Київський національний університет
імені Тараса Шевченка

Н.С.Головащук, Є.А.Кочубінська, С.А.Овсієнко

ЗБІРНИК ЗАДАЧ З ТЕОРІЇ КІЛЕЦЬ (БАЗОВИЙ КУРС)

Навчальний посібник
для студентів механіко – математичного факультету

Київ
Видавничо–поліграфічний центр
"Київський університет"
2013

Н.С.Головащук, Є.А.Кочубінська, С.А.Овсієнко. Збірник задач з теорії кілець (базовий курс). – Навчальний посібник для студентів механіко – математичного факультету. – К.: Видавничо–поліграфічний центр "Київський університет", 2013. – 86 с.

Рецензенти: д-р фіз.-мат. наук, проф. Ю.В.Боднарчук
д-р фіз.-мат. наук, проф. В.В.Кириченко

Наведено завдання для практичних занять з курсу теорії кілець в обсязі, передбаченому навчальними планами механіко – математичного факультету.

Рекомендовано до друку вченою радою механіко – математичного факультету Київського національного університету імені Тараса Шевченка (протокол № 7 від 18 лютого 2013 року)

Зміст

Передмова **3**

Позначення **4**

1 Поняття кільця та підкільця **5**

2 Дільники нуля та одиниці. Нільпотентні елементи. Ідемпотенти **14**

3 Ідеали **20**

4 Гомоморфізми та факторкільця **29**

5 Теорія подільності. Факторіальні кільця **36**

6 Евклідові кільця **42**

7 Китайська теорема про остачі **48**

8 Мала теорема Ферма. Теорема Ейлера **54**

9 Символи Лежандра та Якобі **56**

10 Локалізація **59**

Відповіді і вказівки **62**

Література **83**

Зміст

Передмова

Посібник укладено на основі матеріалів практичних занять з нормативного курсу алгебри та теорії чисел, які автори ведуть на механіко–математичному факультеті Київського національного університету імені Тараса Шевченка.

Посібник складається з 10 розділів. У кожному з них наведено теоретичні відомості, означення та поняття, необхідні для розв'язування задач з даного розділу. До задач даються відповіді, а до більш складних з них — вказівки для розв'язування. Серед задач є приклади, які ілюструють загальні твердження. В кінці посібника дано посилання на джерела, які дозволять поглибити свої знання з курсу теорії кілець.

Посібник є доступним для студента–математика, який володіє базовими знаннями з курсу алгебри. Він створить необхідну загальноматематичну базу для подальшого поглибленого опанування сучасними алгебраїчними методами.

Позначення

$(A, *_1, \ldots, *_k)$	множина A, на якій визначено бінарні дії $*_1, \ldots, *_k$
$a\|b$	a ділить b
(a, b)	найбільший спільний дільник чисел a і b
$\mathbb{C}$	поле комплексних чисел
D	область цілісності
e_{ij}	матрична одиниця
$\mathbb{F}_q$	скінченне поле з q елементів
$\mathbb{H}$	кільце дійсних кватерніонів
$\Bbbk$	абстрактне поле
$\Bbbk^*$	мультиплікативна група поля $\Bbbk$
K_4	четверна група Клейна
$\mathbb{N}$	адитивна напівгрупа натуральних чисел
$\mathbb{N}_0$	адитивна напівгрупа всіх невід'ємних цілих чисел
$M_n(R)$	кільце матриць порядку n з коефіцієнтами з кільця R
$\mathbb{Q}$	поле раціональних чисел
Q_8	група кватерніонів
$\mathbb{R}$	поле дійсних чисел
R	абстрактне кільце
R^*	мультиплікативна група кільця R
$R[G]$	групове кільце групи G над кільцем R
$T_n(R)$	кільце верхніх трикутних матриць
$\mathbb{Z}$	кільце цілих чисел
$\mathbb{Z}[i]$	кільце цілих гаусових чисел
$Z(R)$	центр кільця R
$\mathbb{Z}_n$	кільце лишків за модулем n

1 Поняття кільця та підкільця

Означення 1.1. *Кільцем називається множина R , на якій задано дві бінарні операції, $+, \cdot : \ R \times R \to R$, які називаються додаванням та множенням відповідно, і які задовольняють наступні умови:*

(i) $(R, +)$ *є абелевою групою (яка називається адитивною групою кільця);*

(ii) $(R, \cdot)$ *є моноїдом з одиницею 1;*

(iii) *додавання та множення пов'язані дистрибутивними законами:*

- $a \cdot (b + c) = a \cdot b + a \cdot c$ *для довільних* $a, b, c \in R$*;*
- $(a + b) \cdot c = a \cdot c + b \cdot c$ *для довільних* $a, b, c \in R$*.*

Якщо потрібно підкреслити, що одиниця є одиницею саме кільця R, то писатимемо 1_R. Для елемента $r \in R$ та $n \in \mathbb{N}$ позначатимемо $nr = \underbrace{r + \ldots + r}_{n}$, для елементів $a, b \in R$ писатимемо $a - b = a + (-b)$.

Кільце R називається

- *комутативним*, якщо $(R, \cdot)$ — комутативна напівгрупа.
- *кільцем з діленням*, якщо $1 \neq 0$ і $(R \setminus \{0\}, \cdot)$ — група;
- *полем*, якщо $(R \setminus \{0\}, \cdot)$ — комутативна група.

Приклад 1.2. 1. $R = \{0\}$ — тривіальне, або нульове, кільце. Зауважимо, що $1 = 0$ тоді і лише тоді, коли $R = \{0\}$. Надалі ми будемо розглядати лише ті кільця, в яких $1 \neq 0$.

2. Множина $\mathbb{Z}$ цілих чисел є комутативним кільцем відносно стандартних операцій додавання і множення.

3. Нехай p — фіксоване просте число. Множина $\mathbb{Z}\left[\frac{1}{p}\right]$ всіх таких раціональних чисел, у нескоротному записі яких знаменники є степенями числа p, є комутативним кільцем відносно стандартних операцій додавання і множення.

4. Нехай $d \in \mathbb{Z}$ — вільне від квадратів число. Множина $\mathbb{Z}[\sqrt{d}] = \left\{ a + b\sqrt{d} \,|\, a, b \in \mathbb{Z} \right\}$ є комутативним кільцем відносно стандартних операцій додавання і множення. Кільця такого вигляду називаються *квадратичними кільцями*.

5. Множина $\mathbb{Z}_n$ лишків за модулем n є комутативним кільцем відносно додавання і множення за модулем натурального числа n.

6. Множина $\mathrm{M}_n(R)$ квадратних матриць порядку n над кільцем R є некомутативним кільцем відносно операцій матричних додавання та множення.

7. Нехай $A \subset \mathbb{R}$. Множина всіх функцій $f\colon A \to \mathbb{R}$ є кільцем відносно операцій поточкового додавання і множення, визначених рівностями $(f+g)(x) = f(x) + g(x)$ та $(fg)(x) = f(x)g(x)$ для всіх $x \in A$, $f, g\colon A \to R$.

8. Нехай $\Bbbk[x]$ — множина многочленів від змінної x з коефіцієнтами з поля $\Bbbk$. Сума і добуток многочленів $f(x) = \sum_{i=0}^{n} a_i x^i$ та $g(x) = \sum_{i=0}^{m} b_i x^i$ $(n \geqslant m)$ визначаються як

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

$$f(x)g(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k.$$

Відносно так введених операцій множина $\Bbbk[x]$ є кільцем.

Множина $S \subset A$ називається замкненою відносно бінарної операції $*$, заданої на A, якщо для довільних $s_1, s_2 \in S$ виконується $s_1 * s_2 \in S$.

Означення 1.3. *Підмножина S кільця R називається підкільцем, якщо*

(i) *S є підгрупою адитивної групи кільця;*

(ii) *S замкнена відносно множення;*

(iii) $1 \in S$.

Іншими словами, підмножина $S \subset R$ є підкільцем кільця R, якщо S є кільцем відносно бінарних операцій, що задають структуру кільця на R. Зокрема, кільце є своїм підкільцем. Підкільця поля комплексних чисел називають числовими кільцями.

Централізатром підмножини X кільця R називається множина

$$C(X) = \{r \in R \,|\, rx = xr \text{ для всіх } x \in X\}.$$

Центром кільця R називається множина

$$Z(R) = \{r \in R \,|\, xr = rx \text{ для всіх } x \in R\},$$

тобто центр кільця R — це централізатор множини $X = R$.

Прямим добутком кілець R та S називається множина

$$R \times S = \{(r, s) \,|\, r \in R,\ s \in S\}$$

з покомпонентними операціями додавання і множення:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$

$$(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2),$$

де $r_1, r_2 \in R$, $s_1, s_2 \in S$. Легко перевірити, що прямий добуток кілець є кільцем з одиницею $(1_R, 1_S)$.

Означення 1.4. *Нехай R та S — кільця. Ізоморфізмом кілець називається бієктивне відображення $\varphi\colon R \to S$, яке зберігає операції додавання та множення, тобто для довільних $r_1, r_2 \in R$ виконується:*

(i) $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$;

(ii) $\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$.

Задачі

1.1. Користуючись лише означенням кільця, доведіть, що

a) $a \cdot 0 = 0 \cdot a = 0$ для довільного $a \in R$;

b) $a \cdot (-b) = (-a)b = -ab$ для довільних $a, b \in R$;

c) $a(b - c) = ab - ac$ для довільних елементів $a, b, c \in R$.

1.2. Покажіть, що для довільного кільця R умова комутативності додавання є надлишковою в тому сенсі, що вона випливає з інших аксіом кільця.

1.3. Перевірте, що множина $\mathbb{Z}$ цілих чисел відносно звичайних операцій додавання та множення є комутативним кільцем. Вкажіть підкільця кільця $\mathbb{Z}$.

1.4. Нехай R — кільце, адитивна група якого циклічна. Доведіть, що кільце R є комутативним.

1.5. Покажіть, що перетин $R_1 \cap R_2$ підкілець R_1 та R_2 кільця R є підкільцем кільця R. За яких умов об'єднання $R_1 \cup R_2$ підкілець R_1 та R_2 є підкільцем кільця R?

1.6. Які з наступних множин утворюють кільце відносно стандартних операцій додавання та множення:

a) $\{a + b\sqrt{6} \,|, a, b \in \mathbb{Z}\}$;

b) $\{a + b\sqrt{2} + c\sqrt{6} \,|\, a, b, c \in \mathbb{Q}\}$;

c) $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,|\, a, b, c, d \in \mathbb{Q}\}$;

d) $\{a + b\sqrt[3]{6} \,|, a, b \in \mathbb{Q}\}$;

e) $\{a + b\sqrt[3]{6} + c\sqrt[3]{36} \,|\, a, b \in \mathbb{Z}\}$?

1.7. Які з наступних кілець є полями: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_9$, $\mathbb{Z}_7$, $M_2(\mathbb{Q})$, $M_2(\mathbb{R})$?

1.8. Які з наступних множин утворюють поле відносно стандартних операцій додавання та множення:

a) $\{a + bi\sqrt{3} \,|\, a, b \in \mathbb{Q}\}$;

b) $\{a + bi\sqrt{3} \mid a, b \in \mathbb{Z}\}$;

c) $\{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$;

d) $\{a + b\sqrt{3} \mid a, b \in \mathbb{R}\}$?

1.9. Перевірте, що $\mathbb{Z}_n$ є кільцем відносно операцій додавання і множення за модулем натурального числа n. Для яких $n \in \mathbb{N}$ кільце $\mathbb{Z}_n$ є полем?

1.10. Покажіть, що множина $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ є числовим кільцем. Це кільце називають *кільцем цілих гаусових чисел*.

1.11. Доведіть, що множина $\mathbb{Q}[i] = \{a + bi \mid a, b \in \mathbb{Q}\}$ є полем. Це поле називають *полем раціональних гаусових чисел*.

1.12. Нехай $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Покажіть, що $1 + \omega + \omega^2 = 0$. Доведіть, що множина $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ є числовим кільцем. Числа вигляду $a + b\omega$, $a, b \in \mathbb{Z}$, називаються *цілими числами Ейзенштейна*.

1.13. З'ясуйте, чи є множина $\mathbb{Z}[\eta] = \{a + b\eta \mid a, b \in \mathbb{Z}\}$, де $\eta = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, числовим кільцем.

1.14. Покажіть, що множина $\mathrm{M}_n(R)$ матриць порядку n, $n > 1$, над кільцем R відносно операцій додавання і множення матриць є некомутативним кільцем.

1.15. Які з наступних підмножин кільця матриць $M_n(\mathbb{R})$, $n > 1$, є його підкільцями:

a) множина всіх симетричних матриць;

b) множина всіх кососиметричних матриць;

c) множина всіх вироджених матриць;

d) множина всіх невироджених матриць;

e) множина всіх скалярних матриць;

f) множина всіх діагональних матриць;

g) множина всіх матриць з раціональним визначником?

1.16. Нехай R — довільне кільце. Покажіть, що множина

$$A = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Big| \, a + c = b + d \in R \right\}$$

є підкільцем кільця $\mathrm{M}_2(R)$. Покажіть, що це кільце ізоморфне кільцю верхніх трикутних матриць порядку 2 над R.

1.17. Доведіть, що кільця верхніх та нижніх трикутних матриць порядку n над полем $\Bbbk$ ізоморфні.

1.18. Нехай

$$S = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} \Big| a, b \in \mathbb{Z} \right\},$$

де d — ціле число, яке не є квадратом в $\mathbb{Z}$.

1) Перевірте, що S є підкільцем кільця $\mathrm{M}_2(\mathbb{Z})$.

2) Покажіть, що відображення $\varphi : \mathbb{Z}[\sqrt{d}] \to S$, визначене як $\varphi(a + b\sqrt{d}) = \begin{pmatrix} a & b \\ db & a \end{pmatrix}$, є ізоморфізмом кілець.

1.19. Покажіть, що при $d \equiv 1 \pmod 4$ множина

$$A = \left\{ \begin{pmatrix} a & b \\ \frac{(d-1)\,b}{4} & a + b \end{pmatrix} \Big| a, b \in \mathbb{Z} \right\}$$

є підкільцем кільця $M_2(\mathbb{Z})$. Покажіть, що кільце A ізоморфне квадратичному кільцю $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

1.20. Покажіть, що множина

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \Big| a, b \in \mathbb{R} \right\}$$

є підкільцем кільця $\mathrm{M}_2(\mathbb{R})$, яке ізоморфне полю $\mathbb{C}$.

1.21. Нехай $A \subset \mathbb{R}$. Чи утворюють кільце наступні множини функцій:

а) $F_1 = \{f : A \to \mathbb{R}\}$;

b) $F_2 = \{f : A \to \mathbb{R} \mid f$ — неперервна$\}$;

c) $F_3 = \{f : A \to \mathbb{R} \mid f(x) = a, a \in \mathbb{R}$ — фіксоване$\}$;

d) $F_4 = \{f : \mathbb{R} \to \mathbb{Z}\}$;

e) $F_5 = \{f : A \to \mathbb{R} \mid f(x) = 0$ для всіх $x \in B \subset A\}$;

f) $F_6 = \{\sum_{k=1}^{n} a_k \sin kx \mid a_1, \ldots, a_n \in \mathbb{R}, n \in \mathbb{N}\}$;

g) $F_7 = \{a_0 + \sum_{k=1}^{n} a_k \cos kx \mid a_1, \ldots, a_n \in \mathbb{R}, n \in \mathbb{N}\}$;

h) $F_8 = \left\{a_0 + \sum_{k=1}^{n} (a_k \cos kx + b_k \sin kx) \mid a_k, b_k \in \mathbb{R}, k = \overline{1, n}\right\}$ (многочлени такого вигляду називаються многочленами Фур'є, або тригонометричними многочленами).

1.22. Кільце R називається *булівським* кільцем, якщо $a^2 = a$ для довільного $a \in R$. Доведіть, що довільне булівське кільце є комутативним.

1.23. Нехай $\mathcal{B}(X)$ – множина всіх підмножин множини X з діями додавання та множення, визначеними за правилами

$$A + B = (A \setminus B) \cup (B \setminus A) \text{ (симетрична різниця)}$$

та

$$A \cdot B = A \cap B.$$

Покажіть, що $\mathcal{B}(X)$ — комутативне кільце. Переконайтеся, що кільце $\mathcal{B}(X)$ є булівським.

1.24. Покажіть, що кільце $\mathbb{Z}_2 \times \mathbb{Z}_2$ є булівським.

1.25. Нехай R, S — кільця. Покажіть, що кільце $R \times S$ — булівське тоді і лише тоді, коли кільця R та S — булівські.

1.26. Покажіть, що для довільного кільця R множина діагональних елементів $\{(a, a) \mid a \in R\}$ утворює підкільце кільця $R \times R$, яке ізоморфне кільцю R.

1.27. Покажіть, що для довільного простого числа p

a) кільце, яке складається з p^2 елементів, є комутативним;

b) існує некомутативне кільце, яке складається з p^3 елементів.

1.28. Нехай для символів i, j, k виконуються рівності:

$$i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k, \quad jk = -kj = i \quad ki = -ik = j.$$

Покажіть, що множина $\mathbb{H} = \{a + bi + cj + dk \,|\, a, b, c, d \in \mathbb{R}\}$ є асоціативним некомутативним кільцем. Кільце $\mathbb{H}$ називається *кільцем дійсних кватерніонів*.

1.29. Для кватерніона $q = a + bi + cj + dk \in \mathbb{H}$ визначимо операцію спряження

$$\overline{q} = a - bi - cj - dk$$

та норму

$$|q| = a^2 + b^2 + c^2 + d^2.$$

Через $\operatorname{Re} q = a$ позначимо дійсну частину кватерніона. Покажіть, що

a) $\overline{pq} = \overline{q} \cdot \overline{p}$ для довільних кватерніонів p та q (антикомутативність спряження);

b) для кватерніона $q \in \mathbb{H}$ справедлива тотожність:

$$\overline{q} = -\frac{1}{2}\big(q + iqi + jqj + kqk\big);$$

c) норма в $\mathbb{H}$ мультиплікативна: $|pq| = |p| \cdot |q|$, $p, q \in \mathbb{H}$ (тотожність Ейлера чотирьох квадратів);

d) $\mathbb{H}$ є кільцем з діленням;

e) мультиплікативна група підкільця

$$\{a + bi + cj + dk \,|\, a, b, c, d \in \mathbb{Z}\} \subset \mathbb{H}$$

є групою кватерніонів Q_8;

f) рівняння $q^2 + 1 = 0$ має нескінченно багато розв'язків в $\mathbb{H}$.

1.30. Нехай $G = \{g_1, \ldots, g_n\}$ – деяка скінченна група, R – кільце. Покажіть, що множина усіх скінченних сум вигляду $a_1 g_1 + \ldots + a_n g_n$, $a_i \in R$, утворює кільце відносно операцій

$$\Big(\sum_{i=1}^{n} a_i g_i\Big) + \Big(\sum_{i=1}^{n} b_i g_i\Big) = \sum_{i=1}^{n} (a_i + b_i) g_i$$

та

$$\Big(\sum_{i=1}^{n} a_i g_i\Big) \cdot \Big(\sum_{i=1}^{n} b_i g_i\Big) = \sum_{g \in G} \sum_{g_i g_j = g} (a_i \cdot b_j) g.$$

Воно називається *груповим кільцем* групи G над кільцем R і позначається $R[G]$.

1.31. Покажіть, що множина усіх можливих сум вигляду $\alpha_1 \xi_1 + \ldots + \alpha_n \xi_n$, де $\alpha_1, \ldots, \alpha_n$ — дійсні числа, $\xi_1, \ldots, \xi_n$ — всі комплексні корені степеня n з 1, є груповим кільцем над $\mathbb{R}$.

1.32. Нехай X — деяка підмножина кільця R. Покажіть, що підмножина

$$C(X) = \{r \in R \,|\, rx = xr \text{ для всіх } x \in X\}$$

є підкільцем R. Множина $C(X)$ називається *централізатором* множини X.

1.33. Нехай R — кільце з діленням. Покажіть, що централізатор $C(a) = \{r \in R \,|\, ra = ar\}$ довільного елемента $a \in R$ є кільцем з діленням.

1.34. Покажіть, що кільце R є комутативним тоді і лише тоді, коли $x^2 - x \in Z(R)$ для довільного $x \in R$, де $Z(R)$ — центр кільця R.

1.35. Нехай на множині

$$T = \{f : \mathbb{R} \to \mathbb{R} \,|\, f(x) = a \cos x + b \sin x \,|\, a, b \in \mathbb{R}\}$$

визначені стандартне додавання та множення

$$f * g = \frac{1}{\pi} \int_0^{2\pi} f(t) g(x - t) dt.$$

(Ця операція називається згорткою.) Покажіть, що $\big(T, +, *\big)$ є полем.

2 Дільники нуля та одиниці. Нільпотентні елементи. Ідемпотенти

Елемент $a \in R$, $a \neq 0$, називається *лівим* (*правим*) *дільником нуля*, якщо існує такий елемент $b \in R$, $b \neq 0$, що $ab = 0$ (відповідно, $ba = 0$). Елемент $a \in R$, $a \neq 0$, називається *дільником нуля*, якщо він одночасно є і правим, і лівим дільником нуля.

Елемент $a \in R$ називається *лівим* (*правим*) *дільником одиниці*, якщо існує такий елемент $b \in R$, що $ab = 1$ (відповідно, $ba = 1$).

Лема 2.1. *Правий* (*лівий*) *дільник одиниці не може бути лівим* (*правим*) *дільником нуля.*
Правий (*лівий*) *дільник нуля не може бути лівим* (*правим*) *дільником одиниці.*

Лема 2.2. *Кожний ненульовий елемент скінченного кільця є або дільником нуля, або дільником одиниці.*

Елемент $a \in R$ називається *оборотним елементом* кільця R, якщо він є і правим, і лівим дільником одиниці.

Множина всіх оборотних елементів кільця R позначається через R^*.

Лема 2.3. *Множина R^* є групою відносно множення.*

Ця група називається *мультиплікативною групою* кільця.

Елемент $e \in R$ називається *ідемпотентом*, якщо $e^2 = e$. Елемент $a \in R$ називається *нільпотентним*, якщо $a^n = 0$ для деякого $n \in \mathbb{N}$. Найменше таке n називається *ступенем, або класом, нільпотентності*. Ясно, що кожний нільпотентний елемент є дільником нуля. Зворотне твердження в загальному випадку не є вірним.

Комутативне кільце без дільників нуля називається *областю цілісності*.

Лема 2.4. *Комутативне кільце R є областю цілісності тоді і лише тоді, коли для довільних ненульового елемента $a \in R$ і $b, c \in R$ з рівності $ab = ac$ випливає рівність $b = c$.*

Задачі

2.1. Знайдіть дільники нуля в кільці цілих чисел. Опишіть мультиплікативну групу $\mathbb{Z}^*$.

2.2. Знайдіть дільники нуля в кільці цілих гаусових чисел. Опишіть мультиплікативну групу цього кільця.

2.3. Знайдіть дільники нуля в кільці цілих чисел Ейзенштейна (див. задачу 1.12). Опишіть мультиплікативну групу цього кільця.

2.4. Доведіть, що ненульовий ідемпотент області цілісності D є одиницею в D.

2.5. Доведіть, що

a) кожний елемент кільця $\mathbb{Z}_n$ є або дільником нуля, або дільником одиниці;

b) в кільці $\mathbb{Z}_n$ ненульовий елемент $\overline{a}$ є дільником нуля тоді і лише тоді, коли $(a, n) \neq 1$;

c) в кільці $\mathbb{Z}_n$ ненульовий елемент $\overline{a}$ є дільником одиниці тоді і лише тоді, коли $(a, n) = 1$;

d) елемент $\overline{a} \in \mathbb{Z}_n$ є нільпотентним тоді і лише тоді, коли a ділиться на кожний простий дільник числа n.

2.6. Які з елементів кільця $\mathbb{Z}_{12}$ є дільниками нуля? дільниками одиниці? нільпотентними? ідемпотентами?

