Міністерство освіти і науки України
Житомирський державний університет імені Івана Франка

Погоруй Анатолій Олександрович
Фонарюк Олена Василівна

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

Навчально-методичний посібник

Житомир
2024

УДК 511.2:512(075.8)
А 45

Рекомендовано до друку Вченою радою
Житомирського державного університету імені Івана Франка
(протокол № 17 від 27 вересня 2024 року)

Рецензенти:

Валерій ЖУРАВЛЬОВ – доктор фізико-математичних наук, професор, завідувач кафедри вищої та прикладної математики Поліського національного університету.

Олександр ПРИЛИПКО – кандидат фізико-математичних наук, доцент, доцент кафедри інженерії програмного забезпечення Державного університету «Житомирська політехніка».

Василь МИХАЙЛЕНКО – доктор фізико-математичних наук, професор, професор кафедри алгебри та геометрії Житомирського державного університету імені Івана Франка.

Погоруй А. О., Фонарюк О. В. Алгебра і теорія чисел: Навчально-методичний посібник. Житомир: Вид-во ЖДУ імені Івана Франка, 2024. 86 с.

У навчально-методичному посібнику подано курс лекцій з алгебри і теорії чисел для здобувачів вищої освіти фізико-математичних факультетів, а також аспірантів, викладачів, науковців, докторантів. Викладений матеріал може бути використаний у навчальному процесі як на заняттях, так і при самостійному вивченні здобувачами курсу алгебри та теорії чисел.

УДК 511.2:512(075.8)

Зміст

ПЕРЕДМОВА....4

І ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ....5

ЛЕКЦІЯ 1. **ПОДІЛЬНІСТЬ З ОСТАЧЕЮ. АЛГОРИТМ ЕВКЛІДА**....5

ЛЕКЦІЯ 2. **БАЗОВІ ВЛАСТИВОСТІ** НСД **ТА** НСК**. ЛАНЦЮГОВІ ДРОБИ**....9

ЛЕКЦІЯ 3. **РІВНІСТЬ ЗА МОДУЛЕМ. МАЛА ТЕОРЕМА ФЕРМА**....14

ЛЕКЦІЯ 4. **ФОРМУЛА ВКЛЮЧЕННЯ-ВИКЛЮЧЕННЯ. ФУНКЦІЯ ОЙЛЕРА**....18

ЛЕКЦІЯ 5. **ТЕОРЕМА ОЙЛЕРА. КИТАЙСЬКА ТЕОРЕМА ПРО ЛИШКИ**....21

ЛЕКЦІЯ 6. **КІЛЬЦЕ. ПРИКЛАДИ КІЛЕЦЬ**....25

ЛЕКЦІЯ 7. **ПІДКІЛЬЦЕ. ОБЛАСТЬ ЦІЛІСНОСТІ.**....30

ЛЕКЦІЯ 8. **ІДЕАЛИ. ФАКТОР КІЛЬЦЕ**....34

ЛЕКЦІЯ 9. **ПОЛЕ. ПОЛЕ КОМПЛЕКСНИХ ЧИСЕЛ**....39

ЛЕКЦІЯ 10. **КІЛЬЦЕ МНОГОЧЛЕНІВ**....44

ЛЕКЦІЯ 11. **НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК МНОГОЧЛЕНІВ**....48

ЛЕКЦІЯ 12. **ВЛАСТИВОСТІ КОРЕНІВ МНОГОЧЛЕНА. ОСНОВНА ТЕОРЕМА АЛГЕБРИ**....51

ЛЕКЦІЯ 13. **РОЗШИРЕННЯ КІЛЕЦЬ І ПОЛІВ**....55

ЛЕКЦІЯ 14. **МНОГОЧЛЕНИ ВІД ДЕКІЛЬКОХ ЗМІННИХ**....60

ІІ ЕЛЕМЕНТИ АЛГЕБРИ....67

ЛЕКЦІЯ 15. **АЛГЕБРАЇЧНІ ОПЕРАЦІЇ. АЛГЕБРАЇЧНІ СТРУКТУРИ**....67

ЛЕКЦІЯ 16. **ГРУПИ**....72

ЛЕКЦІЯ 17. **ПІДГРУПА. СИМЕТРИЧНА ГРУПА. ЦИКЛІЧНІ ГРУПИ**....78

ЛЕКЦІЯ 18. **СУМІЖНІ КЛАСИ. ТЕОРЕМА ЛАГРАНЖА**....81

Література....85

ПЕРЕДМОВА

Цей навчальний посібник базується на лекціях з курсу алгебри та теорії чисел, які автори читають для студентів першого курсу бакалаврського рівня фізико-математичного факультету ЖДУ імені І. Франка. У ньому розглядаються основні поняття і твердження елементарної теорії чисел та короткий виклад базових властивостей деяких алгебраїчних структур з бінарною операцією.

Перший розділ посібника присвячений таким основам елементарної теорії чисел: подільність цілих чисел, ланцюгові дроби, еквіваленції та їх базові властивості, мала теорема Ферма та теорема Ойлера, Китайська теорема про лишки, алгоритм шифрування RSA, кільця та їх властивості, поле комплексних чисел, кільце многочленів, розширення кілець і полів, многочлени від кількох змінних.

У другому розділі посібника розглядаються поняття алгебраїчної структури та наводяться приклади таких алгебраїчних структур з бінарною операцією: півгрупа, моноїд, квазігрупа, група. Наводяться такі поняття теорії груп: гомоморфізм та ізоморфізм груп, підгрупа, циклічна група, суміжні класи, терема Лагранжа, тощо. Посібник можна використовувати у навчальному процесі для підготовки бакалаврів як аудиторно, так і при самостійному вивченні здобувачами курсу алгебри та теорії чисел.

І ЕЛЕМЕНТАРНА ТЕОРІЯ ЧИСЕЛ

ЛЕКЦІЯ 1. ПОДІЛЬНІСТЬ З ОСТАЧЕЮ. АЛГОРИТМ ЕВКЛІДА

Надалі будемо використовувати такі позначення:

$\mathbb{N}$ – множина натуральних чисел;

$\mathbb{Z}$ – множина цілих чисел;

$\mathbb{N}_0$ – множина натуральних чисел з нулем;

$\mathbb{Q}$ – множина раціональних чисел;

$\mathbb{R}$ – множина дійсних чисел;

$\mathbb{C}$ – множина комплексних чисел.

Означення 1.1. *Кажуть, що ціле число a ділиться на ціле число b, якщо існує ціле число c таке, що $a = bc$.*

Позначають $a \vdots b$ або $b|a$.

Означення 1.2. *Натуральне число $p \neq 1$ називається простим, якщо серед натуральних чисел воно ділиться тільки на 1 і на себе, тобто має рівно два різних натуральних дільники.*

Приклади: 2, 3, 5, 7, 11, 13, 17, 19 і т. д.

Якщо натуральне число $n \neq 1$ не просте, то воно називається складеним.

Твердження 1.1. *Якщо n складене, то найменший простий дільник числа n не більший ніж $\sqrt{n}$.*

Вправа 1.1. Твердження 1.1 довести самостійно.

Теорема 1.1 (Основна теорема арифметики) *Будь-яке натуральне число $n > 1$ можна факторизувати (розкласти) на прості множники, тобто*

$$n = p_1 p_2 \dots p_k,$$

де p_i, $i = 1,2, \dots, k$ – прості числа.

Доведення. Методом індукції: $4 = 2 \cdot 2$. Припустимо, що для деякого $n \in \mathbb{N}$ будь-яке натуральне число менше від n задовольняє теорему. Покажемо, що й саме n задовольняє теорему. Дійсно, якщо n – просте, то доведення завершено. Якщо ж n – складене, то існують натуральні $1 < l, m < n$ такі, що $n = lm$. За припущенням індукції $l = p_1 p_2 \dots p_r$, $m = q_1 q_2 \dots q_s$, де p_i, $i = 1,2, \dots, r$, q_j, $j = 1,2, \dots, s$ – прості числа. Звідки

$$n = p_1 p_2 \dots p_r q_1 q_2 \dots q_s,$$

Отже, n задовольняє теорему і за математичною індукцією будь-яке натуральне $n > 1$ факторизується в добуток простих множників.

Наслідок 1.1. Будь-яке натуральне $n > 1$ можна зобразити у вигляді

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \qquad (1.1)$$

де $p_1 < p_2 < \dots < p_k$, $\alpha_i \in \mathbb{N}$, $i = 1,2, \dots, k$.

Зображення (1.1) називається канонічним розкладом числа n на прості множники.

Теорема 1.2 (Евклід) *Простих чисел нескінченно багато.*

Доведення. Припустимо, що це не так. Тоді існує найбільше просте число p. Розглянемо число

$$n = 2 \cdot 3 \cdot \dots \cdot p + 1.$$

Тоді n ділиться на якесь просте $q \leq p$, а, отже, $1 \vdots q$, що неможливо. Суперечність виникла через припущення скінченності множини простих чисел.

Теорема 1.3 (Ділення з остачею) *Для довільних цілих a і b, $b \neq 0$ існує єдина пара цілих q і r така, що $a = bq + r$, де $0 \leq r < |b|$.*

q – неповна частка, r – остача.

Доведення. Доведемо спочатку існування q і r. Якщо $a = 0$, то підходять $q = r = 0$. Далі здійснимо доведення за індукцією. Спочатку розглянемо випадок $a \geq 0$ і $b > 0$. База індукції: нехай $a < b$, тоді очевидно $a = 0b + a$.

Якщо $a \geq b$, то знайдеться $n \in \mathbb{N}$ таке, що $0 \leq a - nb < b$ і, отже, за припущенням індукції існують q_1 і r_1 такі, що $a - nb = bq_1 + r_1$ і $0 \leq r_1 < b$. Звідки $a = qb + r$, де $q = q_1 + n$, $r = r_1$.

Якщо $a \leq 0$ і $b > 0$, то за доведеним існують q і r такі, що $-a = bq + r$, $0 \leq r < b$. Звідки $a = -bq - r$, тобто, $a = -b(q + 1) + b - r$, де $0 \leq b - r < b$.

Вправа 1.2. Випадки, коли $a \geq 0$ і $b < 0$ та $a \leq 0$ і $b < 0$ розгляньте самостійно.

Доведемо єдиність. Від зворотного – нехай існує дві пари q і r та q_1 і r_1, що $a = bq + r = bq_1 + r_1$, *де* $0 \leq r, r_1 < |b|$. Звідки $b(q - q_1) = r_1 - r$. Тобто, $|r_1 - r| < |b|$ і при цьому $r_1 - r$ ділиться на b, що можливо тільки при $r_1 - r = 0$. А це означає, що $r_1 = r$ та $q = q_1$.

Найбільший спільний дільник

Означення 1.3. *Нехай $a, b \in \mathbb{Z}$. Тоді $d \in \mathbb{N}$ називається найбільшим спільним дільником чисел a і b, якщо:*

1) $a \vdots d$ *і* $b \vdots d$;
2) *Якщо деяке число $d' \in \mathbb{N}$ таке, що $a \vdots d'$ і $b \vdots d'$, то $d \vdots d'$.*

Позначається найбільший спільний дільник чисел a і b через $\text{НСД}(a, b)$, або просто (a, b). Очевидно, що $\text{НСД}(a, b) = \text{НСД}(b, a)$. Слід відзначити, що $\text{НСД}(0,0)$ невизначений.

Означення 1.3. *Два цілих числа a і b називають взаємно простими, якщо* $\text{НСД}(a, b) = 1$.

