = (\overline{4}, \overline{2}, \overline{2})$. $\square$

Задача 4. *Да се докаже, че за всеки елемент* $\overline{a} \in \mathbb{Z}_{15}^*$ *на мултипликативната група на пръстена от остатъците при деление с 15 и за всяко нечетно естествено число* m*, уравнението* $x^m = \overline{a}$ *има единствено решение в* $\mathbb{Z}_{15}^*$*. Да се реши уравнението* $x^3 = \overline{2}$ *в* $\mathbb{Z}_{15}^*$*.*

Решение. Имаме, че $|\mathbb{Z}_{15}^*| = \varphi(15) = \varphi(3)\varphi(5) = 8$. Един елемент $\overline{c} \in \mathbb{Z}_{15}$ попада в мултипликативната група, точно когато е обратим, а това е еквивалентно на $(a, 15) = 1$. В такъв случай експлицитно намираме, че

$$\mathbb{Z}_{15}^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}.$$

Да разгледаме уравнението $x^m = \overline{a}$. То е еквивалентно на сравнението

$$x^m \cong a (\mathrm{mod}\, 15).$$

Според теоремата на Ойлер ферма $x^{\varphi(15)} = x^8 \equiv 1 (\mathrm{mod}\, 15)$. Следователно можем да намалим степента на уравнението до остатъка r при деление на m с 8. Т.к по условие m е нечетно, възможните остатъци са $1, 3, 5, 7$. Това свежда задачата до разглеждането на четири вида уравнения. Ако $r = 1$, то уравнението е

$$x = \overline{a}$$

и няма нужда от решаване. Ако $r = 3$, имаме уравнението

$$x^3 = \overline{a}$$

и след повдигане на двете страни на трета степен получаваме решението

$$x^9 = x = \overline{a}^3.$$

При $r = 5$ трябва да решим

$$x^5 = \overline{a}.$$

След повдигане на двете страни на втора степен получаваме равенството

$$x^{10} = x^2 = \overline{a}^2.$$

Повдигаме и това равенство на квадрат, за да достигнем до

$$x^4 = \overline{a}^4.$$

Сега, умножавайки последното равенство с изходното, намираме решението

$$x = \overline{a}^5.$$

В последния случай, при $r = 7$ имаме

$$x^7 = \overline{a}.$$

Повдигаме на квадрат и получаваме

$$x^{14} = x^6 = \overline{a}^2.$$

Умножаваме това уравнение с изходното и получаваме

$$x^{13} = x^5 = \overline{a}^3.$$

Умножаваме и това уравенение с изходното и т.н. повтаряме неколкократно процедурата до достигане на

$$x^9 = \overline{a}^7,$$

което всъщност ни дава решението

$$x = \overline{a}^7.$$

Сега, според изследванията, които направихме, имаме че решението на даденото уравнение

$$x^3 = \overline{2}$$

е

$$x = \overline{2}^3 = \overline{8}.$$

Друг (и вероятно по-интересен) начин за решаване на задачата: Искането уравнението $x^m = a$ в $\mathbb{Z}_{15}$ да има единствено решение може да се разглежда като търсене на единствен елемент $b \in \mathbb{Z}_{15}$, за който $b^m = a$. Означаваме $b = \sqrt[m]{a}$ и го наричаме m-ти корен на a. Тогава въпросното искане означава, че трябва да се докаже, че в мултипликативната група $\mathbb{Z}_{15}^*$ има еднозначно извличане на m-ти корен за нечетно число m. Да разгледаме изображението

$$\psi : \mathbb{Z}_{15}^* \longrightarrow (\mathbb{Z}_{15}^*)^m,$$

дефинирано с $\psi(a) = a^m$, където $(\mathbb{Z}_{15}^*)^m = \{a^m \mid a \in \mathbb{Z}_{15}^*\}$. Още от самия начин, по който дефинирахме изображението и множеството от стойностите му, е ясно, че ψ е сюрекция. Директно проверяваме, че $(\mathbb{Z}_{15}^*)^m \leq \mathbb{Z}_{15}^*$ и че изображението ψ всъщност е хомоморфизъм на групи. Нека $a, b \in \mathbb{Z}_{15}^*$ и $a \neq b$. Да допуснем, че $\psi(a) = \psi(b)$, т.е.