2.7. Знайдіть обернені до елементів $\overline{7}$, $\overline{8}$, $\overline{11}$ в кільці $\mathbb{Z}_{15}$.

2.8. Знайдіть усі дільники одиниці квадратичного кільця

$$\mathbb{Z}[i\sqrt{d}] = \left\{ a + bi\sqrt{d} \,|\, a, b \in \mathbb{Z} \right\},$$

де d — вільне від квадратів натуральне число.

2.9. Покажіть, що в квадратичному кільці

$$\mathbb{Z}[\sqrt{3}] = \left\{ a + b\sqrt{3} \,|\, a, b \in \mathbb{Z} \right\}$$

існує нескінченно багато дільників одиниці.

2.10. Покажіть, що в квадратичному кільці

$$\mathbb{Z}[\sqrt{6}] = \left\{ a + b\sqrt{6} \,|\, a, b \in \mathbb{Z} \right\}$$

існує нескінченно багато дільників одиниці.

2.11. Знайдіть усі дільники нуля, оборотні та нільпотентні елементи в кільцях:

a) верхніх трикутних матриць над полем $\Bbbk$;

b) усіх функцій, які визначені на деякій множині X і приймають значення в полі $\Bbbk$;

c) $\mathrm{M}_2(\mathbb{R})$;

d) $\mathcal{B}(X)$ (див. задачу 1.23).

2.12. Знайдіть нільпотентні елементи кільця

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \,\middle|\, a \in \mathbb{Z}_{2^k}, b, c \in \mathbb{Z}_2 \right\}.$$

2.13. Яка з матриць

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ чи } C = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

є дільником нуля в кільці $\mathrm{M}_3(\mathbb{Q})$? Опишіть дільники нуля та одиниці в кільці $\mathrm{M}_n(\mathbb{Q})$, $n > 1$.

2.14. З'ясуйте, які з наступних многочленів

a) $x^2 + x + 1$;

b) $x^2 + 2x + 2$;

c) $2x^2 + 2$;

d) $2x^2 + 4x + 2$;

e) $3x^2 + 2x + 3$;

f) $3x^2 + 3x + 3$

є дільниками нуля в кільці $\mathbb{Z}_6[x]$.

2.15. З'ясуйте, які з наступних многочленів

a) $x^3 + x^2 + x + 1$;

b) $2x^3 + 2x^2 + 2x + 2$;

c) $2x^2 + 2x + 2$;

d) $2x^2 + 2x + 1$;

e) $2x^2 + 2x$;

f) $x^2 + x + 1$

є дільниками нуля в кільці $\mathbb{Z}_4[x]$.

2.16. Доведіть, що кільце многочленів $R[x]$ над R має дільники нуля тоді і лише тоді, коли їх має кільце R.

2.17. Опишіть дільники одиниці, дільники нуля та ніль-потентні елементи у кільцях

a) $\mathbb{Z}_p \times \mathbb{Z}_p$, де p — просте число;

b) $\mathbb{Z}_4 \times \mathbb{Z}_4$;

c) $\mathbb{Z}_4 \times \mathbb{Z}_6$.

2.18. Нехай $\Bbbk$ — довільне поле. Опишіть дільники нуля та одиниці в кільці $\underbrace{\Bbbk \times \ldots \times \Bbbk}_{n}$. Чи є прямий добуток полів полем?

2.19. Нехай R та S — кільця. Доведіть, що ненульовий елемент $(r, s) \in R \times S$ є правим (лівим) дільником нуля тоді і лише тоді, коли хоча б один з елементів r або s є правим (лівим) дільником нуля або нулем.

2.20. Нехай R та S — кільця. Доведіть, що елемент $(r, s) \in R \times S$ є нільпотентним тоді і лише тоді, коли r та s є нільпотентними.

2.21. Нехай R та S — кільця. Доведіть, що елемент $(r, s) \in R \times S$ є оборотним тоді і лише тоді, коли r та s є оборотними.

2.22. Нехай R та S — кільця. Доведіть, що елемент $(r, s) \in R \times S$ є ідемпотентом тоді і лише тоді, коли r та s є ідемпотентами.

2.23. Нехай R — кільце без дільників нуля, $a, b \in R$. Чи справедливі наступні твердження:

a) якщо ab — оборотний елемент кільця R, то a і b теж є оборотними елементами кільця R;

b) якщо a^n — оборотний елемент кільця R, то a — оборотний елемент кільця R?

2.24. Нехай x — нільпотентний елемент комутативного кільця R. Перевірте, що

a) x є або нулем, або дільником нуля;

b) rx є нільпотентним елементом для довільного $r \in R$;

c) елементи $1 + x$ та $1 - x$ є дільниками одиниці в R.

2.25. Нехай R — кільце, $a, b \in R$. Покажіть, що елемент $1 - ab$ є оборотним тоді і лише тоді, коли $1 - ba$ є оборотним. Знаючи обернений до $1 - ab$, знайдіть $(1 - ba)^{-1}$.

2.26. Опишіть дільники нуля та одиниці групового кільця $\mathbb{C}[C_3]$.

2.27. Покажіть, що елементи $a + b + c + 1$ та $a + b + c - 3$ групового кільця $\mathbb{Z}[K_4]$, де $K_4 = \{1, a, b, c\}$ — четверна група Клейна, є дільниками нуля. Чи є дільником нуля елемент $1 + a + b - 3c$?

2.28. Нехай $R[G]$ — групове кільце над скінченною групою G. Покажіть, що

a) довільний елемент $g \in G$ є оборотним в кільці $R[G]$;

b) елемент $g = g_1 + \ldots + g_n$ належить центру кільця $R[G]$;

c) елемент $(1 - g)$ є дільником нуля в кільці $R[G]$.

2.29. Нехай $\Bbbk$ — поле, G — група, яка містить елементи скінченного порядку. Покажіть, що групове кільце $\Bbbk[G]$ має дільник нуля.

2.30. Група називається *групою без скруту*, якщо всі її неодиничні елементи мають нескінченний порядок. Нехай $\Bbbk$ — поле, G — група без скруту. Доведіть, що групове кільце $\Bbbk[G]$ не має дільників нуля.

2.31. Нехай a — фіксований ненульовий елемент кільця R. Визначимо відображення $\mathtt{l}_a$, $\mathtt{r}_a \colon R \to R$ наступним чином $\mathtt{l}_a(x) = ax$, $\mathtt{r}_a(x) = xa$.

1) Доведіть, що відображення $\mathtt{l}_a$ є ін'єктивним тоді і лише тоді, коли a не є лівим дільником нуля.

2) Доведіть, що відображення $\mathtt{l}_a$ є сюр'єктивним тоді і лише тоді, коли a є лівим дільником одиниці.

Сформулюйте аналогічні твердження для відображення $\mathtt{r}_a$.

2.32. Нехай R — скінченне кільце. Доведіть, що коли відображення $\mathtt{l}_a$ ($\mathtt{r}_a$) є ін'єкцією або сюр'єкцією, то воно є бієкцією.

2.33. Нехай R — скінченне кільце. Доведіть, що

a) якщо R не має дільників нуля, то всі його ненульові елементи оборотні;

b) кожний елемент кільця R, для якого існує односторонній обернений, є оборотним;

c) кожний лівий дільник нуля є правим дільником нуля.

2.34. Доведіть, що в скінченному кільці кожний ненульовий елемент є або дільником нуля, або дільником одиниці.

2.35. Доведіть, що в кільці без дільників нуля кожен елемент, який має односторонній обернений, є оборотним.

2.36. Доведіть, що скінченна область цілісності є полем.
Зауваження. Насправді, має місце значно сильніше твердження, а саме: кожне скінченне кільце з діленням є полем. Це відома теорема Веддерберна.

2.37. Назвемо кільце R "хорошим", якщо деякий додатний степінь довільного елемента є ідемпотентом.

Доведіть, що

a) довільне скінченне кільце є хорошим;

b) якщо R — хороше кільце, то довільний елемент з R є або оборотним, або дільником нуля;

c) якщо R — хороше кільце, $u, v \in R$, то умови $uv = 1$ та $vu = 1$ еквівалентні.

3 Ідеали

Теоретичні відомості

Якщо A, B — дві підмножини кільця R, то позначатимемо

$$AB = \{ab \,|\, a \in A, b \in B\}$$

добуток множин A і B.

Означення 3.1. *Нехай R — кільце. Множина $I \subset R$, яка є адитивною підгрупою групи $(R, +)$, називається*

- *правим ідеалом кільця R, якщо $IR \subset I$;*
- *лівим ідеалом кільця R, якщо $RI \subset I$;*
- *ідеалом (або двостороннім ідеалом), якщо $RI \subset I$ та $IR \subset I$.*

Для будь-якого кільця R ідеалами завжди є саме кільце R та нульовий ідеал $\{0\}$. Вони називаються тривіальними ідеалами. Ідеали, які є власними підмножинами кільця, називаються *власними*. Ненульове кільце, яке має лише тривіальні двосторонні ідеали, називається *простим*.

Нехай R — кільце, $\mathfrak{X}$ – деяка підмножина кільця R. Ідеалом, породженим $\mathfrak{X}$, називається найменший ідеал, що містить $\mathfrak{X}$. Позначатимемо його через $(\mathfrak{X})$.

Розглянемо деяку підмножину $\mathfrak{X}$ кільця R. Нехай $\big(\mathfrak{X}\big)$ — ідеал, породжений $\mathfrak{X}$. Через $R\mathfrak{X}$ позначимо множину

$$R\mathfrak{X} = \{r_1x_1 + \ldots + r_nx_n \,|\, r_i \in R, x_i \in \mathfrak{X}, n \in \mathbb{N}\}$$

(за домовленістю, $R\mathfrak{X} = \{0\}$, якщо $\mathfrak{X} = \varnothing$). Аналогічно визначається множина $\mathfrak{X}R$. Покладемо

$$R\mathfrak{X}R = \{r_1x_1r_1' + \ldots + r_nx_nr_n' \,|\, r_i, r_i' \in R, x_i \in \mathfrak{X}, n \in \mathbb{N}\}.$$

Тоді $R\mathfrak{X}$ є лівим, $\mathfrak{X}R$ — правим, а $R\mathfrak{X}R$ — двостороннім ідеалом, породженим $\mathfrak{X}$, та має місце рівність

$$(\mathfrak{X}) = \bigcap_{I-\text{ідеал},\mathfrak{X}\subseteq I} I = R\mathfrak{X}R.$$

Ідеал, який породжений одним елементом $a \in R$, називається *головним ідеалом*, і позначається через (a). Ідеал, породжений скінченною множиною елементів, називається *скінченно породженим*. Скінченно породжений ідеал, який породжений елементами $a_1, \ldots, a_n$, позначається $(a_1, ..., a_n)$.

Зауваження 3.2. *Якщо кільце R не є комутативним, то правий ідеал aR, $a \in R$, у загальному випадку, не є двостороннім ідеалом. Більше того, множина $\{ras \,|\, r, s \in R\}$ не обов'язково є ідеалом, бо вона не замкнена відносно додавання.*

Приклад 3.3. Множина

$$\{(x+1)p(x) \,|\, p(x) \in \mathbb{Z}[x]\} = (x+1)\mathbb{Z}[x]$$

всіх многочленів, коренем яких є -1, є головним ідеалом кільця $\mathbb{Z}[x]$, породженим многочленом $x+1$.
Ідеал $(3, x) = \{3p(x) + xq(x) \,|\, p(x), q(x) \in \mathbb{Z}[x]\}$ не є головним ідеалом кільця $\mathbb{Z}[x]$.

Зауваження 3.4. *Множина усіх головних ідеалів довільного кільця є частково впорядкованою відносно включення, нульовий ідеал є найменшим елементом, а саме кільце найбільшим елементом.*

Власний ідеал I називається *мінімальним*, якщо з того, що існує ідеал J, для якого $\{0\} \subset J \subset I$, випливає $J = I$ або $J = \{0\}$. Власний ідеал I називається *максимальним*, якщо з того, що існує ідеал J, для якого $I \subset J \subset R$, випливає $J = I$ або $J = R$.

Область цілісності, в якій кожен ідеал є головним, називається *кільцем головних ідеалів*. Наприклад, кільця $\mathbb{Z}$, $\mathbb{Z}[i]$ та $\Bbbk[x]$, $\Bbbk$ — поле, є кільцями головних ідеалів.

Зауваження 3.5. *Кільце $\mathbb{Z}[x]$ не є кільцем головних ідеалів.*

Дії над ідеалами. Нехай I, J — ідеали кільця R.

Перетин ідеалів $I \cap J$ ідеалів I та J визначається як звичайний теоретико-множинний перетин.

Сума ідеалів визначається як множина

$$I + J = \{a + b \,|\, a \in I, b \in J\}.$$

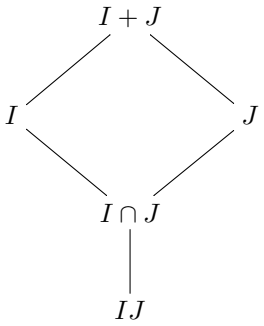
Це найменший ідеал в R, який містить I і J.

Добуток ідеалів IJ визначається як множина

$$\{a_1 b_1 + \ldots + a_k b_k \,|\, a_i \in I, b_i \in J\},$$

що містить усі скінченні суми елементів вигляду ab, $a \in I$, $b \in J$. Множина IJ є ідеалом, який міститься в $I \cap J$. Зауважимо, що множина $\{ab \,|\, a \in I, b \in J\}$ як правило не є замкненою відносно додавання, а отже, не обов'язково має бути ідеалом.

Неважко бачити, що сума $I + J$ ідеалів I та J є найменшим ідеалом в R, який містить одночасно I та J, добуток IJ є найбільшим ідеалом, який міститься в $I \cap J$. Діаграма включень має наступний вигляд:



Для натурального числа n можна індуктивно визначити n-й степінь I^n ідеалу I:

$$I^1 = I, \quad I^2 = II, \quad \ldots, \quad I^n = II^{n-1},$$

тобто це множина, що складається з усіх скінчених сум елементів вигляду $a_1a_2\ldots a_n$, де $a_i \in I$ для $i = 1, 2, \ldots, n$. Ідеал I називається *нільпотентним*, якщо для деякого $n \in \mathbb{N}$ виконується $I^n = \{0\}$, тобто добуток довільних n елементів ідеала I дорівнює 0. *Радикал ідеала* I кільця R визначається як множина

$$\sqrt{I} = \{a \in R \,|\, a^n \in I \text{ для деякого } n \in \mathbb{N}\}.$$

Приклад 3.6. В $\mathbb{Z}_{240}$ ідеал $(\overline{30})$ є нільпотентним. Ідеал $(\overline{30})$ є радикалом ідеалу $(\overline{60})$.

Задачі

3.1. Нехай R — кільце, $S \subset R$ — підкільце, $I \subset R$ — ідеал. Доведіть, що множина $S + I = \{s + i \,|\, s \in S, i \in I\}$ — підкільце кільця R.

3.2. Наведіть приклад кільця R та елемента $a \in R$, для яких множина $\{ras \,|\, r, s \in R\}$ не є ідеалом.

3.3. Доведіть, що множина всіх оборотних елементів кільця ідеал не утворює.

3.4. Нехай R — кільце, $I \subset R$ — ідеал. Доведіть, що $I = R$ тоді і лише тоді, коли $I \cap R^* \neq \varnothing$.

3.5. Покажіть, що комутативне кільце є полем тоді і лише тоді, коли воно не має нетривіальних ідеалів.

3.6. Наведіть приклади такого кільця R і таких його підкільця та ідеалу, щоб

a) підкільце не було ідеалом;

b) ідеал не був підкільцем.

3.7. Покажіть, що в кільці лишків $\mathbb{Z}_n$:

a) множина $k\mathbb{Z}_n$ є ідеалом для довільного $k \in \mathbb{N}$;

b) для $k \in \mathbb{N}$ має місце рівність: $k\mathbb{Z}_n = d\mathbb{Z}_n$, де $d = (n, k)$ — найбільший спільний дільник чисел n і k;

c) довільний нетривіальний ідеал $\mathbb{Z}_n$ має вигляд $d\mathbb{Z}_n$, де d — дільник n.

3.8. Вкажіть усі ідеали кілець $\mathbb{Z}$ та $\mathbb{Q}$. Чи є $\mathbb{Z}$ кільцем головних ідеалів?

3.9. З'ясуйте, для яких n кільце $\mathbb{Z}_n$ має точно один нетривіальний ідеал? точно два нетривіальних ідеали?

3.10. Чи вірно, що множина усіх дільників нуля комутативного кільця утворює ідеал? Для яких n усі дільники нуля кільця лишків $\mathbb{Z}_n$ утворюють ідеал?

3.11. Опишіть мінімальні, максимальні та нільпотентні ідеали кілець $\mathbb{Z}_{60}$; $\mathbb{Z}$; $\mathbb{Q}$.

3.12. Доведіть, що ідеали $(3, x^2)$ та (p, x^k), де p — просте, $k \in \mathbb{N}$, не є головними ідеалами кільця $\mathbb{Z}[x]$.

3.13. В кільці многочленів $\mathbb{Z}[x]$ перевірте, що множини, які визначені наступними умовами, є ідеалами:

a) множина многочленів, коефіцієнти яких кратні 3;

b) множина многочленів, у яких вільний член та коефіцієнти при x і x^2 дорівнюють 0;

c) множина многочленів, у яких сума коефіцієнтів дорівнює нулю;

d) множина многочленів, у яких вільний член є парним числом.

Вкажіть для них системи твірних. Які з цих ідеалів є головними?

3.14. Покажіть, що множина

$$I = \{a_1 x + \ldots + a_n x^n \mid a_i \in \mathbb{Z}, n \geqslant 0\}$$

є головним ідеалом в кільці $\mathbb{Z}[x]$. Опишіть ідеал I^n.

3.15. Які з наступних множин є ідеалами в кільці $\mathbb{Z}[x]$:

a) множина всіх цілочисельних многочленів степеня n;

b) множина всіх цілочисельних многочленів степеня не більшого за n;

c) множина всіх цілочисельних многочленів степеня не меншого n;

d) множина всіх цілочисельних многочленів, у яких коефіцієнт при x^k дорівнює 0.

3.16. Чи є ідеали (x, y) та (x^2, y^3) кільця $\Bbbk[x, y]$ головними? Чи є кільце $\Bbbk[x, y]$ кільцем головних ідеалів?

3.17. Нехай I — ідеал комутативного кільця R, $I[x]$ — множина многочленів з коефіцієнтами з ідеалу I.

1) Покажіть, що $I[x]$ — ідеал кільця $R[x]$.

2) Покажіть, що для довільного $f(x) \in R[x]$ множина $J = f(x)I[x]$ є ідеалом кільця $R[x]$, причому $J \subset I[x]$.

3.18. Нехай R — нетривіальне кільце, $A \in \mathrm{M}_n(R)$, e_{ij} — матрична одиниця, тобто квадратна матриця, у якої елемент i-го рядка j-го стовпчика дорівнює 1, а решта елементів 0.

a) Покажіть, що $\mathsf{e}_{ij}A$ є матрицею, в якій i-й рядок збігається з j-м рядком матриці A, а решта рядків мають нульові елементи. Сформулюйте подібне правило для $A\mathsf{e}_{ij}$.

b) Нехай $B = \mathsf{e}_{pq} A \mathsf{e}_{rs}$. Покажіть, що $b_{ps} = a_{qr}$ для довільних $1 \leqslant p, q, s, r \leqslant n$, а решта елементів матриці B дорівнюють нулю.

3.19. Нехай R — нетривіальне кільце, L_j — підмножина всіх таких матриць кільця $\mathrm{M}_n(R)$, у яких j-й стовпчик довільний, а решта стовпчиків — нульові. Покажіть, що $L_j = \mathrm{M}_n(R)\,\mathsf{e}_{ij}$ для довільного i, тобто, що L_j є лівим ідеалом кільця $\mathrm{M}_n(R)$.

3.20. Покажіть, що ліві (праві) ідеали кільця матриць $\mathrm{M}_n(\Bbbk)$, $n > 1$, над полем $\Bbbk$ знаходяться у бієктивній відповідності з підпросторами векторного простору $\Bbbk^n$.

3.21. Покажіть, що $\mathrm{M}_n(\Bbbk)$ — просте кільце.

3.22. Нехай R — комутативне нетривіальне кільце, I — ідеал кільця матриць $\mathrm{M}_n(R)$.

a) Покажіть, що множина I_R усіх коефіцієнтів усіх матриць з I утворює ідеал в R.

b) Покажіть, що кожний двосторонній ідеал в $\mathrm{M}_n(R)$ збігається з $\mathrm{M}_n(J)$ для деякого ідеалу J кільця R.

c) Опишіть ідеали кілець $\mathrm{M}_n(\mathbb{Q})$, $\mathrm{M}_n(\mathbb{Z})$.

3.23. Верхня трикутна матриця називається строго верхньою трикутною, якщо елементами головної діагоналі є нулі. Покажіть, що строго верхня трикутна матриця $A \in \mathrm{M}_n(R)$ є нільпотентною. Чи вірно це для строго нижніх трикутних матриць?

3.24. В кільці верхніх трикутних матриць $T_3(\mathbb{R})$ опишіть ліві, праві, двосторонні та нільпотентні ідеали.

3.25. Нехай R_1 і R_2 — кільця, $R = R_1 \times R_2$ — прямий добуток цих кілець. Доведіть, що кожний ідеал кільця R має вигляд $I_1 \times I_2$, де I_1 та I_2 — ідеали кілець R_1 та R_2 відповідно. Знайдіть усі ідеали прямого добутку $R = R_1 \times R_2$ простих кілець R_1 та R_2.

3.26. Визначте, які з наступних множин є ідеалами в прямому добутку $\mathbb{Z} \times \mathbb{Z}$:

a) $\{(a,a) \mid a \in \mathbb{Z}\}$;

b) $\{(2a,2b) \mid a,b \in \mathbb{Z}\}$;

c) $\{(2a,0) \mid a \in \mathbb{Z}\}$;

d) $\{(a,-a) \mid a \in \mathbb{Z}\}$.

3.27. Опишіть максимальні, мінімальні та нільпотентні ідеали кілець $\mathbb{Z}_6 \times \mathbb{Z}_8$; $\mathbb{Z} \times \mathbb{Z}$; $\mathbb{Q} \times \mathbb{Q}$.

3.28. Покажіть, що в кільці $\mathbb{Z}$ мають місце тотожності:

a) $(n\mathbb{Z}) \cap (m\mathbb{Z}) = c\mathbb{Z}$, де $c = \text{НСК}(n,m)$;

b) $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, де $d = \text{НСД}(n,m)$;

c) $(n\mathbb{Z})(m\mathbb{Z}) = nm\mathbb{Z} \subset (n\mathbb{Z}) \cap (m\mathbb{Z})$.

Проілюструйте ці твердження на прикладі $n = 24$, $m = 27$.

3.29. Нехай I, J та K — ідеали кільця R. Покажіть, що $I(J+K) = IJ + IK$ та $(I+J)K = IK + JK$.

3.30. Нехай I — ідеал кільця R і S — підкільце кільця R. Перевірте, що $I \cap S$ є ідеалом в S. Покажіть на прикладі, що не кожен ідеал підкільця S можна зобразити у вигляді $I \cap S$, де I — деякий ідеал кільця R.

3.31. Нехай I та J — ідеали кільця R.

a) Доведіть, що $I + J$ є найменшим ідеалом кільця R, який містить I та J.

b) Доведіть, що $I \cap J$ є найбільшим ідеалом кільця R, який міститься і в I, і в J.

c) Доведіть, що IJ — ідеал кільця R, який міститься в $I \cap J$.

d) Наведіть приклад, коли $IJ \neq I \cap J$.

e) Нехай R — комутативне кільце. Покажіть, що коли $I+J = R$, то $IJ = I \cap J$.

f) Знайдіть необхідну та достатню умову того, щоб об'єднання ідеалів $I \cup J$ було ідеалом. Знайдіть приклад, коли об'єднання ідеалів $I \cup J$ не є ідеалом.