Найбільший спільний дільник знаходиться за допомогою алгоритму Евкліда:

Розглянемо таку послідовність ділення з остачею:

$$a = bq_0 + r_1, \qquad 0 \leq r_1 < |b| \tag{1.2}$$

$$b = r_1 q_1 + r_2, \qquad 0 \leq r_2 < r_1 \tag{1.3}$$

$$r_1 = r_2 q_2 + r_3, \qquad 0 \leq r_3 < r_2$$

– – – – – – – – – – – – –

$$r_{s-1} = r_s q_s + r_{s+1}, \qquad 0 \le r_{s+1} < r_s. \tag{1.4}$$

Оскільки $|b| > r_1 > r_2 > \cdots > r_s$ і r_i – натуральні, то на деякому кроці остача буде нуль. Нехай

$$r_s = r_{s+1} q_{s+1}. \tag{1.5}$$

Теорема 2.1. $r_{s+1} = \text{НСД}(a, b)$.

Доведення. Покажемо, що r_{s+1} ділить a і b. Із (1.5) випливає, що $r_{s+1} | r_s$. Із (1.4) та (1.5) маємо $r_{s-1} = r_{s+1} q_{s+1} q_s + r_{s+1} = r_{s+1}(q_{s+1} q_s + 1)$, отже, $r_{s+1} | r_{s-1}$. І т. д., зрештою $r_{s+1} | r_2$ та $r_{s+1} | r_1$ звідки із (1.3) випливає $r_{s+1} | b$, а із (1.2) випливає $r_{s+1} | a$.

Отже, r_{s+1} дільник a і b. Залишилось показати, що це найбільший спільний дільник. Нехай число $d' \in \mathbb{N}$ таке, що $d' | a$ і $d' | b$, тобто, існують $k, l \in \mathbb{Z}$, що $a = kd'$ і $b = ld'$. Звідки із (1.2) випливає, що $(k - lq_1)d' = r_1$, тобто, $d' | r_1$. Далі, із $d' | b$ та $d' | r_1$ та рівняння (1.3) випливає $d' | r_2$ і т. д. Продовжуючи цей процес отримаємо $d' | r_{s-1}$ та $d' | r_s$, звідки, з урахуванням (1.4) $d' | r_{s+1}$, тобто за означенням $r_{s+1} = \text{НСД}(a, b)$.

Теорема 2.2. *Якщо* $d = \text{НСД}(a, b)$, *то існують цілі числа* u, v *такі, що*

$$au + bv = d.$$

Доведення. Використовуючи рівності в алгоритмі Евкліда згори до низу, маємо із (1.2)

$$r_1 = a - bq_0 = au_1 + bv_1, \qquad u_1 = 1, \qquad v_1 = -q_1,$$

із (1.3) випливає

$$r_2 = b - r_1 q_1 = b - (au_1 + bv_1)q_1 = au_2 + bv_2,$$

і т. д. Із (1.4) випливає

$$r_{s+1} = r_{s-1} - r_s q_s = au_{s-1} + bv_{s-1} - (au_s + bv_s)q_s = au_{s+1} + bv_{s+1}.$$

Наслідок 1.1. *Якщо числа a і b взаємно прості, то існують цілі числа u, v такі, що*

$$au + bv = 1.$$

ЛЕКЦІЯ 2. **БАЗОВІ ВЛАСТИВОСТІ** НСД **ТА** НСК**. ЛАНЦЮГОВІ ДРОБИ**

Означення 2.1. *Найменше спільне кратне (НСК) двох цілих чисел – це найменше натуральне число, яке є кратним обох цих чисел.*

Найменше спільне кратне чисел a і b позначають $\text{НСК}(a, b)$, або $[a, b]$.

Для будь-якого цілого a $\text{НСК}(a, 0)$ невизначене. Якщо $a \neq 0$, то $\text{НСК}(a, 1) = |a|$. Очевидно, що $\text{НСК}(a, b) = \text{НСК}(b, a)$.

Нехай $a, b \in \mathbb{N}$, для знаходження $\text{НСК}(a, b)$ скористаємось узагальненим розкладом на прості множники, який полягає в тому, що степені простих чисел можуть бути нульовими, тоді довільні натуральні a і b можна зобразити у вигляді

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \qquad \alpha_i \geq 0,$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \qquad \beta_i \geq 0\,.$$

Легко бачити, що у цьому випадку

$$\text{НСК}(a, b) = p_1^{max(\alpha_1, \beta_1)} p_2^{max(\alpha_2, \beta_2)} \dots p_k^{max(\alpha_k, \beta_k)}. \tag{2.1}$$

А найбільший спільний дільник a і b визначається за формулою

$$\text{НСД}(a, b) = p_1^{min(\alpha_1, \beta_1)} p_2^{min(\alpha_2, \beta_2)} \dots p_k^{min(\alpha_k, \beta_k)}. \tag{2.2}$$

Вправа 2.1. Довести властивості

1. $1 \leq \text{НСД}(a, b) \leq min(|a|, |b|) \leq \text{НСК}(a, b) \leq |ab|$;
2. $\text{НСД}\big(a, \text{НСД}(b, c)\big) = \text{НСД}(\text{НСД}(a, b), c)$;
3. $\text{НСД}(a, b, c, d) = \text{НСД}\big(\text{НСД}(a, b), \text{НСД}(c, d)\big)$;
4. Довести, що $\text{НСК}(a, b)$ ділить будь-яке кратне чисел a і b;

5. $\text{НСК}(ac, bc) = c\text{НСК}(a, b)$ для будь-якого натурального числа c.

Теорема 2.3. *Нехай* $a, b \in \mathbb{Z}$, *причому* $a \neq 0$ і $b \neq 0$. *Тоді має місце рівність*

$$\text{НСК}(a, b)\text{НСД}(a, b) = |ab|. \qquad (2.3)$$

Доведення. Якщо $a, b \in \mathbb{N}$, то рівність (2.3) є наслідком (2.1), (2.2) та очевидної рівності

$$max(\alpha_i, \beta_i) + min(\alpha_i, \beta_i) = \alpha_i + \beta_i, \qquad i = 1,2, \dots, k.$$

Якщо $a, b \in \mathbb{Z}$, то легко переконатись, що $\text{НСК}(a, b) = \text{НСК}(|a|, |b|)$, $\text{НСД}(a, b) = \text{НСД}(|a|, |b|)$. Отже,

$$\text{НСК}(a, b)\text{НСД}(a, b) = \text{НСК}(|a|, |b|)\text{НСД}(|a|, |b|) = |ab|.$$

Ланцюгові дроби

Нехай $r \in \mathbb{R}$. Легко бачити, що це число можна подати у вигляді

$$r = a_0 + \beta_1,$$

де $a_0 \in \mathbb{Z}$, $0 \leq \beta_1 < 1$.

Якщо $\beta_1 = 0$, то процес зупиняється, а якщо $\beta_1 > 0$, то $\frac{1}{\beta_1}$ можна подати у вигляді $\frac{1}{\beta_1} = a_1 + \beta_2$, де $a_1 \in \mathbb{N}$, $0 \leq \beta_2 < 1$, звідки маємо

$$r = a_0 + \frac{1}{1/\beta_1} = a_0 + \frac{1}{a_1 + \beta_2}.$$

Якщо $\beta_2 = 0$, то процес зупиняється, а якщо $\beta_2 > 0$, то в свою чергу $\frac{1}{\beta_2}$ можна подати у вигляді $\frac{1}{\beta_2} = a_2 + \beta_3$, де $a_2 \in \mathbb{N}$, $0 \leq \beta_3 < 1$, звідки

$$r = a_0 + \frac{1}{a_1 + \beta_2} = a_0 + \frac{1}{a_1 + \frac{1}{1/\beta_2}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \beta_3}}.$$

Цей процес може продовжуватись до моменту, коли на якомусь n-тому кроці $\beta_n = 0$, або ж продовжуватись до нескінченності, якщо $\beta_n > 0$ для всіх $n \in \mathbb{N}$. Така конструкція (скінченна чи нескінченна) називається ланцюговим дробом.

Скінченний ланцюговий дріб

$$c = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

де $a_0 \in \mathbb{Z}$, $a_k \in \mathbb{N}$, $k = 1, \dots, n-1$, $a_n \geq 2$ позначається так:

$$c = [a_0; a_1, \dots, a_n].$$

Легко бачити, що довільний скінченний ланцюговий дріб зображає раціональне число. Має місце і зворотне твердження:

Теорема 2.4. *Будь-яке раціональне число можна єдиним чином зобразити у вигляді скінченного ланцюгового дробу.*

Доведення. Нехай $c = \frac{a}{b} \in \mathbb{Q}$ – нескоротний дріб, де $b > 0$. Як і в алгоритмі Евкліда розглянемо таку послідовність ділення з остачею $a = bq_0 + r_1,\ 0 \leq r_1 < b$, $b = r_1q_1 + r_2,\ 0 \leq r_2 < r_1$, $r_1 = r_2q_2 + r_3,\ 0 \leq r_3 < r_2$,…, $r_{n-1} = r_nq_n$.

Тоді

$$c = \frac{bq_0 + r_1}{b} = q_0 + \frac{r_1}{b} = q_0 + \frac{1}{\frac{b}{r_1}} = q_0 + \frac{1}{q_1 + \frac{r_2}{r_1}} = q_0 + \frac{1}{q_1 + \frac{1}{r_1/r_2}}$$

$$= q_0 + \frac{1}{q_1 + \frac{1}{q_2 + r_3/r_2}} = \dots = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}$$

Тобто $c = [q_0; q_1, \dots, q_n]$. Єдиність такого зображення випливає з однозначності (єдиності частки та остачі) ділення з остачею та алгоритму Евкліда.

Означення 2.2. *Будемо казати, що* $\alpha \in \mathbb{R}$ *записується у вигляді нескінченного ланцюгового дробу* $\alpha = [a_0; a_1, \dots, a_n, \dots]$*, якщо для скінченних ланцюгових дробів* $\frac{P_n}{Q_n} = [a_0; a_1, \dots, a_n]$, $P_n \in \mathbb{Z}$, $Q_n \in \mathbb{N}$, $n \geq 0$, *має місце* $\lim\limits_{n\to\infty} \frac{P_n}{Q_n} = \alpha$. *Дріб* $\frac{P_n}{Q_n} = [a_0; a_1, \dots, a_n]$ *називається* n*-тим підхідним для* α.

Властивості скінченних підхідних ланцюгових дробів:

1. Для обчислення P_n та Q_n ланцюгового дробу $\frac{P_n}{Q_n} = [a_0; a_1, \dots, a_n]$ можна використати такі рекурентні співвідношення для цілих $k \geq 0$:

$$\begin{aligned} P_{k+1} &= a_{k+1}P_k + P_{k-1}, \\ Q_{k+1} &= a_{k+1}Q_k + Q_{k-1}, \end{aligned} \tag{2.4}$$

де $P_{-1} = 1$, $Q_{-1} = 0$, $P_0 = a_0$, $Q_0 = 1$.

Доведення. Доведемо за індукцією. Для $k = 0$ маємо

$$P_1 = a_1 a_0 + 1,$$

$$Q_1 = a_1.$$

Тобто $\frac{P_1}{Q_1} = [a_0; a_1] = a_0 + \frac{1}{a_1}$, що правильно. Припустимо, що (2.4) має місце при деякому $l \in \mathbb{N}$, тобто

$$\frac{P_l}{Q_l} = \frac{a_l P_{l-1} + P_{l-2}}{a_l Q_{l-1} + Q_{l-2}} = [a_0; a_1, \dots, a_{l-1}, a_l]. \tag{2.5}$$

Легко бачити, що $\frac{P_{l+1}}{Q_{l+1}} = [a_0; a_1, \dots, a_l, a_{l+1}] = \left[a_0; a_1, \dots, a_{l-1}, a_l + \frac{1}{a_{l+1}}\right]$.