$$a^m = b^m.$$

Това уравнение е еквивалентно на

$$(ab^{-1})^m = 1,$$

което ще рече, че редът на елемента ab^{-1} дели m. Нека $|ab^{-1}| = r$. Тогава $r \mid m$ но също и r дели реда на групата $|\mathbb{Z}_{15}^*| = 8$. Понеже m е нечетно, то $(m, 8) = 1$ и оттук трябва $r = 1$. Следователно получихме, че

$$ab^{-1} = 1$$

или еквивалентното

$$a = b,$$

което противоречеи на избора на елементите a и b, които бяха различни. Противоречието доказва, че ψ е инекция, а оттук и изоморфизъм на групи. Следователно в $\mathbb{Z}_{15}^*$ може еднозначно да се извлича m-ти корен, ако m е нечетно. $\square$

Непразното подмножество $S \subseteq R$ на пръстена R се нарича подпръстен и пишем $S \leq R$, ако $a - b \in S$ и $ab \in S$ за $\forall a, b \in S$.

Непразното подмножество $I_l \subseteq R$ на пръстена R се нарича ляв идеал на R, ако $a - b \in I_l$ и $ra \in I_l$ за $\forall a, b \in I_l, \forall r \in R$. Непразното подмножество $I_r \subseteq R$ на пръстена R се нарича десен идеал на R, ако $a - b \in I_r$ и $ar \in I_r$ за $\forall a, b \in I_r, \forall r \in R$. Ако I е едновременно ляв и десен идеал на R, то казваме, че I е двустранен идеал или само идеал на R и пишем $I \trianglelefteq R$. От дефиницията е ясно, че всеки идеал на R е също и негов подпръстен.

За елемента $a \in R$, множеството

$$(a) = \{ra \mid r \in R\} \trianglelefteq R$$

е идеал на R, наречен главен идеал на R, породен от a.

Задача 5. *Докажете, че множеството*

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$$

е подпрѣстен на прѣстена $\mathbb{Z}_{2\times 2}$ *на* 2×2 *матриците с целочислени елементи, а множеството*

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in 5\mathbb{Z} \right\}$$

е идеал в S

Решение. S е подпръстен на $\mathbb{Z}_{2\times 2}$, защото

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in S$$

и

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix} \in S$$

за всеки два елемента на S.

Множеството J е ляв идеал в S, защото

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{pmatrix} \in J$$

за всеки два елемента от J, т.к. от $a_1, a_2 \in 5\mathbb{Z} \Rightarrow a_1 + a_2 \in 5\mathbb{Z}$, аналогично $b_1 + b_2, c_1 + c_2 \in 5\mathbb{Z}$ и още защото

$$\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = \begin{pmatrix} xa & xb + yc \\ 0 & zc \end{pmatrix} \in J$$

за всяка матрица $\begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in S$ и всяка матрица $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in J$ т.к. от $a \in 5\mathbb{Z} \Rightarrow xa \in 5\mathbb{Z}$ за $\forall a \in \mathbb{Z}$, аналогично $xb + yc, zc \in 5\mathbb{Z}$.

По същия начин проверете, че J е десен идеал в S, откъдето ще следва, че $J \lhd S$. $\square$

Задача 6. *Нека е даден прѣстенът* $R = \{a, b, c, d, e, f\}$, *зададен с таблициата за събиране*

$+$	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

и таблицата за умножение

$\cdot$	a	b	c	d	e	f
a	a	a	a	a	a	a
b	a	b	c	d	e	f
c	a	c	e	a	c	e
d	a	d	a	d	a	d
e	a	e	c	a	e	c
f	a	f	e	d	c	b

Кои са подпръстените и идеалите на R?

Решение. За да имаме подпръстен $S \leq R$, трябва $a + b \in S$ и $ab \in S$ за $\forall a, b \in S$.

От таблиците ясно се вижда, че нулевият елемент е a. Тогава задължително $a \in S$ за произволен подпръстен на R.

Да допуснем, че $b \in S$. Тогава получаваме веригата от следствия $b + b = c \in S \Rightarrow c + c = e \in S \Rightarrow b + c = d \in S \Rightarrow d + c = f \in S$ и получваме, че $S = R$ е целият пръстен.

Нека сега $b \notin S$. Нека $c \in S$. Тогава $c + c = e \in S$ и оттук $e + e = c, e + c = a$. Освен това $cc = e, ee = e, ec = ce = e$. По този начин получихме нетривиален подпръстен $\{a, c, e\}$.