Проілюструйте задачу для випадків, коли а) $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 8\mathbb{Z}$; b) $R = \mathbb{Z}$, $I = 3\mathbb{Z}$, $J = 5\mathbb{Z}$.

3.32. Нехай D — область цілісності, в якій для довільних ідеалів $I, J \in D$ виконується $IJ = I \cap J$. Доведіть, що D — поле.

3.33. Покажіть, що якщо $I_1 \subseteq I_2 \subseteq \ldots$ є ідеалами кільця R, то $I = \bigcup_{n=1}^{\infty} I_n$ також є ідеалом R.

3.34. Нехай a — елемент кільця R. Перевірте, що множина $\{x \in R \,|\, ax = 0\}$ є правим, а множина $\{x \in R \,|\, xa = 0\}$ — лівим ідеалами кільця R (вони називаються, відповідно, *правим* та *лівим анулляторами* елемента $a \in R$). Якщо правий та лівий анулятори збігаються, то говорять про *анулятор* елемента a і позначають цю множину $Ann(a)$.

3.35. Знайдіть праві та ліві анулятори елементів $A_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$ в кільці $\mathrm{M}_2(\mathbb{Z})$.

3.36. Знайдіть анулятор елемента $a = (4, 6)$ кільця $A = \mathbb{Z}_{18} \times \mathbb{Z}_8$. Скільки елементів має $Ann(a)$?

3.37. Доведіть, що у скінченному кільці ідеал є нільпотентним тоді і лише тоді, коли він складається з нільпотентних елементів.

3.38. Покажіть на прикладі $\mathrm{M}_2(\mathbb{Z})$, що в некомутативному кільці множина усіх нільпотентних елементів не обов'язково утворює ідеал.

3.39. Нехай R — комутативне кільце. Перевірте, що множина усіх нільпотентних елементів утворює ідеал. Цей ідеал називається *нільрадикалом* R і позначається $\mathfrak{N}(R)$.

3.40. Знайдіть нільрадикал $\mathfrak{N}$ кільця $\mathbb{Z}_{p^m}$ і перевірте, що $\mathfrak{N}$ є нільпотентним ідеалом в $\mathbb{Z}_{p^m}$.

4 Гомоморфізми та факторкільця

Теоретичні відомості

Гомоморфізмом кілець R та S називається відображення $\varphi : R \to S$, для якого виконується

(i) $\varphi : (R, +) \to (S, +)$ – гомоморфізм адитивних абелевих груп;

(ii) $\varphi : (R\setminus\{0\}, \times) \to (S\setminus\{0\}, \times)$ — гомоморфізм напівгруп;

(iii) $\varphi(1_R) = 1_S$.

Ядром гомоморфізму кілець є ядро гомоморфізму адитивних абелевих груп:

$$\operatorname{Ker}\varphi = \{a \in R \,|\, \varphi(a) = 0\}\,.$$

Образом гомоморфізму кілець називається множина

$$\operatorname{Im}\varphi = \{\varphi(r) \,|\, r \in R\}\,.$$

Очевидно, що коли $\varphi : R \to S$, то $\operatorname{Ker}\varphi \subset R$, $\operatorname{Im}\varphi \subset S$. Більше того, ядро гомоморфізму $\varphi : R \to S$ є ідеалом кільця R, а образ — підкільцем кільця S.

Гомоморфізм кільця в себе називається *ендоморфізмом*. Бієктивний гомоморфізм кілець називається *ізоморфізмом*. Сюр'єктивний гомоморфізм називається *епіморфізмом*. Ін'єктивний гомоморфізм називається *мономорфізмом*.

Приклад 4.1. 1) Для $n \in \mathbb{Z}$ гомоморфізм абелевих груп $\varphi_n : \mathbb{Z} \to \mathbb{Z}$, який заданий $\varphi_n(x) = nx$, не є гомоморфізмом кілець, бо $nxy = \varphi_n(xy) \neq \varphi_n(x)\varphi_n(y) = n^2xy$.

2) Відображення $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x \pmod n$ — гомоморфізм кілець, який називається *редукцією за модулем* n, його ядром є головний ідеал $n\mathbb{Z} = (n)$.

Нехай I — двосторонній ідеал кільця. На факторгрупі R/I операції додавання та множення визначаються за правилами

$$(r+I)+(s+I)=r+s+I,$$
$$(r+I)(s+I)=rs+I.$$

Очевидно, що операції додавання та множення пов'язані дистрибутивними законами. Множина R/I разом з щойно введеними операціями додавання і множення буде кільцем, яке називається *факторкільцем* кільця R за ідеалом I.

Зауваження 4.2. *Поняття факторкільця визначається лише для двосторонніх ідеалів!*

Теореми про гомоморфізми

Теорема 4.3 (Перша теорема про гомоморфізм)**.** *Нехай R та S — кільця.*

a) *Якщо I — ідеал R, то відображення $\varphi_I : R \to R/I$, $r \mapsto r+I$ є епіморфізмом кілець, а $\operatorname{Ker}\varphi_I = I$.*

b) *Якщо $\varphi : R \to S$ є гомоморфізмом кілець, то $\operatorname{Ker}\varphi$ є ідеалом R, $\operatorname{Im}\varphi$ є підкільцем S і*

$$R/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi.$$

Наприклад, для кільця $\mathbb{Z}[x]$ для довільного $n \in \mathbb{N}$ можна задати епіморфізм $\pi_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$, $h(x) \overset{\pi_n}{\longmapsto} h(x) \pmod n$, його ядром буде множина $n\mathbb{Z}[x]$.

Теорема 4.4 (Друга теорема про гомоморфізм)**.** *Нехай A — підкільце кільця R, I — ідеал кільця R. Тоді $A+I$ є підкільцем R, $A \cap I$ є ідеалом A і*

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

Теорема 4.5 (Третя теорема про гомоморфізм)**.** *Нехай I та J — ідеали кільця R і $I \subseteq J$. Тоді J/I є ідеалом кільця R/I і*

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

Теорема 4.6 (Теорема про відповідність)**.** *Нехай I — ідеал R. Відповідність $A \leftrightarrow A/I$ є бієкцією між множиною підкілець A з R, які містять I, і множиною підкілець в R/I. Причому, A є ідеалом кільця R тоді і тільки тоді, коли A/I є ідеалом факторкільця R/I.*

Приклад 4.7. Розглянемо кільце $\mathbb{Z}$ та його ідеали $3\mathbb{Z}$ та $12\mathbb{Z}$. За теоремою 4.6 існує бієкція між ідеалами кільця $\mathbb{Z}$, які містять $12\mathbb{Z}$, та ідеалами факторкільця $\mathbb{Z}/12\mathbb{Z}$, при якій ідеалам $\mathbb{Z}/12\mathbb{Z}$, $3\mathbb{Z}/12\mathbb{Z}$, $12\mathbb{Z}/12\mathbb{Z}$ факторкільця $\mathbb{Z}/12\mathbb{Z}$ ставляться у відповідність ідеали $\mathbb{Z}$, $3\mathbb{Z}$, $12\mathbb{Z}$ кільця $\mathbb{Z}$.

Нехай A — комутативне кільце. Власний ідеал I кільця A називається *простим*, якщо з умови $ab \in I$ для деяких $a, b \in A$ випливає $a \in I$ або $b \in I$. *Спектром кільця* називається множина всіх простих ідеалів.

Лема 4.8. (i) *Ідеал I кільця A є простим тоді і лише тоді, коли A/I є областю цілісності.*

(ii) *Ідеал $\mathfrak{m}$ комутативного кільця A є максимальним ідеалом тоді і лише тоді, коли факторкільце $A/\mathfrak{m}$ є полем. Зокрема, кожний максимальний ідеал є простим.*

(iii) *Нульовий ідеал є максимальним ідеалом кільця A тоді і лише тоді, коли A — поле.*

Приклад 4.9. В кільці $\mathbb{Z}$ кожен простий ідеал є максимальним і породжується простим числом.

Задачі

4.1. Доведіть, що гомоморфний образ комутативного кільця є комутативним кільцем.

4.2. Нехай $\varphi : R \to S$ — ізоморфізм кілець R та S. Доведіть, що якщо $a \in R$ — дільник нуля в кільці R, то $\varphi(a)$ — дільник нуля в кільці S.

4.3. Доведіть, що довільний гомоморфізм кілець зберігає властивість елемента бути оборотним, нільпотентним, ідемпотентом.

4.4. Нехай $\varphi : R \to S$ — гомоморфізм кілець. Доведіть, що прообраз $\varphi^{-1}(J)$ ідеалу J кільця S є ідеалом кільця R.

4.5. Доведіть, що якщо $\varphi : R \to S$ — епіморфізм кілець, I — ідеал R, то $\varphi(I)$ — ідеал S. Чи залишиться це твердженням вірним, якщо φ не епіморфізм?

4.6. Покажіть, що

a) якщо $\varphi : \mathbb{Z} \to \mathbb{Q}$ — довільний гомоморфізм кілець, то $\varphi(n) = n$, $n \in \mathbb{Z}$;

b) єдиним автоморфізмом кільця $\mathbb{Q}$ є тотожний;

c) єдиним автоморфізмом кільця $\mathbb{R}$ є тотожний;

d) автоморфізмами кільця $\mathbb{C}$ є лише тотожне відображення та спряження.

4.7. Покажіть, що епіморфним образом кільця $\mathbb{Z}$ є або $\mathbb{Z}$, або $\mathbb{Z}_n$ для деякого $n \in \mathbb{N}$. Вкажіть ядро гомоморфізму в кожному з випадків.

4.8. Нехай R — кільце дійсних функцій. Доведіть, що відображення $\varphi : R \to \mathbb{R}$, $f(x) \overset{\varphi}{\longmapsto} f(a)$, де $a \in \mathbb{R}$ — фіксований елемент, є гоморфізмом.

4.9. Покажіть, що відображення $\varphi : \mathbb{Q}[x] \to \mathbb{Q}$, яке діє за правилом $p(x) \overset{\varphi}{\longmapsto} p(0)$, є епіморфізмом кілець, ядром якого є $\operatorname{Ker}\varphi = \{p(x) \,|\, a_0 = p(0) = 0\} = \big(x\big)$.

4.10. Нехай F — підполе поля E. Для деякого елемента $u \in E$ визначимо відображення $\varphi_u : F[x] \to E$ за правилом $g(x) \overset{\varphi_u}{\longmapsto} g(u)$. Покажіть, що це відображення є гомоморфізмом кілець, який називається *підстановочним*. Покажіть, що його образ $\operatorname{Im}\varphi_u = F[u] \subset E$ є областю цілісності, а його ядро $\operatorname{Ker}\varphi_u$ є простим ідеалом.

Знайдіть ядро та образ гомоморфізмів $\varphi_{\sqrt{3}} : \mathbb{Q} \to \mathbb{R}$, $\varphi_i : \mathbb{R} \to \mathbb{C}$ та $\varphi_{\sqrt{3}+i} : \mathbb{R} \to \mathbb{C}$.

4.11. Опишіть факторкільце кільця $\mathbb{Z}_{12}$ за ідеалами $I = (\overline{4})$ та $J = (\overline{8})$. Вкажіть усі прості ідеали кільця $\mathbb{Z}_{12}$.

4.12. Опишіть факторкільця

a) кільця $\mathbb{Z}_6 \times \mathbb{Z}_4$ за головним ідеалом $I = \big((4,2)\big)$;

b) кільця $\mathbb{Z}_9 \times \mathbb{Z}_{15}$ за ідеалом $I = \big((3,6)\big)$.

Чи буде який-небудь з цих ідеалів простим?

4.13. Знайдіть усі гомоморфізми кілець з $\mathbb{Z}$ в $\mathbb{Z}_{18}$. Перелічіть усі ідеали кільця $\mathbb{Z}_{18}$ та відповідні факторкільця.

4.14. З'ясуйте, зі скількох елементів складається факторкільце $\mathbb{Z}_3[x]/\big(2x^3 + x^2 + 1\big)$? Чи містить воно дільники 0? Якщо так, то вкажіть їх. З яким з кілець $\mathbb{Z}_3[x]/(x^3 + 2x + 2)$ чи $\mathbb{Z}_3[x]/(x^3 + x + 2)$ воно збігається?

4.15. Позначимо через E факторкільце $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

1) Перевірте, що E складається з чотирьох елементів, а саме: $\overline{0}$, $\overline{1}$, $\overline{x}$, $\overline{x+1}$.

2) Запишіть адитивну таблицю для кільця E і визначте його адитивну групу.

3) Запишіть мультиплікативну таблицю для E і перевірте, що мультиплікативна група E^* ізоморфна циклічній групі третього порядку. Покажіть, що E є полем.

4.16. Покажіть, що кільце $A = \mathbb{Z}_2[x]/\big(x^2 + 1\big)$ з чотирьох елементів не ізоморфне жодному з кілець $\mathbb{Z}_4$ та $\mathbb{Z}_2 \times \mathbb{Z}_2$ і не є полем.

4.17. Доведіть, що факторкільце $\mathbb{Z}_p[x]/(f(x))$ є областю цілісності тоді і лише тоді, коли $f(x)$ незвідний над $\mathbb{Z}_p$.

4.18. З'ясуйте, які з факторкілець є областями цілісності:
a) $\mathbb{Z}_7[x]/(x^2+3)$; b) $\mathbb{Z}_7[x]/(x^2+4)$; c) $\mathbb{Z}_7[x]/(x^2+5)$.

4.19. Нехай $f_1(x) = x^2 + 1$, $f_2(x) = x^3 + x + 1$, $f_3(x) = x^3 + 4x + 4$ — многочлени над полем $\mathbb{Z}_5$. Для якого з многочленів факторкільце $\mathbb{Z}_5[x]/(f_i(x))$, $i = 1, 2, 3$, буде полем.

4.20. Перевірте, що в кільці $\mathbb{Z}[x]$ головні ідеали $I = \big(2\big)$ та $J = (x)$ є простими, але не максимальними.

4.21. Вкажіть усі прості та максимальні ідеали кільця $\mathbb{Z}_{30}$. Доведіть, що факторкільце $\mathbb{Z}_{30}/(5) = \mathbb{Z}_{30}/5\mathbb{Z}_{30}$ ізоморфне кільцю $\mathbb{Z}_5$. Якому кільцю ізоморфне кільце $\mathbb{Z}_{30}/(15)$?

4.22. Доведіть, що

a) $\mathbb{R}[x]/(x-3) \simeq \mathbb{R}$;

b) $\mathbb{R}[x]/(x^2-1) \simeq \mathbb{R}^2$;

c) $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$;

d) $\mathbb{R}[x]/(x^2-x-6) \simeq \mathbb{R}^2$;

e) $\mathbb{Q}[x]/(x^2-2) \simeq \mathbb{Q}[\sqrt{2}]$.

4.23. Доведіть, що $\mathbb{R}[x,y]/(x^2-y) \simeq \mathbb{R}[x]$.

4.24. Доведіть, що кільця $\mathbb{R}[x]/(x^2-2)$ та $\mathbb{R}[x]/(x^2-3)$ ізоморфні. Чи будуть ізоморфними кільця $\mathbb{Q}[x]/(x^2-2)$ та $\mathbb{Q}[x]/(x^2-3)$?

4.25. Покажіть, що $\mathbb{Q}[a+\sqrt{d}] \cong \mathbb{Q}[\sqrt{d}]$, $a, d \in \mathbb{Q}$.

4.26. Якому кільцю — $\mathbb{Q}[\sqrt{3}]$ чи $\mathbb{Q}[\sqrt{5}]$ — ізоморфне кільце $\mathbb{Q}[x]/(x^2-4x-1)$? Вкажіть відповідний ізоморфізм кілець.

4.27. Які з кілець $\mathbb{Z}[x]/(x^2-2x+5)$, $\mathbb{Z}[x]/(x^2+1)$ та $\mathbb{Z}[x]/(x^2+2x+2)$ є ізоморфними?

4.28. Покажіть, що

a) $\mathbb{Z}[x]/\big(3\big) \simeq \mathbb{Z}_3[x]$;

b) $\mathbb{Z}[x]/\big(2,x\big) \simeq \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$;

c) $\mathbb{Z}[x]/(n, f(x)) \cong \mathbb{Z}_n[x]/(f(x))$.

4.29. Покажіть, що ідеал $(2,x)$ є максимальним в $\mathbb{Z}[x]$, а ідеали $(6,x)$, $(2,x^3)$ не є максимальними.

4.30. Нехай $A = \mathbb{Z}_2[x]/\big(x^4+1\big)$, $I = \big(x^2+1\big)A$ — головний ідеал. Покажіть, що $A/I \cong \mathbb{Z}_2[x]/\big(x^2+1\big)$. Чи буде ідеал I простим?

4.31. Нехай $A = \mathbb{Z}_3[x]/\big(x^2+1\big)$. Покажіть, що кільце A є полем з 9 елементів. Переконайтеся, що мультиплікативна група A^* є циклічною, показавши, що $x+1$ є твірним

цієї групи. Вкажіть інші твірні групи A^*. Перевірте, що відображення $\psi : A \longrightarrow A$, $f(x) \overset{\psi}{\longmapsto} f(2x)$, є автоморфізмом кілець.

4.32. Покажіть, що адитивна група $(F, +)$ поля F, яке складається з дев'яти елементів, ізоморфна $\mathbb{Z}_3 \times \mathbb{Z}_3$, тобто порядки всіх ненульових елементів групи $(F, +)$ дорівнює 3. Число 3 називається характеристикою поля F.

4.33. Покажіть, що поле F з дев'яти елементів ізоморфне факторкільцю $\mathbb{Z}_3[x]/\big(f(x)\big)$, де $f(x)$ — незвідний квадратний унітарний многочлен.

4.34. Покажіть, що всі поля, які складаються з 9 елементів, ізоморфні. Поле з 9 елементів позначається $\mathbb{F}_9$.

4.35. Нехай p — непарне просте число, $p \not\equiv 1 \pmod 4$. Перевірте, що кільце $A = \mathbb{Z}_p[x]/\big(x^2+1\big)$ є полем.

4.36. Визначте, якому з кілець $\mathbb{Z}_m$ ізоморфні наступні факторкільця:

a) $\mathbb{Z}[i]/(2+i)$;

b) $\mathbb{Z}[i]/(1-2i)$;

c) $\mathbb{Z}[i]/(3-2i)$;

d) $\mathbb{Z}[i]/(a+bi)$, $a^2+b^2 = p$ — просте ціле.

4.37. Нехай $\mathfrak{N}(R)$ — нільрадикал кільця R. Покажіть, що $\mathfrak{N}\big(R/\mathfrak{N}(R)\big) = 0$.

4.38. Нехай A — абелева група. Покажіть, що множина групових ендоморфізмів $\mathrm{End}(A)$ утворює кільце відносно операцій додавання, визначеного за правилом $(f+g)(a) = f(a) + g(a)$ для $a \in A$, та композиції. Кільце $\mathrm{End}(A)$ називається *кільцем ендоморфізмів* групи A.

4.39. Нехай $A = A_1 \times A_2$ — абелева група. Покажіть, що кільце $\mathrm{End}(A)$ ізоморфне кільцю матриць

$$\left\{ \begin{pmatrix} \mathrm{Hom}(A_1, A_1) & \mathrm{Hom}(A_2, A_1) \\ \mathrm{Hom}(A_1, A_2) & \mathrm{Hom}(A_2, A_2) \end{pmatrix} \right\} \cong \underset{i=1,2;\ j=1,2}{\times} \mathrm{Hom}(A_i, A_j).$$

4.40. Знайдіть усі ендоморфізми кільця $A = \mathbb{Z} \times \mathbb{Z}$.

4.41. Опишіть наступні кільця ендоморфізмів: $\mathrm{End}(\mathbb{Z}_p)$, p – просте число, $\mathrm{End}(\mathbb{Z}_2 \times \mathbb{Z}_2)$, $\mathrm{End}(\mathbb{Z}_{440})$.

5 Теорія подільності. Факторіальні кільця

Теоретичні відомості

Нехай D — область цілісності. Через (a) позначимо головний ідеал, породжений елементом $a \in D$. Наведемо означення понять, пов'язаних з подільністю, у "термінах елементів" і "термінах ідеалів".

Елемент $a \in D$ ділиться на елемент $b \in D$, або b ділить a, (позначається $b \mid a$), якщо

існує такий елемент $q \in D$, що $a = qb$	$(a) \subset (b)$

Елемент b називається *власним* дільником $a \neq 0$, якщо

$b \mid a$ та $b \notin aD^*$, $b \notin D^*$	$\big(a\big) \subsetneq \big(b\big) \subsetneq D$.

Елементи називаються *асоційованими*, якщо

$a \mid b$ та $b \mid a$	$(a) = (b)$

Зауважимо, що одночасне виконання умов $a \mid b$ та $b \mid a$ еквівалентне умові існування оборотного елемента $c \in D^*$, такого, що $a = cb$.

Елемент $a \in D \setminus D^*$ називається *нерозкладним*, якщо

з умови $a = bc$ випливає $b \in D^*$ або $c \in D^*$	ідеал (a) є максимальним серед власних ідеалів D

Інакше елемент називається *розкладним*.

Ненульовий елемент $p \in D \setminus D^*$ називається *простим*, якщо

з того, що $p \mid ab$, випливає $p \mid a$ або $p \mid b$	(p) є простим ідеалом

Лема 5.1. *Нехай D — область цілісності. Якщо $a \in D$ є простим елементом, то він є нерозкладним.*

Приклад 5.2. Нерозкладними елементами кільця $\mathbb{Z}$ є числа $\pm p$, де p — просте число. Незрозкладними елементами кільця $\Bbbk[x]$ є незвідні многочлени.

Зауваження 5.3. *Нерозкладний елемент не обов'язково є простим (див. задачу 5.19).*

Елемент $d \in D$ називається найбільшим спільним дільником елементів $a, b \in D$, якщо

1) $d \mid a$ та $d \mid b$; 2) для кожного $\tilde{d} \in D$, такого, що $\tilde{d} \mid a$ і $\tilde{d} \mid b$, маємо $\tilde{d} \mid d$	$(a) + (b) = (d)$

Найбільший спільний дільник d елементів a і b позначається НСД(a, b) або (a, b). Якщо НСД(a, b) існує, то він визначений не однозначно, а з точністю до асоційованості. Якщо $(a, b) \in D^*$, то елементи a і b називаються *взаємно простими*. В цьому випадку пишуть НСД$(a, b) = 1$.

Елемент $c \in D$ називається найменшим спільним кратним елементів $a, b \in D$, якщо

1) $a \mid c$ та $b \mid c$; 2) для кожного $\tilde{c} \in D$, такого, що $a \mid \tilde{c}$ і $b \mid \tilde{c}$, маємо $c \mid \tilde{c}$	$(a) \cap (b) = (c)$

Найменше спільне кратне елементів $a, b \in D$ визначається з точністю до асоційованості і позначається НСК(a, b).

Послідовно визначаються найбільший спільний дільник і найменше спільне кратне довільної сукупності елементів з D.

Лема 5.4. *В кільці головних ідеалів для довільних двох елементів існують найбільший спільний дільник та найменше спільне кратне.*

Означення 5.5. *Кажуть, що необоротний елемент $a \neq 0$ області цілісності D однозначно розкладається на нерозкладні множники, якщо*
1) його можна подати як добуток нерозкладних елементів;
2) з рівностей

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

де $p_1, p_2, \dots, p_n$, $q_1, q_2, \dots, q_m$ — нерозкладні елементи D, випливає, що $n = m$ та існує така підстановка $\sigma \in \mathcal{S}_n$, що p_i та $q_{\sigma(i)}$, $i = 1, 2, \dots, n$, є асоційованими.

Якщо a — нерозкладний елемент, то вважаємо, що він має однозначний розклад на нерозкладні множники, який складається лише з одного множника.