Зауваження. В останній рівності $[a_0; a_1, \dots, a_l, a_{l+1}]$ розглядається як функція аргументів $a_0, a_1, \dots, a_l, a_{l+1}$.

Звідки, з використанням (2.5), маємо

$$\frac{P_{l+1}}{Q_{l+1}} = \left[a_0; a_1, \dots, a_{l-1}, a_l + \frac{1}{a_{l+1}}\right] = \frac{\left(a_l + \frac{1}{a_{l+1}}\right)P_{l-1} + P_{l-2}}{\left(a_l + \frac{1}{a_{l+1}}\right)Q_{l-1} + Q_{l-2}}$$

$$= \frac{a_l P_{l-1} + P_{l-2} + \frac{1}{a_{l+1}}P_{l-1}}{a_l Q_{l-1} + Q_{l-2} + \frac{1}{a_{l+1}}Q_{l-1}} = \frac{a_{l+1}P_l + P_{l-1}}{a_{l+1}Q_l + Q_{l-1}}.$$

2. Для всіх $k \geq 0$ має місце рівність $P_k Q_{k-1} - P_{k-1}Q_k = (-1)^{k+1}$.

Вправа 2.2. Довести властивість 2 за допомогою математичної індукції.

3. $Q_k \geq 2^{k/2}$ для парних $k \geq 0$ і $Q_k \geq 2^{(k-1)/2}$ для непарних $k \in \mathbb{N}$.

   Дійсно, із $Q_k = a_k Q_{k-1} + Q_{k-2}$, $Q_{k-1} \geq Q_{k-2}$ і $a_k \geq 1$ випливає $Q_k \geq Q_{k-1} + Q_{k-2} \geq 2Q_{k-2}$. Отже, $Q_k \geq 2Q_{k-2} \geq 2^2 Q_{k-4} \geq \cdots$.

4. Для довільного нескінченного ланцюгового дробу $[a_0; a_1, \dots, a_n, \dots]$, парні підхідні дроби зростають $\frac{P_{2k}}{Q_{2k}} < \frac{P_{2k+2}}{Q_{2k+2}}$, а непарні спадають $\frac{P_{2k+1}}{Q_{2k+1}} < \frac{P_{2k+3}}{Q_{2k+3}}$, $k = 0,1,2,\dots$ і, отже, ми маємо послідовність вкладених відрізків $\left[\frac{P_{2k}}{Q_{2k}}, \frac{P_{2k+1}}{Q_{2k+1}}\right]$, довжина яких прямує до нуля при $k \to \infty$. За теоремою про вкладені відрізки (принцип вкладених відрізків Коші — Кантора) будь-яка послідовність вкладених відрізків на дійсній прямій, довжина яких прямує до нуля, має єдину спільну точку, яка відповідає ірраціональному числу, що є значенням нескінченного ланцюгового дробу $[a_0; a_1, \dots, a_n, \dots]$.

   Доведемо властивість 4. Для довільного $k \geq 1$ помножимо формули (2.4) відповідно на Q_{k-1} та P_{k-1} і віднімемо другу від першої, маємо

$$\begin{aligned} P_{k+1}Q_{k-1} - Q_{k+1}P_{k-1} &= a_{k+1}(P_k Q_{k-1} - P_{k-1}Q_k) \\ &= (-1)^{k+1}a_{k+1}. \end{aligned} \tag{2.6}$$

   З урахуванням того, що $a_{k+1} > 0$ та $Q_{k-1}Q_{k+1} > 0$ для $k \geq 1$, ділення (2.6) на $Q_{k-1}Q_{k+1}$ завершує доведення.

5. Підхідний дріб $\frac{P_n}{Q_n} = [a_0; a_1, \dots, a_n]$ наближає число $\alpha = [a_0; a_1, \dots, a_n, \dots]$ з точністю $\left|\alpha - \frac{P_n}{Q_n}\right| \leq \frac{1}{Q_n Q_{n+1}}$.

Дійсно, з урахуванням властивості 2, для $k \in \mathbb{N}$ маємо

$$\left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| = \frac{|P_{k+1}Q_k - P_k Q_{k+1}|}{Q_k Q_{k+1}} \leq \frac{1}{Q_k Q_{k+1}}.$$

Звідки, беручи до уваги властивість 4, одержуємо

$$\left|\alpha - \frac{P_n}{Q_n}\right| \leq \left|\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right| = \frac{|P_n Q_{n+1} - Q_n P_{n+1}|}{Q_n Q_{n+1}} \leq \frac{1}{Q_n Q_{n+1}}.$$

Із властивості 3 випливає, що $Q_k Q_{k+1} \to \infty$ при $k \to \infty$, отже, $\left|\frac{P_{k+1}}{Q_{k+1}} - \frac{P_k}{Q_k}\right| \to 0$ при $k \to \infty$.

Крім цього, враховуючи нерівність $Q_n Q_{n+1} \geq 2^n$, маємо

$$\left|\alpha - \frac{P_n}{Q_n}\right| \leq \frac{1}{2^n}, \quad n \geq 1.$$

ЛЕКЦІЯ 3. **РІВНІСТЬ ЗА МОДУЛЕМ. МАЛА ТЕОРЕМА ФЕРМА**

Означення 3.1. *Нехай $n \in \mathbb{N}$. Цілі числа a і b називаються рівними (конгруентними) за модулем n, якщо $a - b$ ділиться на n.*

Позначається $a \equiv b \pmod{n}$.

Лема 3.1. *Якщо $a \equiv b \pmod{n}$ та $c \equiv d \pmod{n}$, то*

1. $a + c \equiv b + d \pmod{n}$;
2. $ac \equiv bd \pmod{n}$.

Доведення. Оскільки $a \equiv b \pmod{n}$, то існує $l \in \mathbb{Z}$ таке, що $a - b = ln$, а із $c \equiv d \pmod{n}$ випливає, що існує $k \in \mathbb{Z}$ таке, що $c - d = kn$. Звідки

$$a + c - (b + d) = a - b + c - d = (l + k)n,$$

Отже, $a + c \equiv b + d \pmod{n}$.

Далі,

$$ac - bd = ac - ad + ad - bd = a(c - d) + (a - b)d = akn + lnd$$
$$= (ak + ld)n.$$

Тобто, $ac \equiv bd \pmod{n}$.

Наслідок 3.1. Оскільки $\forall m \in \mathbb{Z}$, $m \equiv m \pmod{n}$, то, із $a \equiv b \pmod{n}$ випливає

$$am \equiv bm \pmod{n}.$$

Чи завжди із того, що $am \equiv bm \pmod{n}$ випливає $a \equiv b \pmod{n}$? Ні, наприклад, $2 \cdot 4 = 8 \equiv 12 = 3 \cdot 4 \pmod{4}$, але $2 \not\equiv 3 \pmod{4}$. Скорочувати на m в рівності $am \equiv bm \pmod{n}$ можна у випадку, коли $\text{НСД}(m, n) = 1$. Дійсно, із того, що $(a - b)m$ ділиться на n і при цьому $\text{НСД}(m, n) = 1$ випливає, що $a - b$ ділиться на n, тобто, $a \equiv b \pmod{n}$.

Теорема 3.1. (мала теорема Ферма) *Нехай p – просте число, $a \in \mathbb{N}$ і* $\text{НСД}(a, p) = 1$. *Тоді*

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

Доведення. Розглянемо систему еквіваленцій

$$\begin{aligned} &a \equiv r_1 \pmod{p};\\ &2a \equiv r_2 \pmod{p};\\ &\quad - - -\\ &(p-1)a \equiv r_{p-1} \pmod{p}, \end{aligned} \tag{3.1}$$

де r_i – остача від ділення ia на p. Покажемо, що $r_i \neq r_j$, якщо $i \neq j$. Дійсно, нехай $r_i = r_j$, тоді $ia - ja$ ділиться на p. Але $\text{НСД}(a, p) = 1$, отже, $i - j$ ділиться на p, причому $|i - j| < p$, а це можливо, коли $i = j$.

Легко переконатись, що $0 < r_i \leq p - 1$, $i = 1,2, \dots, p - 1$ і, значить, ці остачі пробігають всі значення від 1 до $p - 1$, тобто, $r_1 r_2 \dots r_{p-1} = (p - 1)!$

Згідно леми 3.1, перемноживши всі еквіваленції системи (3.1), маємо

$$(p-1)!\,a^{p-1} \equiv (p-1)!\pmod{p},$$

Оскільки $(p-1)!$ взаємно просте з p, то на нього можна скоротити і одержимо твердження теореми.

Відношення рівності за модулем $\equiv$ є відношенням еквівалентності, тобто,

1. $\forall a \in \mathbb{Z}\ \ a \equiv a \pmod{n}$;
2. $\forall a, b \in \mathbb{Z}$, *якщо* $a \equiv b \pmod{n}$, *то* $b \equiv a \pmod{n}$;
3. $\forall a, b, c \in \mathbb{Z}$ *із того, що* $a \equiv b \pmod{n}$ *та* $b \equiv c \pmod{n}$ *випливає* $a \equiv c \pmod{n}$.

Вправа 3.1. Довести властивості 1-3.

Цілі числа $\mathbb{Z}$ розбиваються відношенням $\equiv$ на $n-1$ клас еквівалентності:

$$\bar{a} = \{a, a \pm n, a \pm 2n, \dots,\}, \qquad a = 0,1, \dots, n-1.$$

Множина класів еквівалентності за модулем n позначається $\mathbb{Z}/n\mathbb{Z}$, (інколи вона називається множина класів лишків за модулем n), отже,

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

На множині класів еквівалентності за модулем n $\mathbb{Z}/n\mathbb{Z}$ введемо операцію додавання $+$:

$$\bar{a} + \bar{b} := \overline{a+b}$$

та множення $\cdot$:

$$\bar{a} \cdot \bar{b} := \overline{a \cdot b}$$

Очевидні такі основні властивості додавання і множення на множині класів еквівалентності:

a) $\bar{a} + \bar{b} = \bar{b} + \bar{a}$;

b) $\bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}$;

c) $\bar{a} + \bar{0} = \bar{a} = \bar{0} + \bar{a}$;

d) Для довільного $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ існує $\bar{x} = \overline{n-a} \in \mathbb{Z}/n\mathbb{Z}$ такий, що

$$\bar{a} + \bar{x} = \bar{0};$$

e) $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$;

f) $\bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$;

g) $\bar{a} \cdot \bar{1} = \bar{a}$.