Нека $b \notin S$, $c \notin S$, но $d \in S$. Тогава $d + d = a$ и $dd = d$, откъдето следва, че $\{a, d\}$ е друг нетривиален подпръстен на R.

Нека $b, c, d \notin S$, но $e \in S$. Тогава бихме получили, че $e + e = c \in S$, което е противоречие.

Нека $b, c, d, e \notin S$, но $f \in S$. Тогава бихме получили противоречието $f + f = e \in S$.

С това всички нетривиални подпръстени на R са $S_1 = \{a, c, e\}$ и $S_2 = \{a, d\}$.

Всеки идеал $I \trianglelefteq R$ е подпръстен на R и затова трябва просто да проверим кои от вече намерените подпрсъстени издържат на умножение с произволни елементи от пръстена R. За S_1 виждаме от таблицата за умножение, че $cx \in S_1$ и $ex \in S_1$ за $\forall x \in R$, което означава, че $(c) = S_1 \triangleleft R$. За S_2 от таблицата за умножение виждаме, че $dy \in S_2$ за $\forall y \in R$ и следователно $(d) = S_2 \triangleleft R$. Да проверим дали $(c, d) \triangleleft R$. Ако това беше вярно, то щяхме да имеме, че $c + d = f \in (c, d)$, а оттук и $cf = b \in (c, d)$. Т.к. b е единичният елемент на R, това означава, че $(c, d) = R$ е тривиален идеал. И така, всички нетривиални идеали са $I_1 = (c)$ и $I_2 = (d)$. $\square$

Задача 7. *Да разгледаме пръстена на целите гаусови числа*

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

адитивната му подгрупа

$$I = \{a + bi \in \mathbb{Z}[i] \mid a \equiv 2b (\operatorname{mod} 5)\}$$

и хомоморфизма на групи $\varphi : (I, +) \longrightarrow (\mathbb{C}, +)$*, дефиниран чрез*

$$\varphi(a + bi) = \frac{a + bi}{2 + i}.$$

1) Докажете, че образът на φ *е* $\operatorname{Im} \varphi = \mathbb{Z}[i]$ *и* I *е главен идеал в* $\mathbb{Z}[i]$.
2) Намерете всички $a + bi \in I \backslash \{0\}$ *с минимален квадрат на модула* $|a + bi|^2 = a^2 + b^2$.

Решение. 1) За всеки елемент $\varphi(a + bi) \in \operatorname{Im} \varphi$, където $a + bi \in I$ имаме, че

$$\varphi(a+bi) = \frac{a + bi}{2 + i} = \frac{(a + bi)(2 - i)}{(2 + i)(2 - i)} = \frac{2a + b + (2b - a)i}{5} = \frac{2a + b}{5} + \frac{2b - a}{5} i.$$

Понеже $a \equiv 2b (\operatorname{mod} 5)$, то

$$\frac{2a + b}{5} \equiv \frac{2(2b) + b}{5} \equiv \frac{5b}{5} \equiv b (\operatorname{mod} 5),$$

т.е. $\dfrac{2a + b}{5} \in \mathbb{Z}$. Още, $a \equiv 2b (\operatorname{mod} 5)$ означава, че $5 \mid (2b - a)$ или с други думи $\dfrac{2b - a}{5} \in \mathbb{Z}$. По този начи $\varphi(a + bi) \in \mathbb{Z}[i]$ и е доказано включването

$\operatorname{Im}\varphi \subseteq \mathbb{Z}[i]$. За обратното включване да видим, че всяко цяло гаусово число $a+bi$ има за прообраз елемента $(a+bi)(2+i) \in I$. Наистина $(a+bi)(2+i) = 2a-b+(a+2b)i \in I$, защото изпълнява условието $2a-b \equiv 2a+4b \equiv 2(a+2b) (\operatorname{mod} 5)$. Освен това $\varphi((a+bi)(2+i)) = \dfrac{(a+bi)(2+i)}{2+i} = a+bi$. По този начин $\mathbb{Z}[i] \subseteq \operatorname{Im}\varphi$ и окончателно $\operatorname{Im}\varphi = \mathbb{Z}[i]$.