Приклад 5.6. В кільці $\mathbb{Z}[i]$ елемент 2 можна розкласти на нерозкладні множники так: $2 = (1+i)(1-i) = -i(1+i)^2$. Але елементи $(1+i)$ та $(1-i)$ є асоційованими, бо $1 - i = -i(1+i)$, тому розклад 2 у добуток нерозкладних множників визначений однозначно з точністю до асоційованості.

Означення 5.7. *Область цілісності називається* факторіальним *кільцем (або кільцем з однозначним розкладом), якщо у ньому кожний ненульовий необоротний елемент має однозначний розклад на нерозкладні множники.*

Приклад 5.8. Кільце $\mathbb{Z}$ цілих чисел, кільце $\mathbb{Z}[i]$ цілих гаусових чисел та кільце многочленів $\Bbbk[x_1, \dots, x_n]$ від n змінних над полем $\Bbbk$ є факторіальними. Кільце $\mathbb{Z}[i\sqrt{3}]$ не є факторіальним, бо $4 = 2 \cdot 2 = (1 - i\sqrt{3})(1 + i\sqrt{3})$, а елементи $2, (1 \pm i\sqrt{3})$ не асоційовані.

Теорема 5.9. *Область цілісності D є факторіальним кільцем тоді й лише тоді, коли для довільного необоротного елемента $a \in D$ такого, що $a \mid bc$, маємо $a \mid b$ або $a \mid c$, $b, c \in D$.*

Лема 5.10. *Нехай R — факторіальне кільце. Тоді для довільних $a, b \in R$ існує НСД(a, b) та НСК(a, b).*

Приклад 5.11. У кільці $R = \mathbb{Z}[i\sqrt{5}]$ не існує НСД$(6, 2 + 2i\sqrt{5})$, отже, кільце $R = \mathbb{Z}[i\sqrt{5}]$ не є факторіальним.

Задачі

5.1. Покажіть, що відношення асоційованості є відношенням еквівалентності на множині ненульових елементів області цілісності.

5.2. Доведіть, що в області цілісності кожний простий елемент є нерозкладним.

5.3. Доведіть, що у факторіальному кільці множини нерозкладних і простих елементів збігаються.

5.4. Доведіть, що гомоморфний образ головного ідеалу є головним ідеалом.

5.5. Чи буде гомоморфний образ кільця головних ідеалів кільцем головних ідеалом?

5.6. Доведіть, що кільце головних ідеалів є факторіальним.

5.7. Доведіть, що кільце многочленів $R[x]$ над факторіальним кільцем R теж факторіальне.

5.8. Нехай $\mathbb{Z}[\sqrt{d}]$ — квадратичне кільце, де $d \in \mathbb{Z}$ — ціле число, вільне від квадратів, $d \neq 1$.

a) Покажіть, що в кільці $\mathbb{Z}[\sqrt{d}]$ існують лише два автоморфізми $\varphi, \overline{\varphi}\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}]$:

$$\varphi(a + b\sqrt{d}) = a + b\sqrt{d} \quad \text{та} \quad \overline{\varphi}(a + b\sqrt{d}) = a - b\sqrt{d}.$$

b) Покажіть, що функція $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}_0$, задана як

$$N(a + b\sqrt{d}) = |\varphi(a + b\sqrt{d})\,\overline{\varphi}(a + b\sqrt{d})| = |a^2 - b^2 d|,$$

має властивості:

(i) $N(x) = 0 \Leftrightarrow x = 0$;

(ii) $N(xy) = N(x)N(y)$ для довільних $x, y \in \mathbb{Z}[\sqrt{d}]$.

Іншими словами, ця функція визначає на $\mathbb{Z}[\sqrt{d}]$ *мультиплікативну норму.*

c) Покажіть, що x — оборотний $\Leftrightarrow N(x) = 1$.

d) Покажіть, що для $u, v \in \mathbb{Z}[\sqrt{d}]$ з того, що u ділить v, випливає, що $N(u)$ ділить $N(v)$.

e) Покажіть, що коли $N(x)$ — просте число, то x — нерозкладний в $\mathbb{Z}[\sqrt{d}]$. Перевірте, що 7 — нерозкладний в $\mathbb{Z}[\sqrt{6}]$, хоча $N(7) = 7^2$.

5.9. В кільці $\mathbb{Z}[i]$ знайдіть НСД(a, b) чисел

a) $a = 7 + i$, $b = 1 + 13i$;

b) $a = 5 - 5i$, $b = 14 + 8i$;

c) $a = 9 + 7i$, $b = 11 + 3i$

шляхом розкладу на прості множники.

5.10. В кільці $\mathbb{Z}[i]$ знайдіть

a) всі числа $a + bi$ з нормою $N(a + bi) = a^2 + b^2 = 5$;

b) всі числа $a + bi \in \mathbb{Z}[i]$, для яких $(5) = (a+bi)$;

c) всі числа $a + bi \in \mathbb{Z}[i]$, для яких $(5) \subsetneqq (a+bi) \subsetneqq \mathbb{Z}[i]$.

d) НСД$(5, 3 - i)$ та НСК$(5, 3 - i)$.

5.11. В кільці $\mathbb{Z}[i]$ цілих гаусових чисел

a) знайдіть суму та перетин ідеалів $\big(5\big)$ та $\big(3 + i\big)$;

b) знайдіть твірний елемент ідеалу $\big(5, 4 + 3i\big)$ шляхом знаходження найбільшого спільного дільника;

c) покажіть, що $\big(85, 1 + 13i\big) = \big(7 + 6i\big)$.

5.12. В кільці $\mathbb{Z}[i]$ розкладіть на прості множники наступні елементи:
a) $5 + i$; b) $5 + 5i$; c) $7 + i$; d) $7 + 3i$; e) $14 - 2i$.

5.13. Покажіть, що

a) елементи 2 та $1 + i\sqrt{3}$ не є асоційованими в кільці $\mathbb{Z}[i\sqrt{3}]$;

b) ідеал $I = (1 + i\sqrt{3})$ не є простим в $\mathbb{Z}[i\sqrt{3}]$;

c) ідеал I не максимальним в $\mathbb{Z}[i\sqrt{3}]$, бо $I \subsetneqq (2, 1 + i\sqrt{3}) \subsetneqq \mathbb{Z}[i\sqrt{3}]$.

5.14. Визначте, чи існує в кільці $\mathbb{Z}[i\sqrt{3}]$ найбільший спільний дільник елементів 4 і $2 - 2i\sqrt{3}$.

5.15. Покажіть, що

a) в кільці $R = \mathbb{Z}[i\sqrt{5}]$ не існує НСД$(6, 2 + 2i\sqrt{5})$;

b) в кільці $\mathbb{Z}[x^2, x^3]$ не існує НСД(x^5, x^6).

5.16. Знайдіть найбільший спільний дільник та найменше спільне кратне елементів $5 + \sqrt{3}$ та $3 - \sqrt{3}$ кільця $\mathbb{Z}[\sqrt{3}]$.

5.17. Обчисліть суму, добуток та перетин головних ідеалів $I = \left(5 + \sqrt{3}\right)$ та $J = \left(3 - \sqrt{3}\right)$ кільця $\mathbb{Z}[\sqrt{3}]$.

5.18. Перевірте, що кільце $\mathbb{Z}[i\sqrt{6}]$ не факторіальне.

5.19. Доведіть, що в кільці $\mathbb{Z}[i\sqrt{5}]$ елементи 2, 3, $2 \pm i\sqrt{5}$ є нерозкладними, але не є простими. Чи буде кільце $\mathbb{Z}[i\sqrt{5}]$ факторіальним?

5.20. Покажіть, що кільце $\mathbb{Z}[2i]$ не факторіальне.

5.21. Покажіть, що кільце $\mathbb{R}(\cos x, \sin x)$ не факторіальне.

5.22. Покажіть, що в кільці $\mathbb{Z}[i\sqrt{5}]$

a) ідеали $I_1 = \left(2, 1 + i\sqrt{5}\right)$, $I_2 = \left(3, 2 + i\sqrt{5}\right)$, $I_3 = \left(3, 2 - i\sqrt{5}\right)$ прості;

b) ідеали $(2, 1+i\sqrt{5})$, $(3, 1+i\sqrt{5})$, $(3, 2+i\sqrt{5})$ не є головними;

c) має місце однозначний розклад для ідеалів

$$(6) = (2)(3) = (1 + i\sqrt{5})(1 - i\sqrt{5}) = I_1^2 I_2 I_3.$$

5.23. Перевірте справедливість рівностей

$$\left(3, 1 + i\sqrt{5}\right)\left(3, 1 - i\sqrt{5}\right) = \left(3\right) \text{ та } \left(2, 1 + i\sqrt{5}\right)^2 = \left(2\right)$$

в кільці $\mathbb{Z}[i\sqrt{5}]$. Отже, добуток ідеалів, які не є головними, може бути головним ідеалом.

5.24. Покажіть, що якщо $I_1 \subseteq I_2 \subseteq \ldots$ є зростаючим ланцюгом ідеалів в R, то $\bigcup_{n=1}^{\infty} I_n$ також є ідеалом в R. Враховуючи це, доведіть, що довільне кільце головних ідеалів є факторіальним.

6 Евклідові кільця

Теоретичні відомості

Означення 6.1. *Область цілісності R називається евклідовим кільцем, якщо існує функція*

$$N : R \setminus \{0\} \to \mathbb{N},$$

яка задовольняє умови:

a) *для довільних $a, b \in R$ виконується: $N(ab) \geqslant N(a)$;*

b) *для довільних $a, b \in R$, $b \neq 0$, існують елементи $q, r \in R$, для яких*

$$a = bq + r, \ \textit{причому } r = 0 \textit{ або } N(r) < N(b).$$

Умова 2) означає можливість "ділення з остачею" на ненульові елементи кільця. Елементи q і r з останньої рівності називаються відповідно неповною часткою і остачею від ділення a на b. Зауважимо, що однозначної визначеності елементів q і r не вимагається.

Функція N з означення евклідового кільця називається *евклідовою нормою* на R.

До евклідових кілець належать, зокрема, наступні:

- кільце $\mathbb{Z}$ цілих чисел, евклідовою нормою є модуль цілого числа;
- кільце $\Bbbk[x]$ многочленів над полем $\Bbbk$, евклідовою нормою є степінь многочлена;

- кільце цілих гаусових чисел $\mathbb{Z}[i]$, евклідова норма для ненульового елемента $a+bi \in \mathbb{Z}[i]$ задається за правилом $N(a+bi) = a^2 + b^2$.

Лема 6.2. *Кожне евклідове кільце є факторіальним.*

З цього твердження випливає, що для довільних ненульових елементів a і b евклідового кільця існує їхній найбільший спільний дільник, який можна знайти, використовуючи *алгоритм Евкліда*, який полягає у наступному.

Алгоритм Евкліда. Нехай a та b — ненульові елементи евклідового кільця A. Не обмежуючи загальності, можемо вважати, що $N(a) \geqslant N(b)$. Якщо a ділиться на b, то $\text{НСД}(a,b) = b$. Якщо це не так, то розділимо з остачею a на b, потім b на одержану остачу, після цього першу остачу на другу остачу і т.д. Оскільки норми остач спадають, то врешті-решт відбудеться ділення без остачі. В результаті одержимо ланцюжок рівностей:

$$\begin{aligned}
a &= q_1 b + r_1,\\
b &= q_2 r_1 + r_2,\\
r_1 &= q_3 r_2 + r_3,\\
&\cdots\cdots\cdots\cdots\\
r_{n-2} &= q_n r_{n-1} + r_n,\\
r_{n-1} &= q_{n+1} r_n,
\end{aligned}$$

де $N(b) > N(r_1) > N(r_2) > \ldots > N(r_n)$. Остання ненульова остача r_n і є найбільшим спільним дільником елементів a і b.

Рухаючись цим ланцюжком знизу догори, отримаємо послідовно

$$\begin{aligned}
r_1 &= au_1 + bv_1,\\
r_2 &= au_2 + bv_2,\\
r_3 &= au_3 + bv_3,\\
&\cdots\cdots\cdots\cdots\\
\text{НСД}(a,b) &= r_n = au_n + bv_n,
\end{aligned}$$

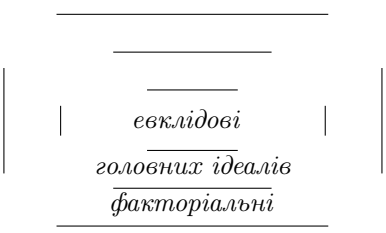
де u_i, v_i $(i = 1, \ldots, n)$ — деякі елементи кільця.

Лема 6.3. *Нехай A — евклідове кільце, $a, b \in A$, $d = (a, b)$. Тоді існують такі елементи $u, v \in A$, що $d = au + bv$.*

Теорема 6.4. *1. Кожне евклідове кільце є кільцем головних ідеалів.*

2. Кожне кільце головних ідеалів є факторіальним.

Схематично ці включення можна зобразити так:



Зауважимо, що твердження, обернені до тверджень теореми 6.4, є, взагалі кажучи, невірними. Наприклад, кільце $\mathbb{Z}[x]$ є факторіальним кільцем, але не є кільцем головних ідеалів. Кільце $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ є кільцем головних ідеалів, але не є евклідовим кільцем. Зауважимо, що доведення цього факту є доволі складним.

Задачі

6.1. Знайдіть $d = \text{НСД}(a, b)$ і зобразіть d у вигляді лінійної комбінації $ax + by$:

a) $a = 20$, $b = 13$;

b) $a = 69$, $b = 372$;

c) $a = 2120$, $b = 3312$;

d) $a = 5 + 5i$, $b = 13 + 3i$;

e) $a = 3 - 4i$, $b = 12 + 5i$;

f) $a = 25 - 6i$, $b = 12 - 7i$.

6.2. Нехай R — евклідове кільце, I — ідеал і d — ненульовий елемент з I, норма якого найменша. Покажіть, що $I = (d)$.

6.3. В кільці $\mathbb{Z}$ знайдіть головні ідеали

a) $I = (2210, 1131)$;

b) $I = (3333, 4444)$;

c) $I = (222, 225)$;

d) $I = (41, 45)$;

e) $I = (3142, 2718)$;

f) $I = (30, 42, 70)$;

g) $I = (1707, 1777, 1811)$.

6.4. За допомогою алгоритму Евкліда, обчисліть обернені (якщо існують):

a) 13^{-1} в кільці $\mathbb{Z}_{20}$;

b) 69^{-1} в кільці $\mathbb{Z}_{89}$;

c) 77^{-1} в кільці $\mathbb{Z}_{444}$;

d) 17^{-1} в кільці $\mathbb{Z}_{85}$;

e) 34^{-1} в кільці $\mathbb{Z}_{505}$;

f) 71^{-1} в кільці $\mathbb{Z}_{428}$.

6.5. За допомогою алгоритма Евкліда розв'яжіть конгруентності:

a) $17x \equiv 18 \pmod{43}$;

b) $19x \equiv 14 \pmod{51}$;

c) $13x \equiv 29 \pmod{61}$.

6.6. За допомогою алгоритма Евкліда, знайдіть обернений

a) до елемента $x^4 + 3x^2 + 4x + 1 + I$ в кільці $\mathbb{Z}_5[x]/I$, де $I = \big(x^5 + 3x^3 + 2x^2 + 1\big)$;

b) до елемента $x^2 + 4x + 1 + I$ в кільці $\mathbb{Z}_5[x]/I$, де $I = \big(x^3 + x + 1\big)$;

c) до елемента $2x^2 + 4x + 3 + I$ в кільці $\mathbb{Z}_5[x]/I$, де $I = \big(x^3 + x + 1\big)$;

d) до елемента $x^3 + x^2 + 2x + 1 + I$ в кільці $\mathbb{Z}_7[x]/I$, де $I = \big(x^4 + x^3 + 2x^2 + 5x + 3\big)$.

6.7. Нехай R — область цілісності, $a, b \in R$ ненульові.

1) Припустимо, що a і b мають найменше спільне кратне. Доведіть, що НСК(a, b) є твірним для однозначно визначеного найбільшого головного ідеалу, що міститься в $(a) \cap (b)$.

2) Доведіть, що якщо елементи a і b мають найменше спільне кратне, то вони мають найбільший спільний дільник.

6.8. Доведіть, що в евклідовому кільці

a) якщо $b|a$, $c|a$ і $(b, c) = 1$, то $bc|a$;

b) якщо $c|ab$ і $(b, c) = 1$, то $c|a$.

6.9. Покажіть, що в евклідовому кільці найменше спільне кратне довільних елементів a і b цього кільця існує, визначене однозначно з точністю до асоційованості і дорівнює НСК$(a, b) = \frac{ab}{\text{НСД}(a,b)}$.

6.10. Доведіть, що функція $N : \mathbb{Z}[i\sqrt{2}] \to \mathbb{N}$, визначена правилом $N(a + bi\sqrt{2}) = a^2 + 2b^2$, є евклідовою нормою.

6.11. Доведіть, що функція $N : \mathbb{Z}[\sqrt{3}] \to \mathbb{N}$, визначена правилом $N(a + b\sqrt{3}) = |a^2 - 3b^2|$, є евклідовою нормою.

6.12. Довести, що кільце $\mathbb{Z}[i\sqrt{3}]$ не є евклідовим.

6.13. Покажіть, що множина чисел вигляду $\frac{1}{2}(x + iy\sqrt{3})$, де x, y — цілі числа однакової парності, є евклідовим кільцем.

6.14. Нехай d — вільне від квадратів ціле число, таке, що $d \equiv 1 \pmod 4$. Покладемо $\omega = \frac{1+\sqrt{d}}{2}$ і визначимо множину

$$\mathcal{O}_{\sqrt{d}} = \{a + b\omega \,|\, a, b \in \mathbb{Z}\}.$$

Перевірте, що для довільного $z = a+b\omega \in \mathcal{O}_{\sqrt{d}}$ норма $N(z) = (a + b\omega)(a - b\omega)$ є цілим числом.

6.15. Нехай A — евклідове кільце. Доведіть, що для елементів $a, b \in A$ рівність $N(ab) = N(a)$ можлива лише тоді, коли b — оборотний.

6.16. В кільці $\mathbb{Z}[i]$ цілих гаусових чисел

1) з'ясуйте, чи будуть прості цілі числа 2, 3 та 5 простими цілими гаусовими числами.

2) доведіть, що коли $N(a + bi) = p$, де p — просте, то $a + bi$ — просте ціле гаусове. Знайдіть усі прості елементи $\mathbb{Z}[i]$ з нормами 17, 29, 43.

6.17. Нехай $p \in \mathbb{N}$ — непарне просте. Доведіть, що $p = (a + bi)(a - bi)$, де $a + bi$ — просте ціле гаусове, тоді і лише тоді, коли $p \equiv 1 \pmod 4$.

6.18. Нехай $p \in \mathbb{N}$ — непарне просте. Покажіть, що коли $p \equiv 3 \pmod 4$, то p — нерозкладне в $\mathbb{Z}[i]$, а якщо $p \equiv 1 \pmod 4$, то p є розкладним в $\mathbb{Z}[i]$.

6.19. Доведіть, що простими елементами в $\mathbb{Z}[i]$ є лише

a) $a + bi \in \mathbb{Z}[i]$, для яких норма $N(a + bi)$ є простим числом;

b) такі прості числа $p \in \mathbb{Z}$, що $p \equiv 3 \pmod 4$.

Знайдіть всі прості цілі гаусові числа, норма яких не перевищує 20.

6.20. Доведіть, що кільце раціональних чисел вигляду $2^{-n}m$ ($m \in \mathbb{Z}$, $n \in \mathbb{N}$) є евклідовим.

6.21. Діофантовим рівнянням першого степеня в кільці $\mathbb{Z}[x, y]$ називається рівняння вигляду $ax + by = c$, $a, b, c \in \mathbb{Z}$.

1) Покажіть, що рівняння $ax + by = c$ має розв'язок в цілих числах тоді і лише тоді, коли $c \in (a, b)$.

2) Якщо відомий один розв'язок x_0, y_0 рівняння $ax + by = c$, то довільний інший розв'язок має вигляд:

$$x = x_0 + t\frac{b}{(a,b)}, \quad y = y_0 - t\frac{a}{(a,b)}, \quad t \in \mathbb{Z}.$$

6.22. Знайдіть усі цілі розв'язки рівнянь:

a) $2x + 4y = 5$;

b) $17x + 29y = 31$;

c) $16x + 28y = 35$;

d) $16x + 28y = 36$;

e) $15x + 25y = 55$;

f) $19x + 23y = 79$.

6.23. Перевірте, що фактор-кільце $\mathbb{Z}[i]/I$ є скінченним для довільного ненульового ідеалу I в $\mathbb{Z}[i]$.

6.24. Нехай α — корінь многочлена $x^3 - x^2 + 3 \in \mathbb{Q}[x]$. За допомогою алгоритму Евкліда, подайте у вигляді многочлена від α степеня не більшого за 2 числа

$$\frac{1}{\alpha}, \quad \frac{1}{\alpha + 1}, \quad \frac{1}{\alpha^2 + 1}, \quad \frac{\alpha + 5}{\alpha^2 + 3}.$$

7 Китайська теорема про остачі

Теоретичні відомості

У цьому розділі всі кільця комутативні.

Лема 7.1. *Відображення $\varphi\colon A \to A_1 \times \ldots \times A_k$ з кільця A в прямий добуток кілець $A_1 \times \ldots \times A_k$ є гомоморфізмом тоді і лише тоді, коли індуковане відображення $\varphi_i : A \to A_i$ на кожну з компонент A_i є гомоморфізмом.*

За означенням, два елемента $a_1, a_2 \in A$ є взаємно простими, якщо рівняння $a_1x_1 + a_2x_2 = 1$ розв'язне в A, або якщо $a_1A + a_2A = (a_1, a_2)A = A$. Припустимо, що $a_1a_2 = 0$ і $a_1b_1 + a_2b_2 = 1$. У цьому випадку елементи $e_1 = a_1b_1$ та $e_2 = a_2b_2$ утворюють повну систему взаємно ортогональних ідемпотентів і $A \simeq e_1A \times e_2A$.

Ідеали I та J кільця A називаються *комаксимальними*, якщо $I + J = A$. Головні ідеали $\big(a\big)$ та $\big(b\big)$ кільця цілих чисел є комаксимальними тоді і лише тоді, коли числа $(a, b) = 1$.

Теорема 7.2 (Китайська теорема про остачі для кілець)**.** *Нехай I_1, I_2 – ідеали в A. Відображення*

$$A \to A/I_1 \times A/I_2, \quad a \mapsto (a + I_1, a + I_2)$$

є гомоморфізмом кілець з ядром $I_1 \cap I_2$. Якщо ідеали I_1 та I_2 є комаксимальними, то це відображення сюр'єктивне і $I_1 \cap I_2 = I_1I_2$, а отже,

$$A/(I_1I_2) = A/(I_1 \cap I_2) \cong A/I_1 \times A/I_2.$$

Наслідок 7.3. *Нехай I_1, I_2 — це комаксимальні ідеали кільця A. Тоді для довільних елементів $a_1 \in A/I_1$, $a_2 \in A/I_2$ система конгруентностей*

$$\begin{aligned} x &\equiv a_1 \pmod{I_1} \\ x &\equiv a_2 \pmod{I_2} \end{aligned}$$

має єдиний розв'язок в кільці A/I_1I_2.

Якщо e_1, e_2 — це система взаємно ортогональних ідемпотентів, яка відповідає цьому розкладу, то розв'язок записується у вигляді $a_1e_1 + a_2e_2 \pmod{I_1I_2}$.