Застосування еквіваленцій за модулем для доведення ознак подільності

Введемо такі позначення: нехай натуральне число N має вигляд

$$N = a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n,$$

де a_k – цифри від 0 до 9 і $a_n \neq 0$. Тоді N будемо записувати у вигляді

$$N = \overline{a_n \dots a_1 a_0}.$$

Твердження 3.1. *Остаток від ділення натурального числа N на* 3 *чи на* 9 *дорівнює остатку від ділення на 3 чи на 9 суми цифр цього числа.*

Доведення. Нехай $N = \overline{a_n \dots a_1 a_0}$. Тоді, оскільки $10 \equiv 1 \pmod 3$ та $10 \equiv 1 \pmod 9$, з урахуванням леми 3.1, маємо

$$\begin{aligned} N &= a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \\ &\equiv a_0 + a_1 + a_2 + \cdots + a_n, \end{aligned} \tag{3.2}$$

Отже, остача від ділення на 3 та на 9 числа N та суми його цифр $a_0 + a_1 + a_2 + \cdots + a_n$ однакова. Зокрема, якщо N ділиться націло на 3 чи на 9, то й суми його цифр ділиться націло на 3 чи на 9 і навпаки, якщо суми його цифр N ділиться націло на 3 чи на 9, то й N ділиться націло на 3 чи на 9.

Твердження 3.2. *Остаток від ділення натурального числа $N = \overline{a_n \dots a_1 a_0}$ на* 11 *дорівнює остатку від ділення на* 11 *знакозмінної суми $a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^n a_n$ цифр цього числа*

Доведення. Нехай $N = \overline{a_n \dots a_1 a_0}$. Тоді оскільки $10^k \equiv -1 \pmod{11}$, якщо k непарне і $10^k \equiv 1 \pmod{11}$, якщо k непарне, зокрема, $10 \equiv -1 \pmod{11}$, $100 \equiv 1 \pmod{11}$ і т. д., то, з урахуванням леми 3.1, маємо

$$N = a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n \qquad (3.3)$$
$$\equiv a_0 - a_1 + a_2 + \cdots + (-1)^n a_n \pmod{11}$$

Отже, остача від ділення числа N на 11 та знакозмінної суми його цифр однакова. Зокрема, якщо N ділиться націло на 11, то й знакозмінна сума його цифр ділиться націло на 11 і навпаки, якщо знакозмінна сума цифр N ділиться націло на 11, то й N ділиться націло на 11.

Вправа 3.1. Застосовуючи властивості еквіваленцій, вивести ознаки ділення на 4, 5, 7, 8, 13.

ЛЕКЦІЯ 4. ФОРМУЛА ВКЛЮЧЕННЯ-ВИКЛЮЧЕННЯ. ФУНКЦІЯ ОЙЛЕРА

Нехай A – деяка скінченна множина. Через $|A|$ будемо позначати кількість елементів цієї множини. Відзначимо, що у деяких підручниках кількість елементів множини A позначається через $N(A)$.

Твердження 4.1. *Нехай $A_1, A_2, \ldots, A_n$ – набір із n скінченних множин, тоді*

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|. \qquad (4.1)$$

Формула (4.1) називається формулою (або методом) включення-виключення.

Доведення. При $n = 2$ формула (4.1) очевидна. Дійсно,

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|, \qquad (4.2)$$

оскільки сума $|A_1| + |A_2|$ двічі враховує спільну кількість елементів множин A_1 та A_2, тобто, кількість елементів множини $A_1 \cap A_2$.

Використовуючи формулу (4.2) одержуємо формулу

$$|A_1 \cup A_2 \cup A_3|$$
$$= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_2|$$
$$+ |A_1 \cap A_2 \cap A_3|.$$

Дійсно,

$$|A_1 \cup A_2 \cup A_3| = |A_1 \cup (A_2 \cup A_3)| = |A_1| + |A_2 \cup A_3| - |A_1 \cap (A_2 \cup A_3)|$$
$$= |A_1| + |A_2| + |A_3| - |A_2 \cap A_3| - |(A_1 \cap A_2) \cup (A_1 \cap A_3)|$$
$$= |A_1| + |A_2| + |A_3| - |A_2 \cap A_2| - |A_1 \cap A_2| - |A_1 \cap A_3|$$
$$+ |(A_1 \cap A_2) \cap (A_1 \cap A_3)|.$$

Очевидна рівність $(A_1 \cap A_2) \cap (A_1 \cap A_3) = A_1 \cap A_2 \cap A_3$ завершує доведення.

У загальному формула (4.1) доводиться методом математичної індукції.

Нехай (4.1) виконується для $n-1$, тобто,

$$|A_1 \cup A_2 \cup \ldots \cup A_{n-1}|$$
$$= \sum_{i=1}^{n-1} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \cdots$$
$$+ (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_{n-1}|.$$

Тоді, використовуючи (4.2), маємо

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = |A_1 \cup A_2 \cup \ldots \cup A_{n-1}| + |A_n| - |A_1 \cup \ldots \cup A_{n-1} \cap A_n|$$
$$= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n-1} |A_i \cap A_j \cap A_k| \ldots$$
$$+ (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_{n-1}| - |(A_1 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n)|$$
$$= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n-1} |A_i \cap A_j \cap A_k| + \cdots$$
$$+ (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_{n-1}|$$
$$- \sum_{k=1}^{n-1} |A_k \cap A_n| + \sum_{1 \le l < m \le n-1} |(A_l \cap A_n) \cap (A_m \cap A_n)| - \cdots$$
$$+ (-1)^{n+1} |(A_1 \cap A_n) \cap (A_2 \cap A_n) \cap \ldots \cap (A_{n-1} \cap A_n)|.$$

Доведення завершується з урахуванням того, що

$$\sum_{1\le l<m\le n-1} |(A_l \cap A_n) \cap (A_m \cap A_n)| = \sum_{1\le l<m\le n-1} |A_l \cap A_m \cap A_n|,$$

– – – – – – – – – – – – – – –

$$|(A_1 \cap A_n) \cap (A_2 \cap A_n) \cap \dots \cap (A_{n-1} \cap A_n)| = |A_1 \cap A_2 \cap \dots \cap A_{n-1} \cap A_n|.$$

Теорема 4.1. *Нехай* $n, a_1, a_2, \dots, a_m \in \mathbb{N}$, *причому* $a_1, a_2, \dots, a_m$ *взаємно прості, тобто,* $\text{НСД}(a_i, a_j) = 1$, $i \ne j$. *Тоді число натуральних* $k: 1 \le k \le m$, *які не діляться на жодне із* $a_1, a_2, \dots, a_m$, *дорівнює*

$$n - \sum_{i=1}^{n} \left[\frac{n}{a_i}\right] + \sum_{1\le i<j\le n} \left[\frac{n}{a_i a_j}\right] - \dots + (-1)^m \left[\frac{n}{a_1\ a_2 \dots a_m}\right]. \qquad (4.3)$$

Доведення. Нехай A_i – множина чисел, які діляться на a_i. Тоді для довільних натуральних $1 \le i_1 < i_2 < \dots < i_r \le m$.

$$|A_i| = \left[\frac{n}{a_i}\right], \left|A_{i_1} \cap A_{i_2}\right| = \left[\frac{n}{a_{i_1}\ a_{i_2}}\right], \dots, \left|A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_r}\right| = \left[\frac{n}{a_{i_1}\ a_{i_2} \dots a_{i_r}}\right]. \qquad (4.4)$$

Легко бачити, що число натуральних $k: 1 \le k \le m$, які діляться хоча б на одне із чисел $a_1, a_2, \dots, a_m$, дорівнює $|\bigcup_{i=1}^{m} A_i|$.

За формулою включення виключення, з урахуванням (4.4), маємо

$$\left|\bigcup_{i=1}^{m} A_i\right| = \sum_{i=1}^{n} \left[\frac{n}{a_i}\right] - \sum_{1\le i<j\le n} \left[\frac{n}{a_i a_j}\right] + \dots + (-1)^{m+1} \left[\frac{n}{a_1\ a_2 \dots a_m}\right].$$

Звідки число натуральних $k: 1 \le k \le m$, які не діляться на жодне із $a_1, a_2, \dots, a_m$, дорівнює

$$n - \left|\bigcup_{i=1}^{m} A_i\right| = n - \sum_{i=1}^{n} \left[\frac{n}{a_i}\right] + \sum_{1\le i<j\le n} \left[\frac{n}{a_i a_j}\right] - \dots + (-1)^m \left[\frac{n}{a_1\ a_2 \dots a_m}\right].$$

Означення 4.1. *Нехай* $n \in \mathbb{N}$. *Позначимо через* $\varphi(n)$ *– число натуральних* $k: 1 \le k \le n$, *таких, що* k *взаємно просте з* n. *Функція* $\varphi(n)$ *називається функцією Ойлера.*

Теорема 4.2. *Нехай* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ *– канонічний розклад натурального числа* n *на прості множники. Тоді*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

Доведення. Для $m = 2$ маємо $n = p_1^{\alpha_1} p_2^{\alpha_2}$. Взаємно простими з n будуть числа, які не діляться ні на p_1, ні на p_2. Покладемо у формулі (4.3) $a_1 = p_1$, $a_2 = p_2$. Тоді

$$\varphi(n) = n - \left(\frac{n}{p_1} + \frac{n}{p_2}\right) + \frac{n}{p_1 p_2} = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right).$$

У загальному випадку покладаємо $a_1 = p_1$, $a_2 = p_2$,…, $a_m = p_m$. Тоді із формули (4.3) маємо

$$\varphi(n) = n - \sum_{i=1}^{m} \frac{n}{p_i} + \sum_{1 \le i < j \le n} \frac{n}{p_i p_j} - \dots + (-1)^m \frac{n}{p_1\, p_2 \dots p_m}$$
$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

Вправа 4.1. Довести теорему Вільсона: *Число* $p \in \mathbb{N}$ *просте тоді і тільки тоді, коли* $(p-1)! = -1 \pmod p$.

ЛЕКЦІЯ 5. ТЕОРЕМА ОЙЛЕРА. КИТАЙСЬКА ТЕОРЕМА ПРО ЛИШКИ

Означення 5.1. *Функція* $f(n)$, $n \in \mathbb{N}$, *називається мультиплікативною, якщо* $\forall a, b \in \mathbb{N}$, *таких, що* $\text{НСД}(a, b) = 1$,

$$f(ab) = f(a) f(b).$$

Теорема 5.1. *Функція Ойлера мультиплікативна.*

Доведення. Нехай $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, $b = q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}$. Оскільки $\text{НСД}(a, b) = 1$, то $p_i \neq q_j$, $i = 1, \dots, m$, $j = 1, \dots, l$.

$$\varphi(ab) = ab\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_m}\right)\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right)\dots\left(1 - \frac{1}{q_l}\right)$$
$$= a\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_m}\right) b\left(1 - \frac{1}{q_1}\right)\dots\left(1 - \frac{1}{q_l}\right) = \varphi(a)\varphi(b).$$

Теорема 5.2 (Ойлер) *Нехай* $a, n \in \mathbb{N}$ *і* $\text{НСД}(a, n) = 1$. *Тоді*

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

Доведення. Позначимо натуральні числа менші від n і взаємно прості з ним так: k_1, k_2, …, $k_{\varphi(n)}$. Із означення функції Ойлера їх кількість дорівнює $\varphi(n)$. Нехай r_i є остачею від ділення ak_i на n, тобто $ak_i \equiv r_i \pmod{n}$. Покажемо, що $r_i \neq r_j$, якщо $i \neq j$. Дійсно, припустимо, що для деяких l та m

$ak_l \equiv r$ і $ak_m \equiv r \pmod{n}$. Тоді $ak_l \equiv ak_m \pmod{n}$.