За да покажем, че I е главен идеал на пръстена $\mathbb{Z}[i]$, трябва да открием елемента, който го поражда. Както вече видяхме, за всяко цяло гаусово число $a+bi$, елементът $(a+bi)(2+i) \in I$, което доказва включването $(2+i) \subseteq I$. За обратното включване $I \subseteq (2+i)$ трябва да покажем, че всеки елемент $a+bi \in I$ се изразява като $a+bi = (x+yi)(2+i)$ за някакъв елемент $x+yi \in \mathbb{Z}[i]$. Тогава въпросният елемент е $x+yi = \dfrac{a+bi}{2+i}$, защото както вече видяхме $\dfrac{a+bi}{2+i} \in \mathbb{Z}[i]$ за всеки елемент $a+bi \in I$. И така, $I = (2+i)$.

2) За всеки елемент $a+bi \in I$ имаме, че

$$|a+bi|^2 = a^2+b^2 \equiv (2b)^2+b^2 \equiv 5b^2 (\operatorname{mod} 5).$$

Тъй като търсим ненулеви елементи, то минималната стойност на израза $|a+b|^2 = 5b$ се достига при $b = \pm 1$. Това задава четирите елемента

$$2+i, 2-i, -2+i, -2-i,$$

които имат минимален квадрат на модула 5. $\square$

Ясно е, че ако R е пръстен, а I е идеал в него, то $(I,+) \trianglelefteq (R,+)$ е нормална подгрупа на адитивната група на R. Тогава множеството

$$R/I = \{r+I \mid r \in R\},$$

състоящо се от съседните класове на R по I, е пръстен относно операциите $+$ и $\cdot$ в R, наречен факторпръстен на R по идеала I.

Ако R_1 и R_2 са два пръстена, а

$$\varphi : R_1 \longrightarrow R_2$$

е изображение, то φ се нарича хомоморфизъм на прсътени, ако са изпълнени условията

$$\varphi(a+b) = \varphi(a)+\varphi(b),$$

$$\varphi(ab) = \varphi(a)\varphi(b)$$

за всеки два елемента $a, b \in R_1$. Множеството

$$\operatorname{Ker}\varphi = \{r \in R_1 \mid \varphi(r) = 0_{R_2}\}$$

се нарича ядро на изображението φ и освен това е идеал в R_1. Множеството

$$\operatorname{Im}\varphi = \{r' \in R_2 \mid \exists r \in R_1 : \varphi(r) = r'\}$$

се нарича образ на φ и е подпръстен на R_2.

Хомоморфизмът на пръстени φ е изоморфизъм на пръстени, ако е взаимно-еднозначен. В такъв случай $R_1 \cong R_2$. В сила е

Теорема за хомоморфизмите на пръстени. *Нека R_1 и R_2 са пръстени, а*

$$\varphi : R_1 \longrightarrow R_2$$

е хомоморфизъм на пръстени. Тогава $R_1/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

Задача 8. *В пръстена $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$ е даден главният идеал $I = (1+2\sqrt{3})$, породен от $1+2\sqrt{3}$. Да се докаже, че $I = \{a+b\sqrt{3} \in \mathbb{Z}[\sqrt{3}] \mid a \equiv 6b (\operatorname{mod} 11)\}$ и факторпръстенът $\mathbb{Z}[\sqrt{3}]/I \cong \mathbb{Z}_{11}$.*

Решение. Нека означим $I_1 = \{a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}] \mid a \equiv 6b (\operatorname{mod} 11)\}$. Всеки елемент от I има вида $(x+y\sqrt{3})(1+2\sqrt{3})$ за произволен елемент $x+y\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Имаме, че

$$(x + y\sqrt{3})(1 + 2\sqrt{3}) = x + 6y + (2x + y)\sqrt{3}.$$

Проверяваме сравнението

$$x + 6y \overset{?}{\equiv} 6(2x + y) (\operatorname{mod} 11),$$

което е еквивалентно на

$$x + 6y \equiv 12x + 6y (\operatorname{mod} 11),$$

а оттам и на очевидно вярното сравнение

$$x + 6y \equiv x + 6y (\operatorname{mod} 11).$$

Следователно всеки елемент от I принадлежи и на I_1 и $I \subseteq I_1$. За обратното включване взимаме произволен елемент $a + b\sqrt{}\in I_1$. Ще покажем, че съществува елемент $x + y\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, такъв че $a + b\sqrt{3} = (x + y\sqrt{3})(1 + 2\sqrt{3})$. Последното е еквивалентно на равенството