Зауважимо, що теорему 7.2 можна узагальнити на випадок скінченної кількості попарно комаксимальних ідеалів I_1, I_2, …, I_k, при цьому

$$A/(I_1 I_2 \dots I_k) = A/(I_1 \cap I_2 \cap \dots \cap I_k) \cong A/I_1 \times A/I_2 \times \dots \times A/I_k.$$

Розглянемо випадок кільця $\mathbb{Z}$ цілих чисел. Якщо m та n — взаємно прості цілі числа, то існує ізоморфізм

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

Згідно з алгоритмом Евкліда, існують $u, v \in \mathbb{Z}$, такі, що $1 = um + vn$, а саме: $u = m^{-1} \pmod n$, $v = n^{-1} \pmod m$. Тоді $e_1 = vn$ та $e_2 = um$ — це взаємно ортогональні ідемпотенти, і для довільного $(a_1, a_2) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ елемент $a = \varphi^{-1}((a_1, a_2))$ визначається за формулою:

$$a = a_1 e_1 + a_2 e_2 \pmod{mn}.$$

Наслідок 7.4. *Нехай n — натуральне число, $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — канонічний розклад n за степенями різних простих чисел. Тоді наступні кільця ізоморфні:*

$$\mathbb{Z}/n\mathbb{Z} \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}).$$

Крім того,

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \dots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^*.$$

Зокрема, з цього твердження випливає формула для обчислення функції Ейлера:

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \dots \cdot \varphi(p_k^{\alpha_k}).$$

Наслідок 7.5 (Китайська теорема про остачі)**.** *Якщо натуральні числа $n_1, n_2, \dots, n_k$ — попарно взаємно прості, то система конгруентностей*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\dots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

має єдиний розв'язок за модулем натурального числа $n = n_1 n_2 \dots n_k$.

Алгоритм Гауса. Розв'язок цієї системи конгруентностей можна знайти наступним чином:

$$x = \sum_{i=1}^{k} a_i N_i M_i,$$

де $N_i = n/n_i$, а $M_i = N_i^{-1} \pmod{n_i}$.

Множина елементів $\{e_i\}_{i=1}^{r} = \{e_i \mid i = 1, \dots, r\}$ комутативного кільця R називається *системою взаємно ортогональних ідемпотентів*, якщо $e_i^2 = e_i$, $e_i e_j = 0$ для довільних $1 \leqslant i, j \leqslant r$, $i \neq j$. Система ідемоптентів $\{e_i\}_{i=1}^{r}$ називається *повною*, якщо $1 = \sum\limits_{i=1}^{r} e_i$.

Задачі

7.1. Опишіть усі розв'язки таких конгруентностей в $\mathbb{Z}$:

a) $3x \equiv 4 \pmod{7}$;

b) $3x \equiv 4 \pmod{12}$;

c) $9x \equiv 12 \pmod{21}$;

7.2. Опишіть всі розв'язки наступних конгруентностей:

a) $27x \equiv 25 \pmod{256}$;

b) $27x \equiv 72 \pmod{900}$;

c) $103x \equiv 612 \pmod{676}$.

7.3. Нехай R — комутативне кільце, e — ідемпотент R. Покажіть, що

a) $\{e, 1 - e\}$ є повною системою взаємно ортогональних ідемпотентів;

b) множини Re та $R(1-e)$ є двосторонніми ідеалами R і $R \simeq Re \times R(1-e)$;

c) Re та $R(1-e)$ є кільцями з одиницями e та $1-e$ відповідно.

7.4. Нехай $\left\{e_k\right\}_{k=1}^{r}$ — це повна система взаємно ортогональних ідемпотентів комутативного кільця R.

1) Покажіть, що ідеал e_iR є кільцем з одиницею e_i.

2) Покажіть, що кільце R ізоморфне прямому добутку кілець $e_1R \times \ldots \times e_rR$, зокрема, $e_iR \cap e_jR = 0$ для довільних $1 \leqslant i, j \leqslant r$, $i \neq j$.

7.5. Покажіть, що кільце R ізоморфне прямій сумі кілець $e_1R \times \ldots \times e_kR$ тоді і лише тоді, коли $\left\{e_i\right\}_{i=1}^{k}$ є повною системою взаємно ортогональних ідемпотентів.

7.6. Покажіть, що

a) ідеал $5\mathbb{Z}_{30}$ кільця $\mathbb{Z}_{30}$ є кільцем з одиницею $e = \overline{25}$, ізоморфним $\mathbb{Z}_6$, а $\mathbb{Z}_{30}/5\mathbb{Z}_{30} \cong \mathbb{Z}_5$;

b) ідеал $5\mathbb{Z}_{25}$ кільця $\mathbb{Z}_{25}$ є кільцем без одиниці з 5 елементів з нульовим множенням (добуток довільних двох елементів дорівнює нулю);

c) елементи $\overline{6}$ і $\overline{25}$ кільця $\mathbb{Z}_{30}$ утворюють повну систему взаємно ортогональних ідемпотентів, яка визначає розклад в пряму суму $\mathbb{Z}_{30} \cong 5\mathbb{Z}_{30} \times 6\mathbb{Z}_{30} \cong \mathbb{Z}_6 \times \mathbb{Z}_5$, та знайдіть ортогональні проекції елемента $\overline{22}$ на підкільця $5\mathbb{Z}_{30}$ і $6\mathbb{Z}_{30}$;

d) елементи $\overline{6}$, $\overline{10}$, $\overline{15}$ кільця $\mathbb{Z}_{30}$ утворюють повну систему взаємно ортогональних ідемпотентів, яка визначає розклад в пряму суму $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

7.7. Нехай $n, m > 1$ — взаємно прості натуральні числа. Доведіть, що в кільці $\mathbb{Z}_{nm}$ існує повна система взаємно ортогональних ідемпотентів e, f, яка визначає розклад в пряму суму $\mathbb{Z}_{nm} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$.

7.8. Вкажіть, який найбільший можливий порядок елементів в групі $\mathbb{Z}_{252}^*$.

7.9. Розв'яжіть систему конгруентностей в $\mathbb{Z}$:

$$\begin{aligned} x &\equiv 2 \,(\mathrm{mod}\ 6) \\ x &\equiv 7 \,(\mathrm{mod}\ 11). \end{aligned}$$

7.10. Нехай $\varphi : \mathbb{Z}_{45} \longrightarrow \mathbb{Z}_5 \times \mathbb{Z}_9$ — ізоморфізм кілець.

a) Знайдіть $\varphi(37)$.

b) Знайдіть відповідну систему $\{e_1, e_2\}$ взаємно ортогональних ідемпотентів кільця $\mathbb{Z}_{45}$ та обчисліть $\varphi^{-1}(2,6)$, $\varphi^{-1}(3,1)$.

7.11. Нехай $n_1, n_2, \ldots, n_k$ — попарно взаємно прості цілі числа, $n = n_1 n_2 \ldots n_k$, $N_i = n/n_i$ для $i = 1, \ldots, k$.

1) Покажіть, що числа N_i та n_i є взаємно простими для всіх $i = 1, \ldots, k$.

2) Покладемо $t_i = N_i^{-1} \,(\mathrm{mod}\ n_i)$, $e_i = t_i N_i$ для всіх $i = 1, \ldots, k$. Перевірте, що $e_1, e_2, \ldots, e_k$ є повною системою взаємно ортогональних ідемпотентів. Покажіть, що розв'язок x системи конгруентностей

$$x \equiv a_1 \,(\mathrm{mod}\ n_1); \quad x \equiv a_2 \,(\mathrm{mod}\ n_2); \quad \ldots; \quad x \equiv a_k \,(\mathrm{mod}\ n_k)$$

визначається рівністю: $x = a_1 e_1 + a_2 e_2 + \ldots + a_k e_k \,(\mathrm{mod}\ n)$.

7.12. Нехай $\varphi : \mathbb{Z}_{84} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_7$ — ізоморфізм кілець.

a) Знайдіть $\varphi(55)$;

b) Знайдіть відповідну систему e_1, e_2, e_3 взаємно ортогональних ідемпотентів кільця $\mathbb{Z}_{84}$ та обчисліть $\varphi^{-1}(1,3,6)$ та $\varphi^{-1}(1,3,1)$.

7.13. Розв'яжіть системи конгруентностей в $\mathbb{Z}$:

$$\begin{array}{lll} & x \equiv 1 \,(\mathrm{mod}\ 2), & x \equiv 2 \,(\mathrm{mod}\ 5), \quad x \equiv 5 \,(\mathrm{mod}\ 9), \\ \text{a)} & x \equiv 1 \,(\mathrm{mod}\ 3), & \text{b)}\ x \equiv 3 \,(\mathrm{mod}\ 7), \quad \text{c)}\ x \equiv 7 \,(\mathrm{mod}\ 8), \\ & x \equiv 9 \,(\mathrm{mod}\ 11); & x \equiv 5 \,(\mathrm{mod}\ 11); \quad x \equiv 3 \,(\mathrm{mod}\ 7); \end{array}$$

$x \equiv 1 \pmod 3$, $4x \equiv 1 \pmod 7$, $3x \equiv 4 \pmod 5$,
d) $5x \equiv 5 \pmod 6$, e) $4x \equiv 3 \pmod 9$, f) $7x \equiv 1 \pmod 8$,
$2x \equiv 10 \pmod 7$; $4x \equiv 9 \pmod{11}$; $10x \equiv 9 \pmod{13}$.

7.14. Знайдіть найменше трицифрове натуральне число N, таке, що $N-3$ ділиться на 5 і 11, а $N-5$ ділиться на 8.

7.15. Знайдіть таке найбільше трицифрове натуральне число, яке при діленні на 5 дає в остачі 7, при діленні на 7 дає в остачі 4, а при діленні на 11 дає в остачі 3.

7.16. Нехай N — це тризначне додатне число, яке при діленні на 9 і 10 дає в остачі 7, а при діленні на 11 дає в остачі 3. Про це число також відомо, що воно є дільником деякого 6-значного натурального числа M, яке при діленні на 9, 10 і 11 дає в остачі 8, 7 і 1 відповідно. Знайдіть частку від ділення M на N.

8 Мала теорема Ферма. Теорема Ейлера

Функція Ейлера $\varphi(n)$ визначена на множині цілих додатних чисел і дорівнює кількості чисел ряду $0, 1, \ldots, n-1$, взаємно простих з n.

Властивості функції Ейлера:

a) $\varphi(p) = p - 1$, де p — просте;

b) $\varphi(p^k) = p^k - p^{k-1}$, де p — просте, $k \in \mathbb{N}$;

c) $\varphi(pq) = \varphi(p)\varphi(q)$, де p та q — взаємно прості числа (мультиплікативність функції Ейлера);

d) нехай $n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ — канонічний розклад натурального числа n, тоді

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \ldots p_s^{k_s-1} (p_1 - 1)(p_2 - 1) \ldots (p_s - 1).$$

Мала теорема Ферма. *Нехай p — просте число, a — ціле число, $(a,p)=1$. Тоді*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Теорема Ейлера. *Нехай a та m — цілі числа, $(a,m)=1$. Тоді*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Задачі

8.1. За допомогою малої теореми Ферма обчисліть: a) $\overline{15}^{-1}$ в $\mathbb{Z}_{17}^*$; b) $\overline{17}^{-1}$ в $\mathbb{Z}_{31}^*$; c) $\overline{13}^{-1}$ в $\mathbb{Z}_{43}^*$; d) $\overline{23}^{-1}$ в $\mathbb{Z}_{47}^*$.

8.2. За допомогою теореми Ейлера розв'яжіть наступні конгруентності:

a) $8x \equiv 13 \pmod{17}$;

b) $9x \equiv 4 \pmod{13}$;

c) $13x \equiv 15 \pmod{36}$;

d) $16x \equiv 17 \pmod{25}$;

e) $27x \equiv 11 \pmod{32}$;

f) $20x \equiv 13 \pmod{33}$.

8.3. З'ясуйте, на яку цифру закінчується число 3^{123}.

8.4. Знайдіть останні дві цифри числа 7^{1242}.

8.5. Знайдіть остачі від ділення
a) 2^{125} на 143; b) 7^{1441} на 1001; c) 9^{999} на 99.

8.6. Покажіть, що $12! = -1 \pmod{13}$.

8.7. Доведіть *теорему Вільсона*: число p — просте тоді і лише тоді, коли $(p-1)! \equiv -1 \pmod{p}$.

8.8. Доведіть, що $100!30! + 1$ ділиться на 131.

8.9. Нехай a та b — взаємно прості числа. Доведіть, що $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$.

8.10. Знайдіть остачу від ділення 444^{235} на 1001.

8.11. Знайдіть остачу від ділення 271^{314} на 1001.

9 Символи Лежандра та Якобі

Теоретичні відомості

Нехай a — ціле, $p > 2$ — просте число. Нехай $\mathbb{F}_p$ — скінченне поле з p елементів. Квадрати елементів в полі $\mathbb{F}_p$ називаються *квадратичними лишками* за модулем p, всі інші ненульові елементи поля $\mathbb{F}_p$ називаються *квадратичними нелишками* за модулем p. В кожному полі з p елементів є рівно $\frac{p-1}{2}$ квадратичних лишків та $\frac{p-1}{2}$ квадратичних нелишків.

Приклад 9.1. Квадратами в полі $\mathbb{F}_{11}$ є елементи $1 = 1^2$, $4 = 2^2$, $9 = 3^2$, $5 = 4^2$, $3 = 5^2$.

Символ Лежандра $\left(\frac{a}{p}\right)$ визначається рівністю:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{якщо } p \mid a\ ; \\ 1, & \text{якщо } a \text{ є квадратичним лишком за модулем } p; \\ -1, & \text{якщо } a \text{ є квадратичним нелишком за модулем } p. \end{cases}$$

Лема 9.2 (Критерій Ейлера)**.** *Якщо a не ділиться на просте число p, то має місце співвідношення:*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Теорема 9.3. *Символ Лежандра має властивості:*

1) *якщо* $a \equiv b \pmod{p}$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

3) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

4) $\left(\frac{1}{p}\right) = 1$; $\quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;

5) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{якщо } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{якщо } p \equiv \pm 3 \pmod{8}. \end{cases}$

Теорема 9.4 (Квадратичний закон взаємності)**.** *Нехай p та q — два непарних простих числа. Тоді*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Нехай a — ціле число, n — довільне непарне ціле число. Нехай $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ — розклад n на прості множники. *Символ Якобі* визначається як добуток символів Лежандра за всіма простими дільниками числа n:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{k_1} \left(\frac{a}{p_2}\right)^{k_2} \dots \left(\frac{a}{p_s}\right)^{k_s}.$$

Зауваження 9.5. *Якщо n — складене число, то рівність $\left(\frac{a}{n}\right) = 1$ не означає, що a є квадратом за модулем n. Наприклад, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, проте не існує такого цілого числа, квадрат якого був би конгруентним 2 за модулем 15.*

Для символа Якобі мають місце аналоги теорем 9.3 та 9.4.

Задачі

9.1. Нехай $p \in \mathbb{N}$ — просте, $a \in \mathbb{N}$ і $p \nmid a$. Доведіть, що відображення $f : \mathbb{Z}_p^* \to (\{1, -1\}, \cdot)$, $a \mapsto \left(\frac{a}{p}\right)$, є гомоморфізмом мультиплікативних абелевих груп. Знайдіть ядро цього гомоморфізму.

9.2. Покажіть, що у полі $\mathbb{F}_p$, p — непарне просте число, є рівно $(p-1)/2$ квадратичних лишків та $(p-1)/2$ квадратичних нелишків.

9.3. Складіть таблицю всіх квадратичних лишків та нелишків за модулем p для $p = 3, 5, 7, 13$.

9.4. З'ясуйте, чи мають конгруеності розв'язок. Якщо так, то вкажіть його.

а) $x^2 \equiv 5 \pmod{29}$;

b) $x^2 \equiv 3 \pmod{29}$;

c) $x^2 \equiv 3 \pmod{31}$;

d) $x^2 \equiv 5 \pmod{31}$.

9.5. Обчисліть символи Лежандра:
a) $\left(\frac{13}{31}\right)$; b) $\left(\frac{31}{131}\right)$; c) $\left(\frac{131}{1031}\right)$; d) $\left(\frac{137}{1037}\right)$; e) $\left(\frac{787}{1787}\right)$; f)$\left(\frac{1039}{2039}\right)$.

9.6. З'ясувати, чи буде просте число 7411 квадратичним лишком за модулем простого числа 9283. Зробіть це, скориставшись a) квадратичним законом взаємності лише для символу Лежандра; b) для символу Якобі.

9.7. Обчислити символ Лежандра $\left(\frac{1801}{8191}\right)$ скориставшись квадратичним законом взаємності a) лише для символу Лежандра; b) для символу Якобі.

9.8. Доведіть, що квадратичний лишок ніколи не може бути твірним елементом групи $\mathbb{F}_p^*$.

9.9. Доведіть, що $p-1$ є квадратичним лишком за модулем p тоді і лише тоді, коли $p = 4k+1$, $k \in \mathbb{N}$.

9.10. Доведіть, що коли $p = 4k+1$, $k \in \mathbb{N}$, то a і $-a$ одночасно є або квадратичним лишками, або квадратичними нелишками за модулем p.

9.11. Доведіть, що існує нескінченно багато простих чисел вигляду $4k+1$.

9.12. Нехай p — просте число, $p \neq 2, 3$. Доведіть, що число -3 буде квадратичним лишком за модулем p тоді і лише тоді, коли $p \equiv 1 \pmod{3}$.

9.13. Доведіть, що коли $2^n - 1$ є простим, то n — просте число. Прості числа вигляду $2^p - 1$, де p — просте, називаються *простими числами Мерсенна*. Випишіть перші п'ять простих чисел Мерсенна.

9.14. Покажіть, що число 3 є квадратичним нелишком за модулем простого числа Мерсенна, більшого за 3.

9.15. Доведіть, що коли $2^n + 1$ є простим, то n є степенем двійки. Прості числа вигляду $2^{2^p} + 1$, де p — просте, нази-

ваються *простими числами Ферма*. Випишіть перші п'ять простих чисел Ферма.

9.16. Нехай p — просте число Ферма. Покажіть, що будь-який квадратичний нелишок є твірним в $\mathbb{F}_p^*$.

9.17. Доведіть, що коли просте число $p > 2$ є дільником числа $b^n + 1$, то або p ділить $b^d + 1$ для деякого власного дільника d числа n, для якого $\frac{n}{d}$ — непарне число, або $p \equiv 1 \pmod{2n}$.

9.18. Припустимо, що просте число p є дільником числа $2^{2^k} + 1$, де $k > 1$.

a) Покажіть, що $p \equiv 1 \pmod{2^{k+1}}$.

b) Покажіть, що $p \equiv 1 \pmod{2^{k+2}}$.

c) Використовуючи пункт b, покажіть, що $2^{16} + 1$ є простим числом.

10 Локалізація

Нехай A — комутативне кільце. Підмножина S кільця A називається *мультиплікативною*, якщо $1 \in S$ і для довільних $s_1, s_2 \in S$ виконується, що $s_1 s_2 \in S$.

Лема 10.1. *Нехай A — кільце, $S \in A$ — мультиплікативна множина. На множині $\left\{ \frac{a}{s} \;\middle|\; a \in A,\, s \in S \right\}$ визначимо відношення $\sim$ за правилом*

$$\frac{a_1}{s_1} \sim \frac{a_2}{s_2} \iff \exists\, s \in S \,:\, s(a_1 s_2 - s_1 a_2) = 0.$$

Відношення $\sim$ є відношенням еквівалентності.

Множина класів еквівалентності

$$S^{-1}A = \left\{ \frac{a}{s} \,\middle|\, a \in A,\, s \in S \right\} / \sim$$

називається *локалізацією* кільця A за мультиплікативною множиною S.

Зауваження 10.2. *Якщо A — область цілісності, то еквівалентність $\sim$ можна переписати так:*

$$\frac{a_1}{s_1} \sim \frac{a_2}{s_2} \iff a_1 s_2 - s_1 a_2 = 0.$$

Надалі ми використовуватимемо запис $\dfrac{a_1}{s_1} = \dfrac{a_2}{s_2}$ замість $\dfrac{a_1}{s_1} \sim \dfrac{a_2}{s_2}$.

Лема 10.3. *Операції додавання та множення*

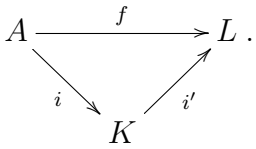
$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}; \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$$

визначають на $S^{-1}A$ структуру кільця.

Лема 10.4. *Нехай A — область цілісності, тоді множина $S = A \setminus \{0\}$ є мультиплікативною, а локалізація $K = S^{-1}A$ є полем.*

Означення 10.5. *Поле $K = S^{-1}A$ називається полем часток області цілісності A.*

Лема 10.6. *Нехай $f : A \hookrightarrow L$ — вкладення області цілісності A в поле L, $i : A \to K$ — вкладення області цілісності A в своє поле часток K, а $\overset{i}{\longmapsto} \frac{a}{1}$. Тоді існує єдиний такий гомоморфізм кілець $i' : K \to L$, що наступна діаграма комутативна:*



Гомоморфізм $i' : K \to L$ називається продовженням вкладення f на поле часток. Іншими словами, якщо поле містить область цілісності A, то воно містить і його поле часток K.

Якщо P — простий ідеал, то $S = A \setminus P$ — мультиплікативна множина, оскільки

$$xy \in A \setminus P \iff x \in A \setminus P \text{ та } y \in A \setminus P.$$

У цьому випадку $S^{-1}A$ називається локалізацією за простим ідеалом P.

Нехай $\Bbbk$ — поле. Ідеал $\mathfrak{M} \subset A$ є максимальним тоді і лише тоді, коли $\mathfrak{M} = \operatorname{Ker} f$ для деякого епіморфізму $f : A \to \Bbbk$.

Лема 10.7. *Ідеал $P \subset A$ є простим тоді і лише тоді, коли існує поле $\Bbbk$ і такий гомоморфізм (не обов'язково епіморфізм!) $f\colon A \to \Bbbk$, що $P = \operatorname{Ker} f$.*

Задачі

10.1. Доведіть, що відношення $\sim$, визначене в лемі 10.1, є відношенням еквівалентності.

10.2. Доведіть, що множина $S^{-1}A$ є кільцем відносно операцій

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}; \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

10.3. Доведіть, що $S^{-1}A = \{0\}$ тоді і лише тоді, коли S містить 0.

10.4. Доведіть, що гомоморфізм кілець

$$f\colon A \to S^{-1}A : \quad a \xmapsto{f} \frac{a}{1}$$

є ін'єктивним тоді і лише тоді, коли S не містить дільників нуля.

10.5. Нехай $\Bbbk$ — поле. Покажіть, що його поле часток ізоморфне $\Bbbk$.

10.6. Опишіть поле часток кільця $\mathbb{Z}$.

10.7. Опишіть поле часток кільця $\mathbb{Z}[i]$ цілих гаусових чисел.

10.8. Опишіть поле часток кільця $A = \Bbbk[x_1, \ldots, x_n]$ кільце многочленів від n змінних над полем $\Bbbk$.

10.9. Нехай $n > 1$, $m > 1$ — взаємно прості цілі числа, Покажіть, що в кільці $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ множина $S = \{(1,0),(1,1)\}$ є мультиплікативною, а відповідною локалізацією є $S^{-1}(\mathbb{Z}/nm\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Відповіді і вказівки

Розділ 1

1.2. *Вказ.* За дистрибутивними законами $(a+b)(1+1) = a(1+1)+b(1+1) = a+a+b+b$, $(a+b)(1+1) = (a+b)1+(a+b)1 = a+b+a+b$.

1.3. Кільце цілих чисел є кільцем без власних підкілець.

1.4. Нехай r — твірний адитивної групи кільця R, $s, t \in R$. Тоді існують такі $a, b \in \mathbb{Z}$, що $s = ar$, $t = br$. Тоді $st = (ar)(br) = (ab)r^2 = (ba)r^2 = (br)(ar) = ts$.

1.5. $R_1 \cup R_2$ — підкільце тоді і лише тоді, коли $R_1 \subset R_2$ або $R_2 \subset R_1$.

1.6. a, c та e.

1.7. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_7$.

1.8. a, c, d.

1.9. $\mathbb{Z}_n$ є полем тоді і лише тоді, коли n — просте.

1.13. Ні, бо тоді $(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2})^2 \in \mathbb{Z}[\eta]$, але $i \notin \mathbb{Z}[\eta]$.