Оскільки $\text{НСД}(a, n) = 1$, то на a можна скоротити, тобто, $k_l \equiv k_m \pmod{n}$, звідки $k_l = k_m$ (переконайтесь). Покажемо, що множина чисел r_1, r_2, …, $r_{\varphi(n)}$ і множина k_1, k_2, …, $k_{\varphi(n)}$ це одна і та ж множина (можливо перемішана). Дійсно, нехай для деякого l $ak_l \equiv r_l \pmod{n}$, тоді існує натуральне c таке, що $ak_l - r_l = cn$, причому $\text{НСД}(r_l, n) = 1$, оскільки в противному разі (якщо $\text{НСД}(r_l, n) = d > 1$) ak_l ділиться на d. Далі, враховуючи $\text{НСД}(a, n) = 1$, маємо k_l ділиться на d, що неможливо за означенням чисел k_l.

Тобто, $1 \leq r_l < n$ і r_l взаємно просте з n для всіх $l = 1, 2, \dots, \varphi(n)$, а це і є числа k_1, k_2, …, $k_{\varphi(n)}$, звідки

$$k_1 k_2 \dots k_{\varphi(n)} = r_1 r_2 \dots r_{\varphi(n)}. \qquad (5.1)$$

Згідно леми 3.1, перемноживши всі еквіваленції $ak_i \equiv r_i \pmod{n}$, по всіх $i = 1,2, \dots, \varphi(n)$ з урахуванням (5.1), маємо

$$k_1 k_2 \dots k_{\varphi(n)} a^{\varphi(n)} \equiv k_1 k_2 \dots k_{\varphi(n)} \pmod{n},$$

Легко бачити, що добуток $k_1k_2 \dots k_{\varphi(n)}$ взаємно простий з n, оскільки кожен його множник взаємно простий з n і тому можна скоротити на цей добуток, тобто, маємо $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Твердження 5.1. *Якщо* $x \equiv y \ (mod\ \varphi(n))$, *то* $a^x \equiv a^y \ (mod\ n)$, *якщо* a *взаємно просте з* n.

Доведення. Дійсно, існує ціле k таке, що $x = y + k\varphi(n)$. Звідки

$$a^{y+k\varphi(n)} \equiv a^y \pmod{n},$$

Оскільки за теоремою Ойлера $a^{\varphi(n)} \equiv 1 \pmod{n}$, а, отже, і $a^{k\varphi(n)} \equiv 1 \pmod{n}$.

Алгоритм шифрування RSA (створили Rivest, Shamir, Adleman, 1977 р.)

1. Вибираються два досить великі різні прості числа p, q.
2. У якості модуля розглядаємо добуток $n = pq$.
3. Враховуючи мультиплікативність функції Ойлера, маємо
$$\varphi(n) = (p-1)(q-1).$$
4. Вибирається ціле число e взаємно просте з $\varphi(n)$ і $1 < e < \varphi(n)$, яке називають *відкритою експонентою*. Часто у якості e вибирають одне із простих чисел Ферма ($2^{2^k} + 1, k \in \mathbb{N}$).
5. Обчислюється число d обернене до e за модулем $\varphi(n)$, тобто
$$de \equiv 1 \pmod{\varphi(n)}.$$
Число d називають *секретною експонентою*.

Пара (e, n) грає роль відкритого ключа. Пара (d, n) є секретною. Числа p, q також секретні і після генерації ключів можуть бути знищеними.

Припустимо потрібно передати повідомлення, що є числом m, $(0 \le m \le n-1)$.

Шифрування повідомлення – зашифровуємо повідомлення m з використанням відкритого ключа (e, n): $c = E(m) \equiv m^e \pmod{n}$.

Дешифрування: Зашифроване повідомлення c передається адресату, який його розшифровує за допомогою секретного ключа (d, n): $m = D(c) \equiv c^d \pmod{n}$.

Дійсно, $c^d \equiv (m^e)^d \equiv m \pmod{n}$, з урахуванням того, що $de \equiv 1 \pmod{\varphi(n)}$ та твердження 5.1.

Теорема 5.2 (Китайська теорема про лишки)

Нехай натуральні числа $m_1, m_2, \ldots, m_n, n \in \mathbb{N}$ *попарно взаємно прості. Тоді система еквіваленцій*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\ldots \\ x &\equiv a_n \pmod{m_n}. \end{aligned} \tag{5.2}$$

Тоді існує розв'язок цієї системи єдиний з точністю до рівності за модулем $M = m_1 m_2 \ldots m_n$.

Доведення. Введемо величини $M_i = \frac{M}{m_i}$, $N_i \equiv M_i^{-1} \pmod{m_i}$, $i = 1, \ldots, n$. Зауважимо, що $M_i^{-1} \pmod{m_i}$ існує, оскільки M_i взаємно просте з m_i.

Розглянемо величину

$$x \equiv a_1 M_1 N_1 + a_2 M_2 N_2 + \cdots + a_n M_n N_n \pmod{M}.$$

Доданок $a_1 M_1 N_1 \equiv a_1 \pmod{m_1}$, а $a_i M_i N_i \equiv 0 \pmod{m_1}$, для всіх $i \neq 1$.

Аналогічно $a_2 M_2 N_2 \equiv a_2 \pmod{m_1}$, а $a_i M_i N_i \equiv 0 \pmod{m_1}$, для всіх $i \neq 2$ і так далі. Тобто, $x \equiv a_1 M_1 N_1 + a_2 M_2 N_2 + \cdots + a_n M_n N_n \pmod{M}$ задовольняє систему еквіваленцій (5.2).

Покажемо, що цей розв'язок єдиний за модулем M. Дійсно, якщо існує ще один розв'язок x' системи (5.2), тоді очевидно, що

$$x - x' \equiv 0 \pmod{m_1}$$

$$x - x' \equiv 0 \pmod{m_2}$$

– – – – –

$$x - x' \equiv 0 \pmod{m_n}.$$

А, значить $x - x' \equiv 0 \pmod{M}$, тобто,

$$x \equiv x' \pmod{M}.$$

Приклад

Знайти розв'язок системи

$$x \equiv 5 \pmod{2}$$

$$x \equiv 4 \pmod{5}$$

$$x \equiv 6 \pmod{7}.$$

Маємо $M = m_1 m_2 m_3 = 70$, $M_1 = 35$, $M_2 = 14$, $M_3 = 10$.

Легко бачити, що

$$N_1 \equiv M_1^{-1} \equiv 35^{-1} \equiv 1 \pmod{2}$$

$$N_2 \equiv M_2^{-1} \equiv 14^{-1} \equiv 4 \pmod{5}$$

$$N_3 \equiv M_3^{-1} \equiv 10^{-1} \equiv 5 \pmod{7}$$

Отже, розв'язок системи

$$x \equiv a_1 M_1 N_1 + a_2 M_2 N_2 + a_3 M_3 N_3 = 5 \cdot 35 + 4 \cdot 14 \cdot 4 + 6 \cdot 10 \cdot 5$$
$$\equiv 69 \pmod{70}.$$

ЛЕКЦІЯ 6. **КІЛЬЦЕ. ПРИКЛАДИ КІЛЕЦЬ**

Означення 6.1. *Множина $\mathcal{R} \neq \emptyset$ називається кільцем, якщо на ній визначені дві операції: додавання $+: \mathcal{R} \times \mathcal{R} \to \mathcal{R}$ та множення $\circ: \mathcal{R} \times \mathcal{R} \to \mathcal{R}$, причому $(\mathcal{R}, +)$ – абелева група, тобто*

a) $\forall x, y \in \mathcal{R},\ x + y = y + x$;

b) $\forall x, y, z \in \mathcal{R},\ (x + y) + z = x + (y + z)$;

c) $\exists 0 \in \mathcal{R}: \forall x \in \mathcal{R},\ x + 0 = x$;

d) $\forall x \in \mathcal{R}\ \exists(-x) \in \mathcal{R}:,\ x + (-x) = 0;$

і, крім цього, виконуються операції дистрибутивності:

$$x \circ (y + z) = x \circ y + x \circ z;$$

$$(x + y) \circ z = x \circ z + y \circ z.$$

Елемент 0 називається нейтральним елементом за додаванням (або нулем), а елемент $(-x)$ називається протилежним елементом до x.

Кільце позначається так: $(\mathcal{R}, +, \circ)$, або просто через $\mathcal{R}$, якщо операції додавання і множення на $\mathcal{R}$ не потребують уточнення.

Якщо множення $\circ$ асоціативне, тобто $x \circ (y \circ z) = (x \circ y) \circ z$, то кільце $(\mathcal{R}, +, \circ)$ називається *асоціативним*.

Твердження 6.1. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *– кільце, яке називається кільцем лишків за модулем* $n \in \mathbb{Z}$.

Доведення випливає із властивостей a) – f) операцій додавання і множення на $\mathbb{Z}/n\mathbb{Z}$ (див. Лекція 3).

Приклади

1. $(\mathbb{Z}, +, \cdot)$ – асоціативне кільце цілих чисел.
2. $(\mathbb{P}, +, \cdot)$ – асоціативне кільце парних чисел.
3. $(\mathbb{R}, +, \cdot)$ – асоціативне кільце дійсних чисел.
4. $(2^X, \Delta,\ \cap)$, (де операція симетричної різниці Δ виступає в якості додавання, а перетин $\cap$ – в якості множення) –Булеве кільце.
5. $(M_{n\times n}(\mathbb{R}), +, \cdot)$ (де $M_{n\times n}(\mathbb{R})$ – множина дійсних матриць розміру $n \times n$) – асоціативне кільце матриць.
6. Кільце чисел $\left(\mathbb{Z}\left[\frac{1}{2}\right], +, \cdot\right)$, де $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{n}{2^m}, m, n \in \mathbb{N}\right\}$.
7. Кільце подвійних чисел $\{a + b\boldsymbol{e} | a, b \in \mathbb{R}, \boldsymbol{e}^2 = \mathbf{1}\}$. Додавання покоординатне, а множення має вигляд:

$$(a + b\boldsymbol{e})(c + d\boldsymbol{e}) = ac + bd + (ad + bc)\boldsymbol{e}.$$

8. $(V, +, \times)$ (V – множина векторів простору з операціями додавання та векторного добутку) – неасоціативне кільце, оскільки у загальному випадку

$$\left(\vec{a} \times \vec{b}\right) \times \vec{c} \neq \vec{a} \times \left(\vec{b} \times \vec{c}\right).$$

9. Кільце дуальних чисел $\{a + b\boldsymbol{\varepsilon} | a, b \in \mathbb{R}, \boldsymbol{\varepsilon}^2 = 0\}$. Додавання по координатне, а множення має вигляд: $(a + b\boldsymbol{\varepsilon})(c + d\boldsymbol{\varepsilon}) = ac + (ad + bc)\boldsymbol{\varepsilon}$.

10. Кільце функцій $f: \mathbb{R} \to \mathbb{R}$ з поточковим додаванням і множенням.

11. $\mathbb{Z}/n\mathbb{Z}$ ($\mathbb{Z}_n$) – кільце класів лишків за модулем n. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$, де $\overline{k} = \{k + mn | \, m \in \mathbb{N}\}$. $\overline{k} + \overline{l} = \overline{k+l}$, $\overline{k} \cdot \overline{l} = \overline{kl}$.

12. Нехай $(\mathcal{R}, +, \cdot)$ комутативне асоціативне кільце. Через $\mathcal{R}[x]$ позначають кільце многочленів $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, де $a_i \in \mathcal{R}$, із звичайними операціями додавання і множення многочленів.

Означення 6.2. *Якщо в кільці існує елемент* $1 \in \mathcal{R}$, *такий що* $\forall x \in \mathcal{R}$,

$$x \circ 1 = x = 1 \circ x,$$

тоді $(\mathcal{R}, +, \circ)$ *називається кільцем з одиницею, а* 1 *– нейтральним елементом або одиницею за множенням.*

Означення 6.3. *Якщо множення* $\circ$ *комутативне, то* $(\mathcal{R}, +, \circ)$ *називається комутативним кільцем*.