$$a + b\sqrt{3} = x + 6y + (2x + y)\sqrt{3}$$

или на съществуване на целочислено решение на системата

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

за произволни числа $a, b \in \mathbb{Z}$, такива че $a \equiv 6b (\bmod 11)$. Решенията на системата са $(x, y) = \left(\dfrac{6b - a}{11}, \dfrac{2a - b}{11}\right)$. Очевидно $x \in \mathbb{Z}$ от условието, наложено върху a и b. За y имаме, че

$$y = \frac{2a - b}{11} = \frac{2(6b + 11k) - b}{11} = \frac{11b + 11k}{11} = b + k \in \mathbb{Z}$$

за произволно цяло число $k \in \mathbb{Z}$. С това всеки елемент от I_1 принадлежи и на I и така $I_1 \subseteq I$. Окончателно $I = I_1$.

Разглеждаме изображението

$$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_{11},$$

дефинирано с $\varphi(a + b\sqrt{3}) = \overline{a - 6b} = a - 6b + 11\mathbb{Z} \in \mathbb{Z}_{11}$. За произволни два елемента от $\mathbb{Z}[\sqrt{3}]$ имаме, че

$$\varphi[(a_1+b_1\sqrt{3})+(a_2+b_2\sqrt{3})] = \varphi[(a_1+a_2)+(b_1+b_2)\sqrt{3}] = (a_1+a_2)-6(b_1+b_2)+11\mathbb{Z} =$$

$$= (a_1 - 6b_1 + 11\mathbb{Z}) + (a_2 - 6b_2 + 11\mathbb{Z}) = \varphi(a_1 + b_1\sqrt{3}) + \varphi(a_2 + b_2\sqrt{3})$$

и

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

$$= (a_1a_2+3b_1b_2)-6(a_1b_2+a_2b_1)+11\mathbb{Z} = a_1a_2-6a_1b_2-6a_2b_1-3b_1b_2 = 11\mathbb{Z} =$$

$$= a_1a_2 - 6a_1b_2 - 6a_2b_1 - 36b_1b_2 + 11\mathbb{Z} = (a_1 - 6b_1 + 11\mathbb{Z})(a_2 - 6b_2 + 11\mathbb{Z}) =$$

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

с което φ е хомоморфизъм на пръстени. Елементът $a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ е от ядрото $\operatorname{Ker}\varphi \iff \varphi(a + b\sqrt{3}) = 11\mathbb{Z} \iff a - 6b = 11\mathbb{Z} \iff a \equiv 6b (\operatorname{mod} 11) \iff a + b\sqrt{3} \in I$, което означава, че $\operatorname{Ker}\varphi = I$. Остава да докажем, че $\mathbb{Z}_{11} \subseteq \operatorname{Im}\varphi$. Наистина, за всяко число $c = 0, 1, \dots, 10$ съществуват някакви цели числа $a, b \in \mathbb{Z}$ (например $a = 7c, b = c$), такива че $a - 6b + 11\mathbb{Z} = c + 11\mathbb{Z}$, т.е. $\varphi(a + b\sqrt{3}) = c + 11\mathbb{Z}$ за $a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Това означава, че всеки елемент на $\mathbb{Z}_{11}$ е от образа $\operatorname{Im}\varphi$ и комбинирайки това с тривиалното включване $\operatorname{Im}\varphi \subseteq \mathbb{Z}_{11}$ имаме, че $\operatorname{Im}\varphi = \mathbb{Z}_{11}$. Сега, прилагайки теоремата за хомоморфизмите на пръстени, доказваме исканото твърдение $\mathbb{Z}[\sqrt{3}]/I \cong \mathbb{Z}_{11}$. □

Задача 9. *Да се докаже, че идеалът* $I = (1+\sqrt{-5}, 1-\sqrt{-5})$ *на пръстена* $\mathbb{Z}[\sqrt{-5}]$ *не е главен и да се докаже, че* $\mathbb{Z}[\sqrt{-5}]/I \cong \mathbb{Z}_2$*.*

Решение. Тъй като идеалът I има два пораждащи елемента, то

$$I = \left\{(a_1 + b_1\sqrt{-5})(1 + \sqrt{-5}) + (a_2 + b_2\sqrt{-5})(1 - \sqrt{-5})\right\},$$