1.15. a Ні, бо множина не замкнена відносно множення. b Ні. c Ні, бо множина не замкнена відносно додавання. d Ні. e, f Так. g Ні. Наприклад, для $A = \left(\begin{smallmatrix} 1 & 0 \\ \sqrt{2} & 1 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ $\det A = 1$, $\det B = 1$, $\det(A+B) = 4 - \sqrt{2}$.

1.16. Ізоморфізм можна задати, наприклад, таким чином: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a-b & b \\ 0 & b+d \end{smallmatrix}\right)$.

1.17. *Вказ.* Розгляньте автоморфізм $\alpha : \mathrm{M}_n(\Bbbk) \to M_n(\Bbbk)$, заданий за правилом $\alpha(A) = [\alpha]^{-1}A[\alpha]$, де $A \in \mathrm{M}_n(\Bbbk)$, $[\alpha]$ — матриця, в якої на побічній діагоналі стоять одиниці, решта елементів нулі.

1.21. a,b, d, e, g так; c, f ні.

1.27. b) $\{\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \mid a, b, c \in \mathbb{Z}_p\}$.

1.29. d $q^{-1} = \dfrac{\overline{q}}{|q|}$; e $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$; f Усі $q \in \mathbb{H}$ вигляду: $q = bi + cj + dk$, $|q| = 1$.

1.33. *Вказ.* Нехай $y \in C(a)$, $y \neq 0$, тоді $y^{-1}a = y^{-1}ayy^{-1} = y^{-1}yay^{-1} = ay^{-1}$, звідки $y^{-1} \in C(a)$.

1.34. *Достатність.* Для довільних $a, b \in R$ виконується $(a+b)^2 - (a+b) = a^2 - a + b^2 - b + ab + ba \in Z(R)$, звідси випливає $ab + ba \in Z(R)$. Отже, $a(ab+ba) = (ab+ba)a$, $a^2b + aba = aba + ba^2$, тому $a^2 \in Z(R)$. Таким чином, $a = a^2 - (a^2 - a) \in Z(R)$.

1.35. *Вказ.* Одиницею є $\cos x$. Оберненим до $a\cos x + b\sin x$ є $\frac{a}{(a^2+b^2)}\cos x - \frac{b}{(a^2+b^2)}\sin x$.

Розділ 2

2.1. Дільників нуля немає. $\mathbb{Z}^* = \{1, -1\}$.

2.2. Дільників нуля немає. $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

2.3. Дільників нуля немає. $\mathbb{Z}[\omega]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$.

2.4. Нехай $b \in D$, $b \neq 0$ — ідемпотент. Тоді $b^2 = b$ і для довільного $a \in D$ маємо наступні імплікації: $b^2a = ba \implies b(ba - a) = 0 \implies ba - a = 0$.

2.5. *Вказ.* Якщо $(a, n) = d > 1$, то, поклавши $b = n/d$, матимемо $ab = 0 \pmod{n}$.

2.6. Дільники нуля: $\overline{2}, \overline{3}, \overline{4}, \overline{6}, \overline{8}, \overline{9}, \overline{10}, \overline{12}$. Дільники одиниці: $\overline{1}, \overline{5}, \overline{7}, \overline{11}$. Нільпотентні: $\overline{0}$, $\overline{6}$. Ідемпотенти: $\overline{0}$, $\overline{1}$, $\overline{4}$, $\overline{9}$.

2.7. $\overline{7}^{-1} = \overline{13}$; $\overline{8}^{-1} = \overline{2}$; $\overline{11}^{-1} = \overline{11}$.

2.8. ± 1

2.9. Це елементи вигляду $(2+\sqrt{3})^n$, $n \in \mathbb{N}$.

2.10. Це елементи вигляду $(5+2\sqrt{6})^n$, $n \in \mathbb{N}$.

2.11. a Дільники нуля: матриці (a_{ij}), у яких $a_{ii} = 0$ хоча б для одного i; оборотні: матриці (a_{ij}), у яких $a_{ii} \neq 0$ для всіх i; нільпотентні: матриці (a_{ij}), у яких $a_{ii} = 0$ для всіх i. b Дільники нуля: такі функції $f : X \to \Bbbk$, що $f \not\equiv 0$ і $f(a) = 0$ для певного $a \in X$; оборотні: скрізь ненульові функції; нільпотентні: $f = 0$. c Дільники нуля: $A \in \mathrm{M}_2(\mathbb{R})$, у яких $\det A = 0$; оборотні: $A \in \mathrm{M}_2(\mathbb{R})$, у яких $\det A \neq 0$; нільпотентні: $A \in \mathrm{M}_2(\mathbb{R})$, у яких $\det A = \operatorname{tr} A = 0$. d Дільники нуля: усі, крім X та $\varnothing$, оборотні: X, нільпотентні: $\varnothing$.

2.12. $\{\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \mid a \in 2\mathbb{Z}_{2^k}, b \in \mathbb{Z}_2\}$

2.13. Дільником нуля є матриця A. Дільниками одиниці в кільці $\mathrm{M}_n(\mathbb{Q})$ є всі невироджені матриці, дільниками нуля

— всі вироджені.

2.14. c, d, f.

2.15. b, c, e.

2.17. a Дільники одиниці: $(\overline{a}, \overline{b})$, де $\overline{a}, \overline{b} \in \mathbb{Z}_p \setminus \{\overline{0}\}$; дільники нуля: $(\overline{a}, \overline{0}), (\overline{0}, \overline{a})$, де $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$; нільпотентні: $(\overline{0}, \overline{0})$. b Дільники одиниці: $(\overline{1}, \overline{1})$, $(\overline{1}, \overline{3})$, $(\overline{3}, \overline{1})$, $(\overline{3}, \overline{3})$; дільники нуля: всі, крім $(\overline{1}, \overline{1})$, $(\overline{1}, \overline{3})$, $(\overline{3}, \overline{1})$, $(\overline{3}, \overline{3})$ та $(\overline{0}, \overline{0})$; нільпотентні: $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{2})$, $(\overline{2}, \overline{0})$, $(\overline{2}, \overline{2})$. c Дільники одиниці: $(\overline{1}, \overline{1})$, $(\overline{1}, 5)$, $(\overline{3}, \overline{1})$, $(\overline{3}, 5)$; дільники нуля: всі, крім $(\overline{1}, \overline{1})$, $(\overline{1}, 5)$, $(\overline{3}, \overline{1})$, $(\overline{3}, 5)$ та $(\overline{0}, \overline{0})$; нільпотентні: $(\overline{0}, \overline{0})$, $(\overline{2}, \overline{0})$.

2.18. Дільники одиниці: $(a_1, a_2, \ldots, a_n)$, де всі $a_i \in \Bbbk \setminus \{0\}$. Дільники нуля: $(a_1, a_2, \ldots, a_n)$, де хоча б один елемент $a_i = 0$. Прямий добуток полів не є полем.

2.23. a Так. *Вказ.* Нехай $ab \cdot c = c \cdot ab = 1$, тоді $a \cdot bc = 1$. З іншого боку, покладемо $d = bc \cdot a$. Домножимо обидві частини на a зліва: $a \cdot d = a \cdot bc \cdot a$. Звідси $a \cdot bc \cdot a = 1 \cdot a = a$. Оскільки R без дільників нуля, то з рівності $a(d-1) = 0$ випливає, що $d = 1$, тобто $bc \cdot a = 1$. Отже, a — одиниця кільця R. *Зауваження.* В загальному випадку це твердження не є вірним!

b Так. *Вказ.* Якщо $a^n c = ca^n = 1$, то $a^{n-1}c$ є правим оберненим, а ca^{n-1} — лівим оберненим до a.

2.24. Для c скористайтеся розкладом $1 + x^r = (1 + x)(1 - x + \ldots + x^{r-1})$.

2.25. $1 + bxa$, де x — обернений до $1 - ab$. *Вказ.* Нехай x — обернений до $1-ab$, тоді $x(1-ab) = 1$, звідси $bx(1-ab)a = ba$. Отже, $1 = 1 - ba + ba = (1 - ba) + bx(1 - ab)a = (1 - ba) + bx(a - aba) = (1 - ba) + bxa(1 - ba) = (1 - ba)(1 + bxa)$.

2.26. $C_3 = \langle g \mid g^3 = 1 \rangle$, $\Lambda = \mathbb{C}[C_3]$. Дільники нуля: ненульові елементи вигляду $f(g) \cdot (g - \xi)$, де $f(g) = ag + b$, $a, b \in \mathbb{C}$, і $\xi^3 = 1$. Дільники одиниці: ненульові елементи вигляду $(g - \lambda)$ та $(g - \lambda)(g - \mu)$, де $\lambda, \mu \in \mathbb{C}$, $\lambda^3 \neq 1$, $\mu^3 \neq 1$. *Вказ.* Елемент вигляду $G = g^2 + ug + v \in \Lambda$, $u, v \in \mathbb{C}$, розкладається в добуток елементів вигляду $g - w$, $w \in \mathbb{C}$. При цьому, якщо G є дільником нуля, то принаймні один із співмножників також

є дільником нуля, якщо G є дільником одиниці, то кожен із співмножників є дільником 1.

2.27. *Вказ.* $(a+b+c)^2 - 2(a+b+c) - 3 = (a+b+c-3)(a+b+c+1) = 0$, $(1+a+b-3c)(1+a+b+c) = 0$.

2.28. с *Вказ.* Нехай n — порядок елемента g. Скористайтеся тим, що $(1-g)(1+g+g^2+\ldots+g^{n-1}) = 1-g^n$.

2.29. Якщо $x \in G$ – елемент порядку $n > 1$, то $(1-x)(1+\ldots+x^{n-1}) = 0$, отже $1-x$ – дільник нуля в $\Bbbk[G]$, причому $1+\ldots+x^{n-1} \neq 0$ в $\Bbbk[G]$, бо елементи $1, \ldots, x^{n-1}$ попарно різні.

2.30. Це відома нерозв'язана гіпотеза Капланського.

2.31. 1 *Вказ.* Припустимо, що a — лівий дільник нуля. Тоді для деякого $y \in R$, $y \neq 0$, $ay = 0$, тобто $\mathtt{l}_a(y) = \mathtt{l}_a(0)$. 2 Оскільки $\mathtt{l}_a$ — сюр'єкція, то у кожного елемента кільця R має бути прообраз, отже, для деякого $x \in R$ $ax = 1$.
Твердження 1 та 2 є вірними для відображення $\mathtt{r}_a$, якщо в них замінити слово "лівий" на "правий".

2.33. а *Вказ.* Оскільки довільний $a \in R \setminus \{0\}$ не є дільником нуля, то $\mathtt{l}_a$ — ін'єкція (див. задачу 2.31), а отже, і бієкція, бо кільце скінченне. Тому $ax = 1$ для деякого $x \in R$. З рівностей $a = (ax)a = a(xa)$ випливає $a(1-xa) = 0$, враховуючи, що $a \neq 0$ і R без дільників нуля, то $xa = 1$. b Нехай a — оборотний справа, тоді існує такий $x \in R$, що $ax = 1$, тобто a — лівий дільник одиниці, а тому не є правим дільником нуля. Отже, відображення $\mathtt{r}_a \colon x \mapsto xa$ — бієкція (див. задачі 2.31 і 2.32). Оскільки кільце скінченне, то для деякого $y \in R$ $ya = 1$. Отже, a — оборотний. с Нехай a є лівим, але не правим дільником нуля. Тоді всі елементи $x_1a, x_2a, \ldots x_na$, $x_i \in R$, — попарно різні, та для деякого i: $x_ia = 1$, тобто a — правий дільник одиниці, що неможливо.

2.34. Нехай $a \in R \setminus \{0\}$. Якщо відображення $\mathtt{l}_a : x \mapsto ax$ не є бієкцією, то існують $x, y \in R$, $x \neq y$ такі, що $ax = ay$, отже, $a(x-y) = 0$ і a — дільник 0. Якщо $\mathtt{l}_a$ — бієкція, то існує $b \in R$ такий, що $ab = 1$, а отже, a — дільник 1.

2.35. Припустимо, що $xy = 1$, тоді $x = (xy)x = x(yx)$,

звідки одержимо $x(1-yx)=0$ і $yx=1$.

2.36. Див. вказівки до задачі 2.33.

2.37. a Для довільного $a \in R$ циклічна напівгрупа $\langle a\rangle$ містить ідемпотент, оскільки $a^{m+n}=a^m$ для деякого $n \geqslant 1$.
b Нехай $a \in R$, $a \neq 0$. Тоді для деякого $n>0$ маємо $a^{2n}=a^n$ або $a^n(a^n-1)=0$. Якщо $a^k=0$ для деякого k, то a – дільник нуля; інакше якщо $a^n-1=0$, то a – дільник 1; інакше існує таке $k \geqslant 1$, що $a^k(a^n-1)=0$, але $a^{k-1}(a^n-1) \neq 0$, знову одержимо, що a – дільник 0.
c Нехай в R $uv=1$. Тоді $u=(uv)u=u(vu)$, звідки одержимо $u(1-vu)=0$.

Розділ 3

3.2. $R=M_2(\mathbb{R})$, $A=\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$. Матриці вигляду RAS, де $R,S \in M_2(\mathbb{R})$ є виродженими. Але сума матриць з цієї множини може буди невиродженою, наприклад $\left(\begin{smallmatrix}0&0\\1&1\end{smallmatrix}\right)\cdot A\cdot\left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)+\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right)\cdot A\cdot\left(\begin{smallmatrix}1&0\\-1&-1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$.

3.3. Нехай $a \in R^*$. Тоді $a+(-a)=0 \notin R^*$.

3.4. Якщо $I=R$, то $1 \in I \cap R^*$. Навпаки, якщо $a \in I \cap R^*$, $a \neq 0$, то $1=aa^{-1} \in I \cap R^*$, отже $I=R$.

3.5. В полі кожний елемент має обернений, тому кожний ненульовий ідеал збігається з усім полем. Нехай A — комутативне кільце, яке не має нетривіальних ідеалів. Тоді для довільного $a \in A$, $a \neq 0$, головний ідеал aA ненульовий, тому $aA=A$ і існує $b \in A$ такий, що $ab=1$.

3.7. b) якщо $d=(n,k)$, то $d \mid k$, отже $k\mathbb{Z}_n \subset d\mathbb{Z}_n$; а оскільки $d=un+vk$ для деяких $u,v \in \mathbb{Z}$, то $d\mathbb{Z}_n \subset k\mathbb{Z}_n$.
c) оберемо таке найменше $d \in \mathbb{N}$, що $\overline{d} \in J$, тоді довільний $x \in J$ ділиться на d без остачі, отже, $J=d\mathbb{Z}_n$.

3.8. Ідеали в $\mathbb{Z}$ мають вигляд $k\mathbb{Z}$, $k \in \mathbb{N}_0$. В $\mathbb{Q}$ нетривіальних ідеалів немає.

3.9. Один: при $n=p^2$, p — просте. Два: при $n=p^3$, $n=pq$, p,q — різні прості числа.

3.10. Ні. Наприклад, в кільці $\mathbb{Z}_6$ елементи $\overline{3}$ та $\overline{4}$ є дільниками нуля, але $\overline{3}+\overline{4}=\overline{1}$. Для $n=p^k$, де p — просте число, дільники нуля утворюють ідеал $p\mathbb{Z}_n$.

3.11. Оскільки $2, 3, 5$ – це усі прості дільники 60, то максимальними ідеалами є $2\mathbb{Z}_{60}$, $3\mathbb{Z}_{60}$, $5\mathbb{Z}_{60}$, а мінімальними – $12\mathbb{Z}_{60}$, $20\mathbb{Z}_{60}$, $30\mathbb{Z}_{60}$. Нільпотентні: $\{0\}$, $30\mathbb{Z}_{60}$. В кільці $\mathbb{Z}$ максимальні ідеали — це $p\mathbb{Z}$, p — просте; мінімальних та нільпотентних немає. В $\mathbb{Q}$ немає нетривіальних ідеалів.

3.12. Припустимо, що ідеал $\big(3, x^2\big)$ є головним, тоді $\big(3, x^2\big) = \big(h(x)\big)$ для деякого $h(x) \in \mathbb{Z}[x]$. Оскільки $3 \in \big(3, x^2\big)$, то існує $p(x) \in \mathbb{Z}[x]$ такий, що $p(x) \cdot h(x) = 3$, але тоді $\deg h(x) = 0$. Оскільки $x^2 \in \big(3, x^2\big)$, то існує $q(x) \in \mathbb{Z}[x]$ такий, що $q(x) \cdot h(x) = x^2$, звідки одержимо, що $h(x) = \pm 1$. Отже, $\big(h(x)\big) = \mathbb{Z}[x] = \big(3, x^2\big)$, але це не так, бо, наприклад, $x \notin \big(3, x^2\big)$.

3.13. a $3\mathbb{Z}[x]$; b $x^3\mathbb{Z}[x]$; c $(x-1)\mathbb{Z}[x]$; d $(2, x)\mathbb{Z}[x]$. Головними ідеалам є a, b, c.

3.14. $I = x\mathbb{Z}[x]$, $I^n = x^n\mathbb{Z}[x]$.

3.15. c, d при $k = 0$.

3.16. Ні. *Вказ.* Доведення аналогічне до доведення з задачі 3.12.

3.17. 2 Нехай $h(x) = \sum_{i=0}^{n} a_i x^i \in I[x]$, $f(x) = \sum_{j=0}^{m} b_j x^j \in R[x]$, тоді $f(x)h(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j\right) x^k$, і $a_i b_j \in I$ для $i = 0, \ldots, n$, $j = 0, \ldots m$.

3.18. а) j-й стовпчик матриці $A\mathsf{e}_{ij}$ збігається з i-м стовпчиком матриці A, а решта стовпчиків мають нульові коефіцієнти.

3.19. Для довільної $A \in \mathrm{M}_n(R)$ в матриці $A\mathsf{e}_{ij}$ усі стовпчики, крім j-го, дорівнюють нулю, а j-й дорівнює i-му стовпчику матриці A, звідки одержимо $\mathrm{M}_n(R)\,\mathsf{e}_{ij} \subset L_j$. Навпаки, $L_j \subset L_i\,\mathsf{e}_{ij} \subset \mathrm{M}_n(R)\,\mathsf{e}_{ij}$.

3.20. *Вказ.* Нехай I — лівий ідеал кільця $\mathrm{M}_n(\Bbbk)$. Позначимо через V множину всіх векторів-рядків усіх матриць з ідеалу I. Для довільної матриці $A \in I$ k-й рядок матриці $\left(\sum_{j=1}^{n} b_j \mathsf{e}_{kj}\right) A$ є лінійною комбінацією рядків матриці A з коефіцієнтами $b_1, \ldots, b_n \in \Bbbk$, а решта рядків є нульовими.

3.21. Нехай I — ідеал кільця $\mathrm{M}_n(\Bbbk)$. Якщо в деякій ма-

триці $B = (b_{ij}) \in I$ елемент $b_{ij} \neq 0$, то існує така матриця $A \in I$, що $a_{ij} = 1$, тоді $\mathsf{e}_{ki}A\mathsf{e}_{jl} = \mathsf{e}_{kl} \in I$ для довільних $k, l = 1, \ldots, n$, отже, $I = \mathrm{M}_n(\Bbbk)$.

3.22. а Якщо $a \in I_R$, то існує така матриця $A \in I$, що $a\mathsf{e}_{11} = \mathsf{e}_{1i}A\mathsf{e}_{j1}$ для деяких i, j, тому $ra\mathsf{e}_{11} = \mathsf{e}_{1i}(rA)\mathsf{e}_{j1} \in I$ для довільного $r \in R$, отже, $ra \in I_R$. Для $b \in I_R$ існує така матриця $B \in I$, що $b\mathsf{e}_{11} = \mathsf{e}_{1k}B\mathsf{e}_{l1}$, тоді $(ra + sb)\mathsf{e}_{11} \in I$ для довільних $r, s \in R$, отже, $ra + sb \in I_R$. Таким чином, I_R — ідеал. b Для довільного двостороннього ідеалу $I \in \mathrm{M}_n(R)$ визначимо ідеал I_R як у попередньому пункті. Очевидно, $I \subset \mathrm{M}_n(I_R)$. Покажемо, що $\mathrm{M}_n(I_R) \subset I$. Для довільного $a \in I_R$ матриця $a\mathsf{e}_{ij} \in \mathrm{M}_n(R)$. Тоді знайдеться така матриця $A \in I$, що $a\mathsf{e}_{ij} = \mathsf{e}_{ik}A\mathsf{e}_{lj} \in I$ для довільних $i, j = 1, \ldots, n$. Отже, $\mathrm{M}_n(I_R) \subset I$. с Кільце $\mathrm{M}_n(\mathbb{Q})$ просте, ідеали $\mathrm{M}_n(\mathbb{Z})$ мають вигляд $\mathrm{M}_n(k\mathbb{Z})$, $k \in \mathbb{N}$.

3.23. Характеристичним многочленом строго верхньої трикутної матриці A є $\chi_A(t) = t^n$, а $\chi_A(A) = 0$ за теоремою Гамільтона-Келі, отже, $A^n = 0$.

3.24. Двосторонні: $\{0\}$, $\left\{\begin{pmatrix} 0 & a & b \\ 0 & c & d \\ 0 & 0 & e \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} 0 & 0 & a \\ 0 & 0 & b \\ 0 & 0 & c \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & 0 \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} a & b & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}$ та їхні перетини та об'єднання.

Праві: $\left\{\begin{pmatrix} 0 & 0 & 0 \\ 0 & a & b \\ 0 & 0 & c \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} a & b & c \\ 0 & 0 & d \\ 0 & 0 & d \end{pmatrix}\right\}$ та їхні перетини та об'єднання.

Ліві: $\left\{\begin{pmatrix} a & 0 & b \\ 0 & 0 & c \\ 0 & 0 & d \end{pmatrix}\right\}$, $\left\{\begin{pmatrix} a & b & 0 \\ 0 & c & 0 \\ 0 & 0 & 0 \end{pmatrix}\right\}$ та їхні перетини та об'єднання.

Нільпотентні: $\left\{\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}\right\}$.

Тут a, b, c, d, e — довільні дійсні числа.

3.25. Нехай $I \subset R$ — ідеал, $I_1 = \{x \in R_1 \mid (x, y) \in I\}$, $I_2 = \{y \in R_2 \mid (x, y) \in I\}$. Якщо $x_1, x_2 \in I_1$, то існують $(x_i, y_i) \in I$, $i = 1, 2$, а тому $(x_i, y_i)(1, 0) = (x_i, 0) \in I$, звідки $(x_1 + x_2, 0) \in I$ і $x_1 + x_2 \in I_1$. Якщо $x \in I_1$, то існує $(x, y) \in I$, а тому для $(r, 0) \in R$ $(x, y)(r, 0) = (rx, 0) \in I$, $(r, 0)(x, y) = (xr, 0) \in I$, звідки $xr, rx \in I_1$. Отже, I_1 — ідеал R_1. Аналогічно доводиться, що I_2 — ідеал R_2, а отже, $I_1 \times I_2$ — ідеал R. Очевидно, $I \subset I_1 \times I_2$. Навпаки, якщо $x_1 \in I_1$ та

$y_2 \in I_2$, то існують $(x_1, 0), (0, y_2) \in I$, звідки $(x_1, y_2) \in I$, тому $I = I_1 \times I_2$. Якщо R_1, R_2 прості кільця, то ідеалами в $R_1 \times R_2$ є $\{0\}$, R, $R_1 \times \{0\}$, $\{0\} \times R_2$.

3.26. b), c).