Як правило, під комутативним кільцем розуміють комутативне асоціативне кільце з одиницею.

Вправа 6.1. Які із наведених вище прикладів кілець є кільцями з одиницею?

Кілець нескінченно багато[*]

Цей пункт може бути пропущеним, якщо невідомі такі поняття як *потужність* множини, *зліченність*, *континуум*.

Постає питання: кількість кілець скінченна чи нескінченна? Відповідь – кілець нескінченно багато причому потужність множини кілець не менш ніж континуальна.

Нехай $S \subset \mathbb{P} = \{2,3,5,7, \dots\}$ підмножина множини простих чисел. Розглянемо множину:

$$R_S = \left\{ \frac{m}{\prod_{p \in S} p^{l_p}} \mid m \in \mathbb{Z}, l_p \in \mathbb{N}_0 \right\}.$$

Легко перевірити, що $(R_S, +, \cdot)$ (тут " $+$ " , " $\cdot$ " – відповідно операції додавання і множення дійсних чисел) є кільцем.

Звідки випливає, що кілець існує нескінченно багато, а саме, кількість підмножин натуральних чисел (континуум)

$$|\mathbb{P}| = |\mathbb{N}| = \aleph_0$$

$$\left|2^{\mathbb{P}}\right| = \aleph_1 = c.$$

Пряма сума кілець

Означення 6.4. *Нехай* $(R, +, \circ)$, $(S, \boxplus, *)$ *два кільця. Прямою сумою цих кілець називається кільце* $(R \oplus S, +, \cdot)$, *де* $R \oplus S = \{(x, y) | x \in R, y \in S\}$, *на якій задані операції:*

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 \boxplus y_2),$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \circ x_2, y_1 * y_2).$$

Неважко переконатись, що нейтральним елементом операції додавання є

$$0_{R \oplus S} = (0_R, 0_S),$$

а нейтральним елементом операції множення є

$$1_{R \oplus S} = (1_R, 1_S).$$

Вправа 6.2. Перевірити, що $(R \oplus S, +, \cdot)$ є кільцем.

Означення 6.5. *Нехай* $(R,+,\cdot)$ *кільце. Протилежним кільцем називається кільце* $(R^0,+,\circ)$*, де* $R^0 = R$*, а операція* $\circ$ *визначається так:*

$$x \circ y = y \cdot x.$$

Вправа 6.3. Навести приклади кілець, протилежні кільця до яких відрізняються від самих кілець.

Приєднання одиниці

Нехай $(R,+,\cdot)$ – кільце без одиниці. Розглянемо множину $\mathbb{Z} \times R$:

$$\mathbb{Z} \times R = \{(x,y) | x \in \mathbb{Z}, y \in R\}.$$

На множині $\mathbb{Z} \times R$ введемо операції додавання і множення:

$$(m,x) + (n,y) = (m+n, x+y),$$

$$(m,x) \cdot (n,y) = (mn, nx + my + x \cdot y).$$

Тут $mx = \underbrace{x + x + \cdots + x}_{m}$, $0x = \mathbf{0}$, $\mathbf{0} \in R$, $m\mathbf{0} = \mathbf{0}$, $(-1)x = -x$, $(-2)x = 2(-x)$.

Легко переконатись, що структура $(\mathbb{Z} \times R,+,\cdot)$ є кільцем, причому у такому кільці одиниця це $(1,\mathbf{0})$. Дійсно,

$$(m,x) \cdot (1,\mathbf{0}) = (m, 1x + m \cdot \mathbf{0} + x \cdot \mathbf{0}) = (m,x),$$

$$(1,\mathbf{0}) \cdot (n,y) = (n, n \cdot \mathbf{0} + 1y + \mathbf{0} \cdot y) = (n,y).$$

Означення 6.6. *Кільце* $(L,+,\otimes)$ *називається кільцем Лі, якщо для множення виконуються умови:*

1. $\forall x \in L,\ \ x \otimes x = 0,$
2. $\forall x,y,z \in L$

$$(x \otimes y) \otimes z + (y \otimes z) \otimes x + (z \otimes x) \otimes y = 0. \qquad (6.1)$$

Співвідношення (6.1) називається *тотожністю Якобі*.

Із умови 1 випливає, що $\forall x,y \in L,\ x \otimes y = -y \otimes x$.

ЛЕКЦІЯ 7. **ПІДКІЛЬЦЕ. ОБЛАСТЬ ЦІЛІСНОСТІ.**

Підкільце. Критерій підкільця

Нехай $(\mathcal{R}, +, \cdot)$ – кільце.

Означення 7.1. *Підкільцем кільця* $(\mathcal{R}, +, \cdot)$ *називається кільце* $(\mathcal{R}_1, +, \cdot)$, для якого $\mathcal{R}_1 \subset \mathcal{R}$, *а операції додавання та множення такі ж як у кільця* $(\mathcal{R}, +, \cdot)$.

Позначається $(\mathcal{R}_1, +, \cdot) \subset (\mathcal{R}, +, \cdot)$.

Теорема 7.1. (Критерій підкільця) *Нехай* $\emptyset \neq \mathcal{R}_1 \subset \mathcal{R}$. *Для того, щоб* $(\mathcal{R}_1, +, \cdot)$ *було підкільцем кільця* $(\mathcal{R}, +, \cdot)$ *необхідно і достатньо виконання умов*:

1) $\forall a, b \in \mathcal{R}_1 \Rightarrow a + b \in \mathcal{R}_1$,
2) $\forall a \in \mathcal{R}_1 \Rightarrow -a \in \mathcal{R}_1$,
3) $\forall a, b \in \mathcal{R}_1 \Rightarrow a \cdot b \in \mathcal{R}_1$.

Доведення. Необхідність випливає із означення кільця.

Достатність. З урахуванням умов 1), 2), легко переконатись, що $0 \in \mathcal{R}_1$ оскільки $0 = a + (-a) \in \mathcal{R}_1$. Асоціативність та комутативність додавання в $(\mathcal{R}_1, +)$ є наслідком асоціативності та комутативності додавання в $(\mathcal{R}, +)$. Отже, $(\mathcal{R}_1, +)$ – абелева група.

Дистрибутивність множення відносно додавання в $(\mathcal{R}_1, +, \cdot)$ є наслідком дистрибутивності в $(\mathcal{R}, +, \cdot)$.

Вправа 7.1. Довести, що умови 1) – 3) критерія підкільця можна замінити двома умовами:

1) $\forall a, b \in \mathcal{R}_1 \Rightarrow a - b \in \mathcal{R}_1$,
2) $\forall a, b \in \mathcal{R}_1 \Rightarrow a \cdot b \in \mathcal{R}_1$.

Приклади

1. Кільце раціональних чисел є підкільцем кільця дійсних чисел, а воно підкільце кільця комплексних чисел: $(\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot)$.

2. Парні числа $2\mathbb{Z}$ є підкільцем кільця $\mathbb{Z}$, але без 1

$$(2\mathbb{Z}, +, \cdot) \subset (\mathbb{Z}, +, \cdot).$$

3. $\forall n \in \mathbb{N}$ $(n\mathbb{Z}, +, \cdot)$ є підкільцем кільця $(\mathbb{Z}, +, \cdot)$. Дійсно,

$$\forall m_1, m_2 \in \mathbb{Z}, \qquad m_1 n, m_2 n \in n\mathbb{Z},$$

$$m_1 n - m_2 n = (m_1 - m_2)n \in n\mathbb{Z},$$

$$m_1 n m_2 n = \big((m_1 m_2)n\big)n \in n\mathbb{Z}.$$

Вправа 7.2. Чи існують підкільця кільця $(\mathbb{Z}, +, \cdot)$, які відмінні від підкілець виду $(n\mathbb{Z}, +, \cdot)$?

Дільники нуля. Оборотні елементи

Нехай $(R, +, \cdot)$ кільце.

Означення 7.2. *Ненульовий елемент $a \in R$ називається правим (лівим) дільником нуля, якщо існує ненульовий елемент $b \in R$ такий, що $ba = 0$ $(ab = 0)$. Елемент, який є одночасно правим і лівим дільником нуля називається дільником нуля.*

Означення 7.3. *Елемент $a \in R$ називається нільпотентом, якщо існує $n \in \mathbb{N}$ таке, що $a^n = 0$.*

Вправа 7.3. Довести, що нільпотент $a \neq 0$ є дільником нуля.

Означення 7.4. *Асоціативне комутативне кільце з одиницею, яке не містить дільників нуля називається областю цілісності.*

Приклади

1. $(\mathbb{Z}, +, \cdot)$,
2. $\mathbb{Z}[\sqrt{2}] = \{n + m\sqrt{2} \mid n, m \in \mathbb{Z}\}$,
3. $(\mathbb{Q}, +, \cdot)$,
4. $\mathbb{Z}/p\mathbb{Z}$, де p – просте число.

Означення 7.5. *Елемент $a \in R$ називається оборотним в кільці $(R, +, \cdot)$ з одиницею 1, якщо існує $a^{-1} \in R$ такий, що*

$$a \cdot a^{-1} = 1 = a^{-1} \cdot a.$$

Елемент a^{-1} називається оберненим до a.

Множину всіх оборотних елементів кільця $(R, +, \cdot)$ позначають R^*.

Теорема 7.2. *В асоціативному кільці $(R, +, \cdot)$ з одиницею 1 оборотний елемент не може бути ні правим, ні лівим дільником нуля.*

Доведення. Нехай $a \in R$ – оборотний і a^{-1} – обернений до a. Якщо припустити, що при цьому a, наприклад, правий дільник нуля, тобто, існує ненульовий елемент $b \in R$ такий, що $ba = 0$. Тоді

$$0 = 0 \cdot a^{-1} = (b \cdot a) \cdot a^{-1} = b \cdot (a \cdot a^{-1}) = b \cdot 1 = b,$$

що суперечить умові $b \neq 0$. Для лівого елемента нуля доведення аналогічне.

Зауважимо, що умова відсутності дільників нуля у кільці з одиницею не гарантує оберненість усіх ненульових елементів кільця. Наприклад, кільце $(\mathbb{Z}, +, \cdot)$ не містить дільників нуля, але крім 1 та -1, всі інші елементи цього кільця необоротні.

Закони скорочення в кільці $(R, +, \cdot)$:

$$\forall a, b, x \in R, \quad x \neq 0, \quad a \cdot x = b \cdot x \Leftrightarrow a = b, \quad \text{(праве скорочення)};$$

$$\forall a, b, x \in R, \quad x \neq 0, \quad x \cdot a = x \cdot b \Leftrightarrow a = b, \quad \text{(ліве скорочення)}.$$

Теорема 7.3. *У будь-якому кільці $(R, +, \cdot)$ праве і ліве скорочення виконується тоді і тільки тоді, коли це кільце не містить дільників нуля.*

Доведення. Необхідність випливає із того, що якщо $x \neq 0$ і $a \cdot x = b \cdot x$, то $(a - b) \cdot x = 0$ і, за умови, що $(R, +, \cdot)$ не містить дільників нуля, маємо $a - b = 0$, тобто $a = b$.

Якщо ж виконуються закони скорочення і $a \neq 0$, $b \neq 0$, $a \cdot b = 0$, то

$$0 = a \cdot b = a \cdot 0 \Rightarrow b = 0,$$

що суперечить умові $b \neq 0$.