където $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Тогава произволен елемент от него има вида

$$a + b\sqrt{-5} = (a_1 + b_1\sqrt{-5})(1 + \sqrt{-5}) + (a_2 + b_2\sqrt{-5})(1 - \sqrt{-5}) =$$

$$= \underbrace{a_1 + a_2 - 5b_1 + 5b_2}_{a} + \underbrace{(a_1 - a_2 + b_1 + b_2)}_{b}\sqrt{-5}.$$

Забелязваме, че $a - b = 2a_2 - 6b_1 + 4b_2$ и очевидно $a - b \equiv 0 (\operatorname{mod} 2)$, т.е. $a \equiv b (\operatorname{mod} 2)$. С други думи, т.к. елементът $a+b\sqrt{-5} \in I$ беше произволен, доказахме включването

$$I \subseteq \{a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] \mid a \equiv b (\operatorname{mod} 2)\}.$$

Да видим дали имаме обратното включване. Нека $a + b\sqrt{-5}$ е такъв елемент, че $a \equiv b (\operatorname{mod} 2)$. Тогава може да запишем, че $a = b + 2k$ за някакво цяло число $k \in \mathbb{Z}$. Ще докажем, че този елемент се съдържа в I. За целта трябва да намерим елементи $a_1+b_2\sqrt{-5}, a_2+b_2\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, такива че

$$a + b\sqrt{-5} = (a_1 + b_1\sqrt{-5})(1 + \sqrt{-5}) + (a_2 + b_2\sqrt{-5})(1 - \sqrt{-5}) =$$

$$= a_1 + a_2 - 5b_1 + 5b_2 + (a_1 - a_2 + b_1 + b_2)\sqrt{-5}.$$

Поселдното е еквивалентно на това да намерим целочислено решение на системата

$$\left|\begin{array}{lllll} a_1 & +a_2 & -5b_1 & +5b_2 & = b+2k, \\ a_1 & -a_2 & +b_1 & +b_2 & = b \end{array}\right.$$

за произволни фиксирани числа $b, k \in \mathbb{Z}$. Ако b_1, b_2 са свободните параметри на системата, тя ще има безбройно много решения за a_1 и a_2, като $a_2 = 3b_1 - 2b_2 + k \in \mathbb{Z}$ и $a_1 = -b_1 - b_2 + b - 4k \in \mathbb{Z}$. Следователно наистина можем да намерим целочислено решение на системата и тогава обратното включване е в сила. По този начин доказахме, че

$$I = \{a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}] \mid a \equiv b (\operatorname{mod} 2)\}.$$

Сега е ясно, че $1 \notin I$, защото $1 = 1 + 0\sqrt{-5}$ и $1 \not\equiv 0 (\operatorname{mod} 2)$. Оттук следва и че $I \neq \mathbb{Z}[\sqrt{-5}] = (1)$. Още, $2 \in I$, но $I \neq (2)$, защото например $1 + 3\sqrt{-5} \in I$, но не е в (2).

Нека сега да допуснем, че идеалът I е главен, т.е. че съществува елемент $a_0 + b_0\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]\backslash\{1, 2\}$, такъв че $I = (a_0 + b_0\sqrt{-5})$. Т.к. $2 \in I$, то тогава трябва да съществува елемент $x + y\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, такъв че

$$(x + y\sqrt{-5})(a_0 + b_0\sqrt{-5}) = 2.$$

Последното е еквивалентно на съществуване на целочислено решение на системата

$$\left|\begin{array}{lll} a_0 x & +5b_0 y & = 2, \\ b_0 x & -a_0 y & = 0 \end{array}\right.$$

за неизвестните x, y, което е невъзможно. Противоречието доказва, че допускането е грешно и остава да е вярно, че не съществува елемент на $\mathbb{Z}[\sqrt{-5}]$, който да поражда I, т.е. I не е главен идеал.

За останалата част на задачата разгледайте изображението

$$\varphi : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}_2,$$

дефинирано с $\varphi(a + b\sqrt{-5}) = a - b + 2\mathbb{Z}$ за всеки елемент от $\mathbb{Z}[\sqrt{-5}]$. Докажете, че то е хомоморфизъм на пръстени с ядро $\operatorname{Ker} \varphi = I$ и образ $\operatorname{Im} \varphi = \mathbb{Z}_2$ и приложете теоремата за хомоморфизмите на пръстни. $\square$