3.27. В $\mathbb{Z}_6 \times \mathbb{Z}_8$ максимальні ідеали: $2\mathbb{Z}_6 \times \mathbb{Z}_8$, $3\mathbb{Z}_6 \times \mathbb{Z}_8$ та $\mathbb{Z}_6 \times 2\mathbb{Z}_8$; мінімальні: $2\mathbb{Z}_6 \times \{0\}$, $3\mathbb{Z}_6 \times \{0\}$ та $\{0\} \times 4\mathbb{Z}_8$; нільпотентні: $\{0\} \times 2\mathbb{Z}_8$ та $\{0\} \times 4\mathbb{Z}_8$. В $\mathbb{Z} \times \mathbb{Z}$ максимальні: $p\mathbb{Z} \times \mathbb{Z}$ та $\mathbb{Z} \times p\mathbb{Z}$, p — просте; мінімальних та нільпотентних немає. В $\mathbb{Q} \times \mathbb{Q}$ є два нетривіальні ідеали $\{0\} \times \mathbb{Q}$ та $\mathbb{Q} \times \{0\}$.

3.28. a Позначимо $c = \text{НСК}(n, m)$. Якщо $x \in (n\mathbb{Z}) \cap (m\mathbb{Z})$, то $x \mid c$, звідки $c\mathbb{Z} \subset x\mathbb{Z} \subset (n\mathbb{Z}) \cap (m\mathbb{Z})$. А з того, що $n\mathbb{Z} \subset c\mathbb{Z}$ та $m\mathbb{Z} \subset c\mathbb{Z}$ одержимо $(n\mathbb{Z}) \cap (m\mathbb{Z}) \subset c\mathbb{Z}$. b Нехай $d = \text{НСД}(n, m)$, тоді існують $u, v \in \mathbb{Z}$ такі, що $d = nu + mv$, отже $d\mathbb{Z} \subset n\mathbb{Z} + m\mathbb{Z}$. Навпаки, оскільки $d \mid n$, то $n\mathbb{Z} \subset d\mathbb{Z}$.

3.30. Нехай $R = \text{M}_2(\mathbb{Q})$, $S = T_2(\mathbb{Q})$ — підкільце верхніх трикутних матриць. Тоді множина $\left\{\left(\begin{smallmatrix} 0 & a \\ 0 & 0 \end{smallmatrix}\right) \mid a \in \mathbb{Q}\right\}$ утворює ненульовий ідеал кільця S, але в R ненульових ідеалів не існує.

3.31. e Оскільки I та J є ідеалами, то $IJ \subset I$, $IJ \subset J$, звідки $IJ \subset I \cap J$. Якщо $I + J = R$, то існують такі $x_I \in I$, $x_J \in J$, що $1 = x_I + x_J$. Тоді для довільного $y \in I \cap J$ маємо: $y = x_I y + x_J y \subset IJ + JI \subset IJ$, звідки одержимо рівність.
f $I \cup J$ є ідеалом тоді і лише тоді, коли один із них міститься в іншому. Наприклад, $2 + 3 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$, отже, це не ідеал.

3.32. Нехай $a \in D$. Тоді $(aD)(aD) = aD \cap aD = aD$, отже, $a \in (aD)(aD)$, що дає $a = \sum_{i=1}^{k} (ab_i)(ac_i)$ для деяких $b_i, c_i \in D$, $i = 1, \ldots, k$. Звідси $a = a^2 r$, де $r = \sum_{i=1}^{k} b_i c_i$. Якщо $a \neq 0$, то, скоротивши на a, одержимо $1 = ar$.

3.33. Для довільних $x, y \in I$ існує $n > 0$, таке, що $x, y \in I_n$, але тоді $x + y \in I_n \subset I$ і $rx \in I_n \subset I$ для довільного $r \in R$, отже, I – ідеал.

3.35. Правий анулятор матриці A_1: $\left\{\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}\right\}$, лівий анулятор матриці A_1: $\left\{\left(\begin{smallmatrix} 0 & a \\ 0 & b \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}\right\}$. Правий анулятор матриці A_2: $\left\{\left(\begin{smallmatrix} -2a & -2b \\ a & b \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}\right\}$, лівий анулятор матриці A_2: $\left\{\left(\begin{smallmatrix} 0 & a \\ 0 & b \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}\right\}$.

3.36. $(x, y) \in Ann(a)$ тоді і лише тоді, коли $4x \equiv 0 \pmod{18}$ і $6y \equiv 0 \pmod 8$. Звідси $Ann(a) = 9\mathbb{Z}_{18} \times 2\mathbb{Z}_8$, $|Ann(a)| = 8$.

3.37. Якщо I — нільпотентний ідеал, то для деякого $n \in \mathbb{N}$: $I^n = \{0\}$. Тому для довільного $a \in I$ $a^n = 0$. Навпаки, нехай I — такий ідеал, що всі його елементи є нільпотентними. Нехай $a_1, a_2, \ldots, a_k$ — довільні елементи з I, такі, що $a_1 a_2 \ldots a_k \neq 0$. Покладемо $b_j = a_1 \ldots a_j$ для $j = 1, \ldots, k$, зауважимо, що $b_j \neq 0$. Припустимо, що для деякого $l < k$ $b_j = b_l$. Позначимо $c = a_{j+1} \ldots a_l$. Тоді для будь-якого $m \in \mathbb{N}$: $b_j c^m = (b_j c)c^{m-1} = b_l c^{m-1} = b_j c^{m-1} = \ldots = b_j$. Звідси випливає, що $c^m \neq 0$ для жодного $m \in \mathbb{N}$, що суперечить припущенню. Таким чином, для $j = 1, \ldots, k$ всі b_j різні і $b_j \neq 0$, отже, $k < |I|$. Зокрема, $I^{|I|} = \{0\}$.

3.38. Матриці $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ та $\left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$ нільпотентні, а їх сума — ні.

3.39. *Вказ.* Використайте біноміальну формулу щоб довести замкненість відносно додавання.

3.40. $\mathfrak{N} = p\mathbb{Z}_{p^m}$.

Розділ 4

4.5. Ні, не залишиться.

4.6. a Оскільки $\varphi(1) = 1$, то $\varphi(n) = n \cdot \varphi(1) = n \cdot 1 = n$.
b Обмеження гомоморфізму кілець $\varphi : \mathbb{Q} \to \mathbb{Q}$ на $\mathbb{Z}$ є гомоморфізмом, отже, $\varphi(n) = n$. Тоді для $\frac{n}{m} \in \mathbb{Q}$ маємо: $m \cdot \varphi\left(\frac{n}{m}\right) = \varphi\left(m \cdot \frac{n}{m}\right) = \varphi(n) = n$, отже, $\varphi\left(\frac{n}{m}\right) = \frac{n}{m}$.
c Нехай $\varphi : \mathbb{R} \to \mathbb{R}$ — автоморфізм. Якщо $x \geqslant 0$, тоді $x = (\sqrt{x})^2$. Таким чином, $\varphi(x) = \varphi((\sqrt{x})^2) = (\varphi(\sqrt{x}))^2 \geqslant 0$. Отже, відображення $\varphi : \mathbb{R} \to \mathbb{R}$ є монотонним, бо коли $b - a > 0$, то $\varphi(b - a) = \varphi(b) - \varphi(a) > 0$. Припустимо тепер, що для деякого $r \in \mathbb{R}$ $\varphi(r) \neq r$. Нехай $\varphi(r) < r$. Оскільки $\mathbb{Q}$ є скрізь щільною в $\mathbb{R}$ множиною, то існує таке $q \in \mathbb{Q}$, що $\varphi(r) < q < r$, але $q = \varphi(q) < \varphi(r)$. Аналогічно розглядається випадок $\varphi(r) > r$. Отже, $\varphi(r) = r$. d Випливає з того, що $\varphi(-1) = \varphi(i^2) = (\varphi(i))^2 = -1$, отже, $\varphi(i) = \pm i$.

4.10. $\operatorname{Ker} \varphi_{\sqrt{3}} = (x^2 - 3)$, $\operatorname{Im} \varphi_{\sqrt{3}} = \mathbb{Q}[\sqrt{3}]$, $\operatorname{Ker} \varphi_{\sqrt{3}+i} = \left(x^2 - 2\sqrt{3}x + 4\right)$, $\operatorname{Im} \varphi_{\sqrt{3}+i} = \mathbb{Q}[\sqrt{3} + i]$

4.11. $\mathbb{Z}_{12}/I \simeq \mathbb{Z}_{12}/J \simeq \mathbb{Z}_4$. Прості ідеали: $(\overline{2})$, $(\overline{3})$.

4.12. a $\mathbb{Z}_2 \times \mathbb{Z}_2$, I не є простим. b $\mathbb{Z}_3 \times \mathbb{Z}_3$, I не є простим.

4.13. Існує єдиний гомоморфізм кілець $\varphi : \mathbb{Z} \to \mathbb{Z}_{18}$, $\varphi(k) = k \pmod{18}$. Всі ідеали кільця $\mathbb{Z}_{18}$ — це головні ідеали вигляду $(\overline{d})$, де d — дільник 18. Факторкільця: $\mathbb{Z}_{18}/\big(\overline{d}\big) \simeq \mathbb{Z}_d$.

4.14. Кількість елементів 27. Нехай $I = \big(2x^3 + x^2 + 1\big)$, дільники нуля: $x + 1 + I$, $x^2 + x + 2 + I$. З $\mathbb{Z}_3[x]/(x^3 + 2x + 2)$, бо $2(2x^3 + x^2 + 1) = x^3 + 2x + 2$ в $\mathbb{Z}_3[x]$.

4.16. $A \not\simeq \mathbb{Z}_4$, бо в A маємо $a + a = 0$ для довільного $a \in A$. Крім того, A містить нільпотентний елемент $x + 1 \neq 0$, а в $\mathbb{Z}_2 \times \mathbb{Z}_2$ і в полі немає ненульових нільпотентних елементів.

4.18. $\mathbb{Z}_7[x]/(x^2 + 4)$.

4.19. Для $f_2(x)$.

4.20. *Вказ.* Гомоморфізм $f(x) \in \mathbb{Z}[x] \xmapsto{\varphi} f(x) \pmod{2} \in \mathbb{Z}_2[x]$ є епіморфізмом і $\operatorname{Ker}\varphi = I$. Тоді $\mathbb{Z}[x]/I \cong \mathbb{Z}_2[x]$. Отже, ідеал I — простий, бо $\mathbb{Z}_2[x]$ є областю цілісності, але не максимальний, бо $\mathbb{Z}_2[x]$ не поле. Для ідеалу J розгляньте епіморфізм $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$, $f(x) \mapsto f(0)$.

4.21. *Вказ.* Розгляньте епіморфізм $\varphi : \mathbb{Z}_{30} \to \mathbb{Z}_5$, $a \mapsto a \pmod{6}$ з ядром $5\mathbb{Z}_{30}$.

4.22. a Достатньо вказати епіморфізм кілець $\varphi : \mathbb{R}[x] \to \mathbb{R}$, ядром якого є ідеал $\big(x-3\big)\mathbb{R}[x]$. Покладемо $\varphi(f(x)) = f(3)$. b Відображення $\varphi : \mathbb{R}[x] \to \mathbb{R}^2$, $f(x) \mapsto \big(f(1), f(-1)\big)$ є епіморфізмом з ядром $\operatorname{Ker} f = (x^2 - 1)\mathbb{R}[x]$; c Відображення $\varphi : \mathbb{R}[x] \to \mathbb{C}$, $f(x) \mapsto f(i)$ є епіморфізмом, ядро якого утворюють дійсні многочлени, які діляться на $(x - i)$, а отже і на $(x + i)$, тобто $\operatorname{Ker} f = (x^2 + 1)\mathbb{R}[x]$. d Розгляньте відображення $\varphi : \mathbb{R}[x] \to \mathbb{R}^2$, $f(x) \mapsto \big(f(3), f(-2)\big)$. e Розгляньте відображення $\varphi : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{2}]$, $f(x) \mapsto f(\sqrt{2})$.

4.23. Розглянемо епіморфізм кілець $\varphi : \mathbb{R}[x, y] \to \mathbb{R}[x]$, $\varphi(f(x, y)) = f(x, x^2)$. Покажемо, що довільний многочлен $f(x, y)$ можна зобразити у вигляді $f(x, y) = f'(x) + (y - x^2) \cdot f''(x)$. Дійсно, запишемо $f(x, y)$ як многочлен від y з коефіці-

єнтами з $\mathbb{R}[x]$. Нехай $a(x)y^k$, $k>0$ є старшим членом $f(x,y)$. Тоді $f(x,y) = (y-x^2)a(x)y^{k-1} + g(x,y)$, де $\deg_y g(x,y) < \deg_y f(x,y)$. Маємо: $f(x,y) \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(f(x,y)) \equiv 0$. Якщо $f(x,y) = f'(x) + (y-x^2)\cdot f''(x) \in \operatorname{Ker}\varphi$, то $f'(x) \equiv 0$, а отже $f(x,y) \in \big(x^2-y\big)$.

4.24. *Вказ.* В полі $\mathbb{R}[x]$ многочлени x^2-2 та x^2-3 звідні, отже, $\mathbb{R}[x]/(x^2-2) \cong \mathbb{R}^2 \cong \mathbb{R}[x]/(x^2-3)$. Ізоморфізм $\varphi : \mathbb{R}[x]/(x^2-2) \to \mathbb{R}[x]/(x^2-3)$ можна задати як $x \mapsto \sqrt{\frac{2}{3}}\, x$.

$\mathbb{Q}[x]/(x^2-2) \ncong \mathbb{Q}[x]/(x^2-3)$. *Вказ.* Якщо $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[x]/(x^2-3)$, то $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[\sqrt{3}]$, тоді $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$. Отже, існують такі a і b, що $\sqrt{2} = a+b\sqrt{3}$, звідки одержимо $2ab\sqrt{3} = 2-a^2-3b^2$, тобто $\sqrt{3} \in \mathbb{Q}$.

4.25. Зауважимо, що $\mathbb{Q}[a+\sqrt{d}] \cong \mathbb{Q}[x]/(x^2-2ax+a^2-d)$. Ядром епіморфізмів $\varphi_\pm : \mathbb{Q}[x] \to \mathbb{Q}[\sqrt{d}]$, $x \mapsto a \pm \sqrt{d}$ є ідеал $(x^2-2ax+a^2-d)$, за першою теоремою про гомоморфізм одержимо потрібний ізоморфізм.

4.26. Відображення $\varphi_\pm : \mathbb{Q}[x]/(x^2-4x-1) \to \mathbb{Q}[\sqrt{5}]$, $x \mapsto 2 \pm \sqrt{5}$ є ізоморфізмами кілець.

4.27. Усі три кільця ізоморфні.

4.28. a Ядром епіморфізму кілець $\pi_3 : \mathbb{Z}[x] \to \mathbb{Z}_3[x]$, визначеного як $f(x) \overset{\pi_3}{\longmapsto} f(x) \pmod 3$, є ідеал $\big(3\big)$. b Ядром епіморфізму кілець $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_2$, визначеного як $f(x) \overset{\varphi}{\longmapsto} f(0) \pmod 2$, є ідеал $\big(2,x\big)$. c Ядром композиції епіморфізмів

$$\mathbb{Z}[x] \xrightarrow{\pi_n} \mathbb{Z}_n[x] \xrightarrow{\pi} \mathbb{Z}_n[x]/(f(x))$$

є ідеал $I = (n, f(x))$.

4.30. Визначимо відображення $\varphi : A \to \mathbb{Z}_2[x]/\big(x^2+1\big)$ за правилом: $f(x)+I \mapsto f(x) + \big(x^2+1\big)$. Це відображення визначене коректно, бо x^2+1 ділить x^4+1 над $\mathbb{Z}_2$. Легко перевірити, що φ — епіморфізм і $\operatorname{Ker}\varphi = I$. Ідеал $\big(x^2+1\big)$ не є простим в A, оскільки $(x+1)(x+1) \equiv 0 \pmod{(x^2+1)}$.

4.31. Твірні: $x+1$, $2x+1$, $2x+2$, $x+2$.

4.32. Адитивна група поля F не може бути циклічною. Дійсно, якщо a — твірний циклічної групи порядку 9, то

$a+a+a \neq 0$, а $(a+a+a)\cdot(a+a+a) = 9\cdot a^2 = 0$, а в полі немає нільпотентних елементів.

4.33. Поле F містить нейтральний елемент 0 та елемент 1 порядку 3, отже, $2 \in F$. Нехай $\alpha \in F \setminus \{0,1,2\}$, тоді $\alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2$ — різні елементи поля F. Отже, $F = \{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$. Тоді $\alpha^2 = a\alpha + b$ для деяких $a, b \in \mathbb{Z}_3$, а отже, α – корінь многочлена $f(x) = x^2 + 2ax + 2b \in \mathbb{Z}_3[x]$ і $F \cong \mathbb{Z}_3[x]/\big(f(x)\big)$. Оскільки F — поле, то многочлен $f(x)$ — незвідний.

4.34. Існує три незвідних унітарних квадратних многочлени в кільці $\mathbb{Z}_3[x]$, а саме: $f_1(x) = x^2+1$, $f_2(x) = x^2+x+2$, $f_3(x) = x^2+2x+2$. Причому довільні два многочлени одержуються один з одного лінійною заміною змінних. Позначимо $A_i = \mathbb{Z}_3[x]/\big(f_i(x)\big)$.

Побудуємо ізоморфізм кілець A_1 та A_2. Відображення кілець $\varphi : \mathbb{Z}_3[x] \to A_2$, $f(x) \overset{\varphi}{\longmapsto} f(x+2) \pmod{\big(f_2(x)\big)}$, є гомоморфізмом. Ядро φ складається з таких многочленів $f(x) \in \mathbb{Z}_3[x]$, що $f(x+2)$ ділиться на $f_2(x)$, а це можливо лише тоді, коли $f(x)$ ділиться на $f_2(x+1) = f_1(x)$. Таким чином, $\operatorname{Ker}\varphi = \big(f_1(x)\big)$. За першою теоремою про гомоморфізм для кілець $A_1 \cong \mathbb{Z}_3[x]/\big(f_1(x)\big) \cong \operatorname{Im}\varphi$, а оскільки A_1 та A_2 мають однакову кількість елементів, то φ — епіморфізм. Отже, одержимо ізоморфізм $\varphi : A_1 \to A_2$. Інші ізоморфізми встановлюються аналогічно.

4.35. Достатньо показати, що многочлен $f(x) = x^2 + 1$ не має коренів в полі $\mathbb{Z}_p$. Інакше, якщо $a \in \mathbb{Z}_p$ — корінь, то $a^2 = -1 \neq 0$, $a^4 = 1$ і a — елемент порядку 4. Але порядок мультиплікативної групи $\mathbb{Z}_p^*$ дорівнює $p-1$ і, за умовою, не ділиться на 4, що суперечить теоремі Лагранжа.

4.36. $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5$. Дійсно, $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[x]/(x^2+1, x+2)$, бо ідеал $I = (x^2+1, x+2)$ є ядром композиції епіморфізмів $\mathbb{Z}[x] \to \mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i] \to \mathbb{Z}[i]/(2+i)$. Покажемо, що $I = (5, x+2)$. З рівності $5 = x^2+1-(x+2)(x-2)$ одержимо, що $5 \in I$ і $(5, x+2) \subset I$. Навпаки, $x^2+1 = (x+2)(x-2)+5$, звідки $I \subset (5, x+2)$ і маємо рівність. Звідси $\mathbb{Z}[i]/(2+i) \cong$

$\mathbb{Z}[x]/(5, x+2) \cong \mathbb{Z}_5$. b $\mathbb{Z}[i]/(1-2i) \cong \mathbb{Z}_5$, оскільки $(1-2i) = \big(i(1-2i)\big) = (2+i)$ (елементи $1-2i$ та $2+i$ асоційовані в $\mathbb{Z}[i]$). c $\mathbb{Z}[i]/(3+2i) \cong \mathbb{Z}_{13}$.d $\mathbb{Z}[i]/(a+bi) \cong \mathbb{Z}_p \cong \mathbb{Z}[x]/I$, $I = (x^2+1, ax+b) = (p, ax+b)$.

4.40. Елементи $e_1 = (1,0)$, $e_2 = (0,1)$ є ідемпотентами з властивостями $e_1 \cdot e_2 = 0$, $e_1 + e_2 = 1_A$. Оскільки в кільці A є лише чотири ідемпотенти: 0_A, e_1, e_2 та 1_A, то можливі лише такі гомоморфізми $\varphi_i : A \to A$, $i = 1, \ldots, 4$, що: $\varphi_1(e_1) = e_1$, $\varphi_1(e_2) = e_2$; $\varphi_2(e_1) = e_2$, $\varphi_2(e_2) = e_1$; $\varphi_3(e_1) = 1_A$, $\varphi_3(e_2) = 0_A$; $\varphi_4(e_1) = 0_A$, $\varphi_4(e_2) = 1_A$. Тобто $\varphi_1(x,y) = (x,y)$, $\varphi_2(x,y) = (y,x)$, $\varphi_3(x,y) = (x,x)$, $\varphi_4(x,y) = (y,y)$.

4.41. $\mathrm{End}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, $\mathrm{End}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \{(0,0)\}$, $\mathrm{End}(\mathbb{Z}_{440}) \cong \mathrm{End}(\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_{11}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_{10}$.

Розділ 5

5.2. Припустимо, що (a) — простий ідеал. Тоді якщо $a = bc$, то або $b \in (a)$, або $c \in (a)$. Припустимо, що $b \in (a)$, це означає, що $b = ad$ для деякого $d \in R$. Отже, $a = adc$, звідси $dc = 1$, тобто $c \in R^*$.

5.3. Нехай R — факторіальне кільце. Тоді кожний простий елемент є нерозкладним (див. задачу 5.2). Нехай $p \in R$ — нерозкладний, $a, b \in R$, $ab \in (p)$. Тоді $ab = cp$ для деякого $c \in R$. Нехай $a = up_1 \ldots p_s$, $b = vq_1 \ldots q_r$ — розклади елементів a і b в добуток нерозкладних, де $u, v \in R^*$. З однозначності розкладу маємо, що $p = u_i p_i$ або $p = v_j q_j$ для деяких $u_i, v_j \in R^*$. Таким чином, $a \in (p)$ або $b \in (p)$.

5.5. Ні, наприклад, якщо n складене, то $\mathbb{Z}_n$ не є кільцем головних ідеалів, оскільки не є областю цілісності.

5.9. a) Розкладемо a на прості множники: $a = 7+i = (i+2)^2(1-i)$. Перевіривши, одержимо, що $c = (i+2)(1-i) = 1+3i$ ділить b, причому числа $\frac{a}{c}$ та $\frac{b}{c}$ взаємно прості, оскільки вони мають взаємно прості норми: 5 та 17 відповідно. Отже, $\mathrm{НСД}(a,b) = 1+3i$. b) $3+i$; c) $1+3i$.

5.10. a $\pm 1 \pm 2i$, $\pm 2 \pm i$; b ± 5, $\pm 5i$; c Це всі числа з нормою 5. d Оскільки $5 = (1-2i)(1+2i)$ і $3-i = (1-2i)(1+i)$, то $\mathrm{НСД}(5, 3-i) = 1-2i$, $\mathrm{НСК}(5, 3-i) = 5(1+i)$.

5.11. a НСД норм чисел 5 та $3+i$ дорівнює 5, серед чисел з нормою 5 знаходимо НСД$(5, 3+i) = 1+2i$. Отже, $\big(5\big) + \big(3+i\big) = \big(1+2i\big)$, $\big(5\big) \cap \big(3+i\big) = \big(\frac{5(3+i)}{1+2i}\big) = \big(5-5i\big)$. b Твірним є НСД$(5, 4+3i) = 2-i$. c Оскільки $1+13i = (7+6i)(1+i)$ і $85 = (7+6i)(7-6i)$, то $\big(85, 1+13i\big) \subset \big(7+6i\big)$. Навпаки, $85 = (7+6i) - (1+13i)\cdot 6i$, звідки одержимо $\big(7+6i\big) \subset \big(85, 1+13i\big)$.