Означення 7.6. *Булеве кільце – це асоціативне кільце:* $(\mathcal{R}, +, \circ)$*, таке що* $\forall x \in \mathcal{R}, x \circ x = x$.

Твердження 7.1. *Нехай* $(\mathcal{R}, +, \circ)$ - булеве кільце, тоді

1. $\forall\, x, y \in \mathcal{R},\ \ x \circ y = y \circ x;$
2. $\forall\, x \in \mathcal{R},\ \ x + x = 0.$

Доведення. Із означення випливає, що $(x + y) \circ (x + y) = x + y$, звідки

$$x \circ y + y \circ x = 0.$$

Підставивши $y = x$, отримаємо $x + x = 0$.

Далі, оскільки $x \circ y + y \circ x = 0$ та $x \circ y + x \circ y = 0$, то $x \circ y = y \circ x$.

Якщо у множині 2^X, $X \neq \emptyset$, в якості суми множин A і B взяти симетричну різницю $A + B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A)$, а в якості добутку перетин $A \times B \stackrel{\text{def}}{=} A \cap B$, то отримаємо булеве кільце.

Інший приклад булевого кільця $\mathbb{Z}/2\mathbb{Z}$ $(\mathbb{Z}_2)$ – кільце класів лишків за модулем 2.

Пряма сума кілець

Нехай R, S два кільця

$$R \oplus S = \{(x, y) | x \in R, y \in S\},$$

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2, y_1 \cdot y_2),$$

$$0_{R \oplus S} = (0_R, 0_S),$$

$$1_{R \oplus S} = (1_R, 1_S).$$

Протилежне кільце

Нехай $(R, +, \cdot)$ – кільце. Розглянемо множину з операціями $(R^{\mathrm{o}}, +, \circ)$,

де $R^{\mathrm{o}} = R$, $+$ така ж операція, як і в $(R, +, \cdot)$, а

$$x \circ y = y \cdot x.$$

Вправа 7.4. Переконайтесь, що $(R^o, +, \circ)$ також є кільцем.

Кільце $(R^o, +, \circ)$ називається протилежним до $(R, +, \cdot)$.

Приєднання одиниці

Нехай $(R, +, \cdot)$ – кільце без одиниці. Введемо множину

$$\mathbb{Z} \oplus R = \{(x, y) | x \in \mathbb{Z}, y \in R\}.$$

Та операції на $\mathbb{Z} \oplus R$:

$$(m, x) + (n, y) = (m + n, x + y),$$

$$(m, x) \cdot (n, y) = (mn, nx + my + x \cdot y).$$

Тут $mx = \underbrace{x + x + \cdots + x}_{m}$, $0x = \mathbf{0}$, $(-1)x = -x$, $(-2)x = 2(-x)$.

У такому кільці одиниця це $(1, \mathbf{0})$, дійсно

$$(m, x) \cdot (1, \mathbf{0}) = (m, 1x + m\mathbf{0} + x \cdot \mathbf{0}) = (m, x),$$

$$(1, \mathbf{0}) \cdot (n, y) = (1n, n\mathbf{0} + 1y + \mathbf{0} \cdot y) = (n, y).$$

ЛЕКЦІЯ 8. **ІДЕАЛИ. ФАКТОР КІЛЬЦЕ**

Означення 8.1. *Підкільце I кільця $(R, +, \cdot)$ називається лівим ідеалом, якщо $\forall a \in I, \forall r \in R$ маємо $r \cdot a \in I$ ($RI \subset I$). Аналогічно підкільце I кільця $(R, +, \cdot)$ називається правим ідеалом, якщо $\forall a \in I, \forall r \in R$ маємо $a \cdot r \in I$ ($IR \subset I$).*

Підкільце I кільця $(R, +, \cdot)$ називається ідеалом, якщо I – лівий і правий ідеал одночасно.

Очевидно, що саме кільце $(R, +, \cdot)$ та нульове кільце $(0, +, \cdot)$ є ідеалами в $(R, +, \cdot)$, які називають тривіальними. Звичайно, інтерес становлять нетривіальні або власні ідеали кільця.

Твердження 8.1. *Непорожня множина $I \subset R$ є ідеалом тоді і тільки тоді, коли*

1. $\forall a, b \in I, a - b \in I;$
2. $\forall a \in I, \forall r \in R, r \cdot a \in I \; i \; a \cdot r \in I.$

Доведення є прямим наслідком вправи 7.1.

Приклади

1. $n\mathbb{Z}$, де $n \in \mathbb{N}$ є ідеалом кільця $(\mathbb{Z}, +, \cdot)$.
2. Нехай $\mathbb{R}[x]$ – кільце многочленів над дійсними числами. Многочлени, які діляться на деякий ненульовий многочлен $p(x) \in \mathbb{R}[x]$ є ідеалом.

Твердження 8.2. *Перетин довільної кількості ідеалів деякого кільця є ідеалом.*

Доведення. Нехай I_α, $\alpha \in \mathrm{A}$ – набір ідеалів кільця $(R, +, \cdot)$. Розглянемо перетин цих ідеалів $I = \bigcap_{\alpha \in \mathrm{A}} I_\alpha$.

Нехай маємо довільні $a, b \in I$ та $r \in R$. Тоді $a, b \in I_\alpha$ та $a \cdot r \in I_\alpha$ для всіх $\alpha \in \mathrm{A}$. Звідки $a - b \in I$ та $a \cdot r \in I$, для $\forall a, b \in I$ та $\forall r \in R$. Отже, за твердженням 8.2 I – ідеал кільця $(R, +, \cdot)$.

Означення 8.2. *Нехай $(R, +, \cdot)$ – кільце і $S \subset R$. Ідеал(S) , який є перетином ідеалів кільця $(R, +, \cdot)$, що містять S*

$$(S) = \bigcap_{S \subset I,\ I\text{–ідеал}} I$$

називається ідеалом, породженим множиною S.

Легко бачити, що (S) є найменшим ідеалом, який містить S.

Якщо S – одноелементна множина, що складається з одного елемента a, то ідеал (S) позначають (a) і називають *головним ідеалом*, породженим елементом a. Якщо $(R, +, \cdot)$ – комутативне кільце, то неважко переконатись, що головний ідеал, породженим елементом a має вигляд

$$(a) = \{ar : r \in R\}.$$

Операції над ідеалами

Нехай I та J ідеали кільця $(R, +, \cdot)$.

Означення 8.3. *Сумою ідеалів* I та J *називається множина*

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

Добутком ідеалів I та J *називається множина*

$$IJ = \left\{ \sum_{k=1}^{n} a_k b_k : a_k \in I, b_k \in J, \ \ n \in \mathbb{N} \right\}.$$

Твердження 8.3. *Нехай* I_k, $k = 1, \dots, n$ *– набір ідеалів кільця* $(R, +, \cdot)$. *Тоді*

1) $\sum_{k=1}^{n} I_k$ *та* $\prod_{k=1}^{n} I_k$ *– ідеали;*
2) *добуток ідеалів асоціативний;*
3) *добуток ідеалів дистрибутивний.*

Доведення. Досить показати, що 1) виконується для $n = 2$. Для доведення застосуємо твердження 8.1.

Нехай $a_1, a_2 \in I$, $b_1, b_2 \in J$. Тоді $a_1 + b_1 - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in I + J$. Далі, $\forall r \in R$, $r(a_1 + b_1) = ra_1 + rb_1 \in I + J$ та $(a_1 + b_1)r = a_1 r + b_1 r \in I + J$. Отже, $I + J$ – ідеал.

Нехай $a_1, .., a_n, a_1', .., a_n' \in I$, $b_1, \dots, b_n, b_1', \dots, b_n' \in J$. Тоді

$$\sum_{k=1}^{n} a_k b_k - \sum_{k=1}^{n} a_k' b_k' = \sum_{k=1}^{n} a_k b_k + \sum_{k=1}^{n} (-a_k') b_k' \in IJ;$$

$$r\left(\sum_{k=1}^{n} a_k b_k \right) = \sum_{k=1}^{n} (r a_k) b_k \in IJ;$$

$$\left(\sum_{k=1}^{n} a_k b_k \right) r = \sum_{k=1}^{n} a_k (b_k r) \in IJ.$$

Аналогічно доводяться пункти 2) та 3).

Означення 8.4. *Ідеал I кільця $(R,+,\cdot)$ називається максимальним, якщо $I \neq R$ і, якщо J ідеал кільця $(R,+,\cdot)$ такий, що $I \subset J \subset R$, то $I = J$ або $J = R$.*

Гомоморфізм

Нехай $(R,+,\cdot)$, $(S,\oplus,\circ)$ – кільця.

Означення 8.5. *Відображення $\varphi: R \to S$ називається гомоморфізмом, якщо $\forall a,b \in R$ має місце*

$$\varphi(a+b) = \varphi(a) \oplus \varphi(b);$$

$$\varphi(a \cdot b) = \varphi(a) \circ \varphi(b).$$

Якщо гомоморфізм $\varphi: R \to S$ є взаємно однозначним відображенням, то φ називається ізоморфізмом.

Означення 8.5. *Ядром гомоморфізму $\varphi: R \to S$ називається множина*

$$ker(\varphi) = \{r \in R | \varphi(r) = 0\}.$$

Образом гомоморфізму φ називається множина

$$Im(\varphi) = \{s \in S | \exists r \in R: \varphi(r) = s\}.$$

Твердження 8.4. *Нехай $\varphi: R \to S$ – гомоморфізм кілець $(R,+,\cdot)$ та $(S,\oplus,\circ)$. Тоді*

1) *$ker(\varphi)$ – ідеал в $(R,+,\cdot)$;*
2) *$Im(\varphi)$ – підкільце $(S,\oplus,\circ)$.*

Доведення. 1). Нехай $a_1, a_2 \in ker(\varphi)$. Тоді $\varphi(a_1) = 0$, $\varphi(a_2) = 0$, звідки $\varphi(a_1 - a_2) = 0$ і, отже, $a_1 - a_2 \in ker(\varphi)$. Нехай $a \in ker(\varphi)$, $r \in R$. Тоді $\varphi(a \cdot r) = \varphi(a) \circ \varphi(r) = 0 \circ \varphi(r) = 0$. З урахуванням твердження 8.1 $ker(\varphi)$ – ідеал.

2) Нехай $s_1, s_2 \in Im(\varphi)$. Тоді $\exists r_1, r_2 \in R$: $\varphi(r_1) = s_1$, $\varphi(r_2) = s_2$. Звідки

$$\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) = s_1 - s_2 \in Im(\varphi),$$

$$\varphi(r_1 \cdot r_2) = \varphi(r_1) \circ \varphi(r_2) = s_1 \circ s_2 \in Im(\varphi).$$

Отже, $Im(\varphi)$ – підкільце.

Факторкільце

Нехай $(R, +, \cdot)$ – кільце, $S \subset R$, $a \in R$. Записом $a + S$ позначається множина

$$a + S \coloneqq \{a + b : b \in S\}.$$

Нехай I ідеал кільця $(R, +, \cdot)$. Розглянемо множину $R/I = \{a + I : a \in R\}$, на якій введені такі операції додавання та множення:

$$(a + I) \oplus (b + I) := a + b + I,$$

$$(a + I) \circ (b + I) := a \cdot b + I.$$

Теорема 8.1. $(R/I, \oplus, \circ)$ *– кільце, яке називають фактор кільцем кільця* $(R, +, \cdot)$ *за ідеалом* I.