5.12. a) Оскільки $N(5+i) = 26$, то дільники числа $5+i$ можуть мати норму 2 або 13, тобто знаходяться серед чисел $\pm 1 \pm i$, $\pm 2 \pm 3i$, $\pm 3 \pm 2i$. Перевірка показує, що дільниками з нормою 2 є усі числа вигляду $\pm 1 \pm i$, вони є простими і попарно асоційованими. З нормою 13 дільниками є числа вигляду $\pm(3-2i)$, $\pm(2+3i)$, також прості і попарно асоційовані. Маємо, наприклад, такий розклад $5+i = (1+i)\,(3-2i) = (1-i)\,(2+3i)$. b) $(2+i)(2-i)(1+i)$; c) $(2+i)^2(1-i)$; d) $(1+i)(5-2i)$; e) $-(1-i)^3(2-i)^2$.

5.13. b Розгляньте $4 = 2\cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$.

5.14. Не існує. *Вказівка.* Спільними дільниками чисел 4 і $2-2i\sqrt{3}$ є ± 1, ± 2, $\pm 1 \pm i\sqrt{3}$. Жодне з чисел ± 1, $\pm 1 \pm i\sqrt{3}$ не ділиться на 2, тому жодне з них не є НСД$(4, 2-2i\sqrt{3})$. Числа 2 і -2 теж не будуть НСД даних чисел, бо 2 і -2 не діляться на $1+i\sqrt{3}$.

5.15. a Обидва числа 2 та $1+i\sqrt{5}$ є дільниками чисел 6 та $2+2i\sqrt{5}$, але жодне з них не ділиться на інше. b Обидва многочлени x^2 та x^3 є дільниками многочленів x^5 та x^6, але жодний з них не ділиться на інший.

5.16. НСД$(5+\sqrt{3}, 3-\sqrt{3}) = 1+\sqrt{3}$, НСК$(5+\sqrt{3}, 3-\sqrt{3}) = 9-7\sqrt{3}$.

5.17. $I+J = (1+\sqrt{3})$, $IJ = \big(12-2\sqrt{3}\big)$, $I\cap J = \big(9-7\sqrt{3}\big)$.

5.18. $10 = 2\cdot 5 = (2+i\sqrt{6})(2-i\sqrt{6})$ — два різні розклади в добуток нерозкладних.

5.19. Елемент 3 не є простим, бо $(2+i\sqrt{5})(2-i\sqrt{5}) = 3^2$ ділиться на 3, але $(2+i\sqrt{5})$ та $(2-i\sqrt{5})$ не діляться на 3. Аналогічно для інших.

5.20. Елементи 2 та $2i$ є нерозкладними, проте не асоці-

йованими в $\mathbb{Z}[2i]$, оскільки $i \notin \mathbb{Z}[2i]$, але $4 = 2\cdot 2 = (-2i)\cdot(2i)$ — два різних розклади в добуток нерозкладних.

5.21. *Вказівка.* $\cos^2 x - \sin^2 x = (\cos x - \sin x)(\cos x + \sin x) = 1 - 2\sin^2 x$.

5.22. a Мають місце ізоморфізми: $\mathbb{Z}[i\sqrt{5}]/\big(2, 1+i\sqrt{5}\big) \cong \mathbb{Z}_2$, $\mathbb{Z}[i\sqrt{5}]/\big(3, 2+i\sqrt{5}\big) \cong \mathbb{Z}_3$, $\mathbb{Z}[i\sqrt{5}]/\big(3, 2-i\sqrt{5}\big) \cong \mathbb{Z}_3$. b Припустимо, що $(3, 2+i\sqrt{5}) = (a+bi\sqrt{5})$, $a, b \in \mathbb{Z}$. Тоді $3 = \alpha(a+bi\sqrt{5})$ і $2+i\sqrt{5} = \beta(a+bi\sqrt{5})$ для деяких $\alpha, \beta \in \mathbb{Z}[i\sqrt{5}]$. Розглянемо норму $N(a+bi\sqrt{5}) = a^2+5b^2$. Тоді $9 = N(\alpha)(a^2+5b^2)$, отже, a^2+5b^2 може бути рівним 1, 3 або 9. У кожному з випадків приходимо до суперечності. c Однозначність випливає з того, що дільниками елемента 6 можуть бути лише числа 2, 3, $1+i\sqrt{5}$, $1-i\sqrt{5}$ та асоційовані до них.

5.23. Добуток ідеалів породжується добутками твірних, тому $\big(3, 1+i\sqrt{5}\big)\big(3, 1-i\sqrt{5}\big) = \big(9, 6, 3(1+i\sqrt{5}), 3(1-i\sqrt{5})\big) = \big(3, 3i\sqrt{5}\big) = \big(3\big)$.

Розділ 6

6.1. a $1 = 2a - 3b$; b $3 = 27a - 5b$; c $8 = 25a - 16b$; d $1+i = (-3+2i)a + 2b$; e $1 = (2-3i)a + (1+i)b$; f $1 = (-7+i)a + (13+2i)b$.

6.3. 1) $13\mathbb{Z}$ (бо НСД$(2210, 1131) = 13$); 2) $1111\mathbb{Z}$; 3) $3\mathbb{Z}$; 4) $\mathbb{Z}$; 5) $2\mathbb{Z}$; 6) $\mathbb{Z}$.

6.4. 1) $1 = 2\cdot 20 - 3\cdot 13$, звідси $(13)^{-1} \equiv -3 \equiv 17 \pmod{20}$; 2) 40; 3) 173; 4) не існує; 5) 104; 6) 211.

6.5. a НСД$(17, 43) = 1$, за алгоритмом Евкліда $1 = 17\cdot(-5) + 43\cdot 2$. Тоді $18 = 18\cdot 17\cdot(-5) + 18\cdot 43\cdot 2$. Звідси $x = 18\cdot 17\cdot(-5) \equiv 39 \pmod{43}$. b $x \equiv 41 \pmod{51}$; c $x \equiv 21 \pmod{61}$.

6.6. a НСД$(x^4+3x^2+4x+1, x^5+3x^3+2x^2+1) = 1$, за розширеним алгоритмом Евкліда, маємо, що $1 = (2x^3+4x^2+1)(x^4+3x^2+4x+1) + (3x^2+x)(x^5+3x^3+2x^2+1)$. Звідси випливає, що оберненим до $x^4+3x^2+4x+1+I$ є $2x^3+4x^2+1+I$. b x^2+I, c $4x^2+4x+I$; d $6x^3+5x^2+3x+3+I$.

6.7. 1 Нехай $c = \text{НСК}(a,b) \implies (c) \subset (a) \cap (b)$. Якщо $c' \in (a) \cap (b)$, то $(c') \subset (a)$ та $(c') \subset (b) \implies a \,|\, c',\ b \,|\, c' \implies c \,|\, c' \implies (c') \subset (c)$.

6.12. $\mathbb{Z}[i\sqrt{3}]$ не є факторіальним.

6.15. Припустимо, що b — необоротний, тоді a не ділиться на ab. Розділимо a на ab з остачею: $a = q(ab) + r$. Оскільки $r = a(1 - qb)$, то $N(a) \leqslant N(r) < N(ab)$.

6.16. 1 3 є простим гаусовим, 2 та 5 не є простими гаусовими. *Вказ.* $2 = (1+i)(1-i)$, $5 = (2+i)(2-i)$. 2 *Вказ.* Якщо $z = uv \in \mathbb{Z}[i]$, то $N(z) = N(u)N(v)$. Норму 17 мають $4 \pm i$ та асоційовані з ними, норму 29 мають $5 \pm 2i$ та асоційовані з ними. Простих гаусових чисел з нормою 43 не існує.

6.17. *Вказ.* $p = (a+bi)(a-bi) = a^2+b^2 \Leftrightarrow a^2 \equiv -b^2 \pmod p \Leftrightarrow (ab^{-1})^2 = -1 \pmod p$. Отже, порядок елемента ab^{-1} в групі $\mathbb{F}_p^*$ дорівнює 4, тому $4|(p-1)$.

6.19. $1 \pm i$, $2 \pm i$, 3, $3 \pm 2i$, $4 \pm i$ та асоційовані з ними.

6.20. *Вказ.* Розгляньте норму $N\left(\frac{m}{2^n}\right) = |m|$. Припустимо, що $n_1 \leqslant n_2$. Запишемо $\dfrac{m_1}{2^{n_1}} = \dfrac{m_1 \cdot 2^{n_2-n_1}}{2^{n_2}}$. Розділивши з остачею чисельник на m_2, одержимо $\dfrac{m_1}{2^{n_1}} = q\dfrac{m_2}{2^{n_2}} + \dfrac{r}{2^{n_2}}$, де $0 \leqslant r < |m_2|$, отже, $N\left(\dfrac{r}{2^{n_2}}\right) < N\left(\dfrac{m_2}{2^{n_2}}\right)$.

6.21. 2 Якщо x_0, y_0 та x, y — розв'язки, то $a(x - x_0) = -b(y - y_0)$, а отже $\dfrac{a}{(a,b)}(x - x_0) = \dfrac{-b}{(a,b)}(y - y_0) \implies$

$\dfrac{a}{(a,b)} \,|\, (y - y_0)$ і $\dfrac{b}{(a,b)} \,|\, (x - x_0)$

6.22. a, c розв'язків не існує; b $x = -5 + 29t$, $y = 4 - 17t$, $t \in \mathbb{Z}$;d $x = 4 + 7t$, $y = -1 - 4t$, $t \in \mathbb{Z}$; e $x = 2 + 5t$, $y = 1 - 3t$, $t \in \mathbb{Z}$; f $x = 9 + 23t$, $y = -4 + 19t$, $t \in \mathbb{Z}$.

6.23. *Вказ.* Використовуючи факт, що $I = (\alpha)$ для деякого $\alpha \neq 0$, покажіть, що представником кожного класу суміжності можна взяти елемент, норма якого менша за $N(\alpha)$.

6.24. Нехай $f(x) = x^3 - x^2 + 3$, $g(x) = x$. Розділимо $f(x)$ на $g(x)$ з остачею: $f(x) = g(x)(x^2 - x) + 3$. Оскільки α — корінь

$f(x)$, то $0 = g(\alpha)(\alpha^2 - \alpha) + 3$, звідки $\frac{1}{\alpha} = \frac{\alpha - \alpha^2}{3}$.

$\frac{1}{\alpha+1} = -\alpha^2 + 2\alpha - 2$; $\frac{1}{\alpha^2+1} = -\frac{\alpha^2+3\alpha-5}{16}$; $\frac{\alpha+5}{\alpha^2+3} = \frac{4-\alpha^2}{3}$.

Розділ 7

7.1. a) $6 \pmod 7$; b) немає розв'язків; c) $6 \pmod n$.

7.2. a $219 \pmod{256}$; b $36 \pmod{100}$; c $636 \pmod{676}$.

7.3. *Вказ.* Визначимо відображення $\varphi : R \to Re \times R(1-e)$ за правилом: $\varphi(r) = \big(re, r(1-e)\big)$, $r \in R$. Воно є гомоморфізмом, оскільки $\varphi(r)\varphi(s) = \big(re, r(1-e)\big)\big(se, s(1-e)\big) = \big(rse^2, rs(1-e)^2\big) = \big(rse, rs(1-e)\big) = \varphi(rs)$. Відображення φ — мономорфізм, оскільки рівність $\varphi(r) = \varphi(s)$ еквівалентна рівностям $re = se$ і $r(1-e) = s(1-e)$, що еквівалентно $r = s$, також φ — епіморфізм, оскільки для довільного $\big(ae, b(1-e)\big)$ маємо $\big(ae, b(1-e)\big) = \varphi(r)$, де $r = ae + b(1-e)$.

7.4. 1 Довільний елемент кільця e_iR має вигляд e_ia, де $a \in R$. Маємо: $e_ia = 1 \cdot e_ia = \sum\limits_{k=1}^{r} e_ke_ia = e_i^2a = e_ia$. Отже, e_i – одиниця кільця e_iR. 2 Якщо $a \in e_iR \cap e_jR$, то $e_ka = 0$ для довільного $1 \leqslant k \leqslant r$, але тоді $a = 1 \cdot a = 0$.

7.6. a $25 \cdot 5k = 125k \equiv 5k \pmod{30}$, отже $\overline{25}$ – одиниця в $5\mathbb{Z}_{30}$. Відображення $\varphi : \mathbb{Z}_6 \to 5\mathbb{Z}_{30}$, $\overline{1}_6 \mapsto 5 \cdot \overline{1}_{30}$ є ізоморфізмом. Крім того, за третьою теоремою про ізоморфізм, маємо: $\mathbb{Z}_{30}/5\mathbb{Z}_{30} \cong \big(\mathbb{Z}/30\mathbb{Z}\big)\big/\big(5\mathbb{Z}/30\mathbb{Z}\big) \cong \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$.

c $1 \equiv 25{+}6 \pmod{30}$ і $25{\cdot}6 \equiv 0 \pmod{30}$, $25^2 \equiv 25 \pmod{30}$, $6^2 \equiv 6 \pmod{30}$. Тоді $22 \equiv 25 \cdot 22 + 6 \cdot 22 \equiv 10 + 12 \pmod{30}$, а отже елементи $\overline{10}$ та $\overline{12}$ є ортогональними проекціями.

d $\mathbb{Z}_{30} \cong 15\mathbb{Z}_{30} \times 10\mathbb{Z}_{30} \times 6\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

7.7. За алгоритмом Евкліда: $1 = u \cdot n + v \cdot m$. Тоді $\overline{1} = \overline{un} + \overline{vm}$ в $\mathbb{Z}_{nm}$, причому $\overline{un} \cdot \overline{vm} = \overline{0}$. Елементи $\overline{un}$, $\overline{vm}$ є ідемпотентами, оскільки $\overline{un} + \overline{vm} = \overline{1} = \overline{1} \cdot \overline{1} = \overline{un}^2 + \overline{vm}^2$ і $n\mathbb{Z}_{nm} \cap m\mathbb{Z}_{nm} = \overline{0}$.

7.8. Оскільки $252 = 4 \cdot 9 \cdot 7$, то $\mathbb{Z}_{252} \cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$ (як кільце), а отже $\mathbb{Z}_{252}^* \cong \mathbb{Z}_4^* \times \mathbb{Z}_9^* \times \mathbb{Z}_5^* \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_6$. Найбільший порядок є найменшим спільним кратним $\text{НСК}(2, 6, 6) = 6$.

7.9. $1 = 2 \cdot 6 - 11 \equiv 55 + 12 \pmod{66}$ — розклад 1, $e_1 = 55$, $e_2 = 12$ – система ідемпотентів. Тоді $x \equiv 2 \cdot 55 + 7 \cdot 12 \equiv 62 \pmod{66}$.

7.10. a $\varphi(37) = (2, 1) \in \mathbb{Z}_5 \times \mathbb{Z}_9$. b $1 = 2 \cdot 5 - 1 \cdot 9$ — розклад 1 в $\mathbb{Z}_{45}$, $e_1 = -9 \equiv 36 \pmod{45}$, $e_2 = 10$ — шукана система ідемпотентів. Тоді $\varphi^{-1}(2, 6) \equiv 2 \cdot 36 + 6 \cdot 10 \equiv 42 \pmod{45}$, $\varphi^{-1}(3, 1) \equiv 28 \pmod{45}$.

7.12. a $\varphi(55) = (1, 3, 6) \in \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_7$. b Нехай $n_1 = 3$, $n_2 = 4$, $n_3 = 7$. Обчислимо

$$\begin{array}{lll} N_1 = 28, & t_1 = (28)^{-1} \pmod 3 = 1, & e_1 = t_1 N_1 = 28, \\ N_2 = 21, & t_2 = (21)^{-1} \pmod 4 = 1, & e_2 = t_2 N_2 = 21, \\ N_3 = 12, & t_3 = (12)^{-1} \pmod 7 = 3, & e_3 = t_3 N_3 = 36. \end{array}$$

Маємо розклад одиниці $1 = N_1 + N_2 + 3N_3 \pmod{84}$, отже, $\varphi^{-1}(1, 3, 6) \equiv N_1 + 3N_2 + 18N_3 \equiv N_1 - N_2 + 4N_3 \equiv 55 \pmod{84}$ (ми враховуємо, що $n_i N_i \equiv 0 \pmod n$).
$\varphi^{-1}(1, 3, 1) \equiv 31 \pmod{84}$.

Другий спосіб. Оскільки $\text{НСД}(N_2, N_3) = -N_2 + 2N_3$ і $1 = N_1 - 9 \cdot \text{НСД}(N_2, N_3)$, то $1 = N_1 + 9N_2 - 18N_3 \equiv N_1 + N_2 + 3N_3 \pmod{84}$ – розклад 1.

7.13. a) 31 (mod 66); b) 192 (mod 385); c) 311 (mod 504); d) 19 (mod 42); e) 93 (mod 693); f) 23 (mod 520).

7.14. 333.

7.15. 872.

7.16. 851. *Вказ.* Частка дає остачі 5, 1 і 4 при діленні на 9, 10 і 11 відповідно. Дійсно, покладемо $N = 9x + 7$, $M = 9y + 8$, $\frac{M}{N} = z = 9q + r$, звідси $7r \equiv 8 \pmod 9$, отже, $r = 5$. Аналогічно можна знайти остачі від ділення частки на 10 і 11. За китайською теоремою про остачі шукана частка матиме вигляд $851 + 990m$, $m \in \mathbb{Z}$, а число N матиме вигляд $817 + 990n$, $n \in \mathbb{Z}$. Оскільки N — тризначне число, то $n = 0$. Оскільки M — 6-значне число, то і $m = 0$.

Розділ 8

8.1. a) $\overline{8}$; b) $\overline{11}$; c) $\overline{10}$; d) $\overline{45}$. *Вказ.* З малої теореми Ферма

випливає $a^{p-2} \equiv a^{-1} \pmod{p}$. Отже, $23^{-1} \equiv 23^{45} \equiv (23^2)^{22} \cdot 23 \equiv 12^{22} \cdot 23 \equiv 3^{11} \cdot 23 \equiv 4 \cdot 23 \equiv 45 \pmod{47}$.

8.2. a 8 (mod 17). *Вказ.* За теоремою Ейлера $8^{16} \equiv 1 \pmod{17}$. Оскільки $(8, 17) = 1$, то можемо домножити обидві частини конгуентності на 8^{15}. Одержимо $x \equiv 13 \cdot 2^{45} \equiv -2^{47} \pmod{17}$ (врахували, що $13 \equiv -4 \pmod{17}$). Скористаємось ще раз теоремою Ейлера: $2^{16} \equiv 1 \pmod{17}$. Звідси отримаємо $x \equiv -2^{-1} \equiv 8 \pmod{17}$. b 12 (mod 13), c 15 (mod 36), d 12 (mod 25), e 17 (mod 32) , f 32 (mod 33).

8.3. 7. *Вказ.* $3^4 \equiv 1 \pmod{10}$.

8.4. 49 *Вказ.* Врахуйте, що $\varphi(100) = 40$, і скористайтеся теоремою Ейлера.

8.5. a) 32; b) 7; c) 27.

8.6. *Вказ.* Розбийте числа $1, 2, \ldots, 12$ на пари взаємно обернених за модулем 13.

8.8. *Вказ.* Застосуйте теорему Вільсона.

8.10. 661. *Вказ.* Перейдемо від $x = 444^{235} \pmod{1001}$ до системи конгруентностей

$$x \equiv 444^{235} \pmod{7};\ x \equiv 444^{235} \pmod{11};\ x \equiv 444^{235} \pmod{13}.$$

До кожної конгруентності можна застосувати малу теорему Ферма та зменшити основу степеня за відповідним модулем:

$$\begin{array}{ll} 444 \equiv 3 \pmod{7}, & 235 \equiv 1 \pmod{6}, \\ 444 \equiv 4 \pmod{11}, & 235 \equiv 5 \pmod{10}, \\ 444 \equiv 2 \pmod{13}, & 235 \equiv 7 \pmod{12}. \end{array}$$

Одержимо еквівалентну початковій систему

$$x \equiv 3 \pmod{7}; \quad x \equiv 4^5 \pmod{11}; \quad x \equiv 2^7 \pmod{13}.$$

Після спрощень дістанемо

$$x \equiv 3 \pmod{7}; \quad x \equiv 1 \pmod{11}; \quad x \equiv 11 \pmod{13}.$$

Розв'язок одержимо, використавши китайську теорему про остачі.

8.11. 641.

9.3. $\{1\}$ при $p = 3$; $\{1, 4\}$ при $p = 5$; $\{1, 2, 4\}$ при $p = 7$; $\{1, 3, 4, 9, 10, 12\}$ при $p = 13$.

9.4. a ± 11; b, c не мають розв'язків; d ± 6.

9.5. a), b), c), e), f) -1; d) 1.

9.6. $\left(\frac{7411}{9283}\right) = -1$.

9.7. $\left(\frac{1801}{8191}\right) = -1$.

9.8. *Вказ.* Степінь квадратичного лишка завжди є квадратичним лишком.

9.11. Припустимо, що $p_1, p_2, \ldots, p_s$ — скінченна послідовність всіх простих чисел вигляду $4k+1$. Розглянемо складене число $1 + 4p_1^2 p_2^2 \ldots p_s^2$, нехай q —його нетривіальний дільник. Тоді

$$4p_1^2 p_2^2 \ldots p_s^2 \equiv -1 \pmod{q} \text{ і } \left(\frac{-1}{q}\right) = 1.$$

Отже, $q = 4k + 1$ і q є числом зі списку $p_1, p_2, \ldots, p_s$, що неможливо.

9.12. $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{(3-1)(p-1)}{4}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$.

9.13. Якщо $n = ab$, $1 < a \leqslant b$, то $2^{ab} - 1$ ділиться на $2^a - 1$. Перші п'ять простих чисел Мерсенна: 3, 7, 31, 127, 8191.

9.14. $\left(\frac{3}{2^p-1}\right) = -\left(\frac{2^p-1}{3}\right) = -\left(\frac{1}{3}\right) = -1$.

9.15. Якщо просте число $p > 2$ є нетривіальним дільником n, тобто $n = pn_1$, то $(2^{n_1})^p + 1$ ділиться на $2^{n_1} + 1$. Перші п'ять простих чисел Ферма: 3, 5, 17, 257, 65537.

9.16. Оскільки $p - 1 = 2^k$ для деякого $k \in \mathbb{N}$, то порядок будь-якого елементу g теж є степенем 2. Якщо g — нелишок, то $-1 = \left(\frac{g}{p}\right) \equiv g^{\frac{p-1}{2}} \pmod{p}$. Тому порядок g не може бути меншим за $p - 1$.

9.17. *Вказ.* Покажіть, що $b^d \equiv \pm 1 \pmod{p}$. Оскільки за умовою $(b^d)^{n/d} \equiv -1 \pmod{p}$, то $b^d \equiv -1 \pmod{p}$ і n/d — непарне.

9.18. a Скористайтесь задачею 9.17. b Скористайтесь пунктом 5 теореми 9.3.

10.2. *Вказ.* Перевірте коректність задання операцій. Нулем є клас $\frac{0}{1}$; протилежним до $\frac{a}{s}$ є клас $\frac{-a}{s}$; одиницею є клас $\frac{1}{1}$.

10.6. $\mathbb{Q}$.

10.7. $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

10.8. Поле $K = \Bbbk(x_1, \ldots, x_n)$ раціональних функцій від змінних $x_1, \ldots, x_n$.

10.9. *Вказ.* Покажіть, що в кожному класі еквівалентності є представник $(x, 0)$, де $x \in \mathbb{Z}/n\mathbb{Z}$.

Література

[1] Ван дер Варден Б.Л. *Алгебра* – М.: Мир, 1976.

[2] Винберг Э.Б. *Курс алгебры.* 3-е изд. – М.: «Факториал Пресс», 2002.

[3] Коблиц Н. *Курс теории чисел и криптографии.* – М., Научное изд-во ТВП, 2001.

[4] Кострикин А.И. *Сборник задач по алгебре.* – М., Физматлит, 2001.

[5] Ленг С. *Алгебра* – М.: Мир, 1968.

[6] Lam T.Y. *Exercises in Classical Ring Theory.* 2nd ed. – New York, NY: Springer, 2003.

[7] Verma J.K. *Basic ring theory.* Електронне видання http://www.math.iitb.ac.in/atm/atmt1/jkv.pdf