Доведення. Доведемо коректність додавання і множення.

Дійсно, нехай $a + I = a' + I$ і $b + I = b' + I$. Це означає, що існують $i, j \in I$ такі, що $a' = a + i$, $b' = b + j$. Звідки, з урахуванням того, що $i + j + I = I$, маємо

$$(a' + I) \oplus (b' + I) = (a + i + I) \oplus (b + j + I) = a + i + b + j + I = a + b + I$$
$$= (a + I) \oplus (b + I).$$

Далі, неважко переконатись, що $a \cdot i + b \cdot j + i \cdot j \in I$. Звідки

$$(a' + I) \circ (b' + I) = (a + i + I) \circ (b + j + I) = a \cdot b + a \cdot i + b \cdot j + i \cdot j + I$$
$$= a \cdot b + I = (a + I) \circ (b + I).$$

Властивості кільця для додавання $\oplus$ і дистрибутивність множення відносно додавання перевірте самостійно.

Приклади

1. Кільце $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ є фактор кільцем кільця $(\mathbb{Z}, +, \cdot)$ за ідеалом $n\mathbb{Z}$, де $n \in \mathbb{N}$.
2. Кільце $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$, де $\mathbb{Q}[\sqrt{2}] = \{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$ містить ідеал $I(\sqrt{2}) = \{s\sqrt{2} \mid s \in \mathbb{Q}\}$. Легко переконатись, що фіктор кільце $\left(\mathbb{Q}[\sqrt{2}]/I(\sqrt{2}), +, \cdot\right)$ ізоморфне кільцю раціональних чисел $(\mathbb{Q}, +, \cdot)$.

ЛЕКЦІЯ 9. **ПОЛЕ. ПОЛЕ КОМПЛЕКСНИХ ЧИСЕЛ**

Тіло. Поле

Означення 9.1. *Асоціативне кільце з одиницею називають тілом (або некомутативним полем, англійською skew field), якщо в ньому виконується умова* $\forall x \in \mathcal{R} : x \neq 0, \exists x^{-1}$, *такий, що* $x \circ x^{-1} = 1 = x^{-1} \circ x$.

Означення 9.2. *Комутативне тіло називається полем (англійською field).*

Приклади

1) Поле дійсних чисел $(\mathbb{R}, +, \cdot)$;

2) Поле раціональних чисел $(\mathbb{Q}, +, \cdot)$;

3) Поле комплексних чисел $(\mathbb{C}, +, \cdot)$;

4) Тіло кватерніонів $(\mathbb{H}, +, \cdot)$.

5) Поле Галуа $\mathbb{Z}/p\mathbb{Z}$ $(\mathbb{Z}_p)$ – поле класів лишків за модулем p, де p – просте число.

6) Поле $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$, де $\mathbb{Q}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$

Вправа 9.1. Переконайтесь, що $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$ – поле.

Комплексні числа

Через i будемо позначати уявну одиницю, яка символізує один із розв'язків рівняння $x^2 + 1 = 0$ або по іншому $i^2 = -1$.

Означення 9.4. *Комплексним числом називається вираз* $x + yi$, *де* $x, y \in \mathbb{R}$.

Означення 9.5. *Множина комплексних чисел позначається через*

$$\mathbb{C} = \{z: z = x + yi\ , x, y \in \mathbb{R}\},$$

При цьому $x = Re(z)$ називається дійсною частиною, а $y = Im(z)$ – уявною частиною комплексного числа z, а запис $z = x + yi$ називається *алгебраїчною формою запису* комплексного числа z.

Операції над комплексними числами

Числа $z_1 = x_1 + y_1 i$ та $z_2 = x_2 + y_2 i$ рівні тоді і тільки тоді, коли $x_1 = x_2$ та $y_1 = y_2$.

Додавання (віднімання): $z_1 \pm z_2 = x_1 \pm x_2 + (y_1 \pm y_2)i$.

Множення: $z_1 z_2 = x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1)i$.

Формальне означення комплексних чисел

Комплексне число $z = x + yi$ розглядається як пара дійсних чисел $\binom{x}{y}$.

Операції задаються так:

Додавання: $\binom{x_1}{y_1} + \binom{x_2}{y_2} = \binom{x_1 + x_2}{y_1 + y_2}$,

Множення: $\binom{x_1}{y_1} \cdot \binom{x_2}{y_2} = \binom{x_1 x_2 - y_1 y_2}{x_1 y_2 + x_2 y_1}$.

Перевага формального означення комплексних чисел у тому, що не потрібно вводити уявне число $i = \sqrt{-1}$, при цьому дійсне число x задається парою $\binom{x}{0}$, а чисто уявне число iy – парою $\binom{0}{y}$, зокрема $i = \binom{0}{1}$. Легко переконатись, що

$$i^2 = \begin{pmatrix}0\\1\end{pmatrix} \cdot \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}-1\\0\end{pmatrix},$$

$$\begin{pmatrix}0\\y\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} \cdot \begin{pmatrix}y\\0\end{pmatrix} = iy.$$

Ділення комплексних чисел

Означення 9.6. *Комплексне число* $\bar{z} = x - yi$ *називається спряженим до* $z = x + yi$.

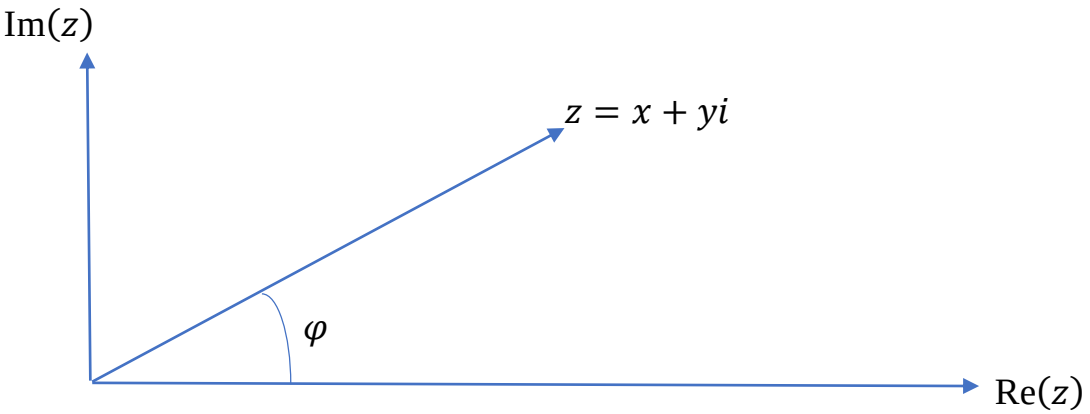
Легко бачити, що $z\bar{z} = x^2 + y^2 = \bar{z}z$. Звідси для $z_1 = x_1 + y_1 i$, $z_2 = x_2 + y_2 i \neq 0$, маємо

$$\frac{z_1}{z_2} = \frac{x_1 + y_1 i}{x_2 + y_2 i}\frac{\overline{z_1}}{\overline{z_2}} = \frac{x_1x_2 + y_1y_2 - (x_1y_2 - x_2y_1)i}{x_2^2 + y_2^2} = \frac{x_1x_2 + y_1y_2}{x_2^2 + y_2^2} - \frac{x_1y_2 - x_2y_1}{x_2^2 + y_2^2}i.$$

Зауваження 9.1. Операція ділення на ненульові комплексні числа разом з тим, що $(\mathbb{C}, +, \cdot)$ є комутативним кільцем свідчить, що $(\mathbb{C}, +, \cdot)$ – поле.

Геометричне зображення комплексних чисел

Комплексне число $z = x + yi$ може розглядатись як вектор на площині з ортогональним базисом $\{1, i\}$. Тому можна здійснювати перехід від прямокутної системи координат (x, y) до полярної $(|z|, \varphi)$, де $|z| = \sqrt{x^2 + y^2}$ – модуль комплексного числа z, а $\varphi = Arg(z)$ – аргумент z.



$Arg(z)$ визначається з точністю до періоду 2π, тобто $Arg(z) = \varphi + 2\pi k$, $k \in \mathbb{Z}$. Для однозначності вводиться поняття головного значення аргументу числа z: $\varphi = arg(z) \in]-\pi, \pi]$ (у деяких підручниках $arg(z) \in [0,2\pi[$).

Обчислення $arg(z)$ залежить від квадранту системи координат, у якому знаходиться число z:

1. Якщо $z \in I$ або $z \in IV$, то

$$arg(z) = \arctan\frac{y}{x};$$

2. Якщо $z \in II$, то

$$arg(z) = \pi + \arctan\frac{y}{x};$$

3. Якщо $z \in III$, то

$$arg(z) = -\pi + \arctan\frac{y}{x}.$$

Формула переходу від полярної системи $(|z|, \varphi)$ координат до декартової (x, y):

$$\begin{cases} x = |z|\cos\varphi \\ y = |z|\sin\varphi \end{cases}$$

Тригонометрична форма запису комплексного числа

$$z = |z|(\cos\varphi + i\sin\varphi).$$

Цією формою зручно користуватись при обчисленні добутку чи ділення комплексних чисел, а також при піднесенні комплексного числа до степеню та взяття кореня.

Нехай для $z_1 = |z_1|(\cos\varphi_1 + i\sin\varphi_1)$, $z_2 = |z_2|(\cos\varphi_2 + i\sin\varphi_2)$. Тоді

$$z_1 z_2 = |z_1||z_2|(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 + i\sin\varphi_2)$$
$$= |z_1||z_2|\big(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2$$
$$+ i(\cos\varphi_1\sin\varphi_2 + \cos\varphi_2\sin\varphi_1)\big)$$
$$= |z_1||z_2|(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)).$$

Аналогічно показується, що

$$\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).$$

Піднесення до степеню

Використовуючи формулу добутку комплексних чисел, легко бачити, що для $n \in \mathbb{N}$

$$z^n = |z|^n(\cos n\varphi + i\sin n\varphi).$$

Корінь з комплексного числа

Означення 9.7. *Коренем степеню $n \in \mathbb{N}$ комплексного числа z називається комплексне число v таке, що $v^n = z$.*

Нехай $z = |z|(\cos\varphi + i\sin\varphi)$, а $v = |v|(\cos\alpha + i\sin\alpha)$. Тоді

$$v^n = |v|^n(\cos n\alpha + i\sin n\alpha) = |z|(\cos\varphi + i\sin\varphi).$$

Звідки маємо співвідношення

$$|v| = \sqrt[n]{|z|},$$

$$n\alpha = \varphi + 2\pi k,\ k \in \mathbb{Z}.$$

Отже, маємо рівно n різних значень для α (з точністю до періоду 2π):

$$\alpha = \frac{\varphi + 2\pi k}{n},\ k = 0,1,\dots,n-1.$$

Показникова форма запису комплексного числа

Формула Ойлера $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Доведення цієї формули здійснюється шляхом розкладу функцій e^{-ix}, $\cos x$ та $\sin x$ у ряди Тейлора. Звідки випливає показникова форма запису

$$z = |z|e^{i\varphi}.$$

ЛЕКЦІЯ 10. **КІЛЬЦЕ МНОГОЧЛЕНІВ**

Нехай $(\mathbb{K}, +, \cdot)$ – комутативне кільце з одиницею 1.

Через $\mathbb{K}[x]$ позначимо множину многочленів з коефіцієнтами із кільця $\mathbb{K}$:

$$\mathbb{K}[x] = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n | \, n \in \mathbb{N}, a_k \in \mathbb{K}\}.$$

Означення 10.1. *Степенем многочлена* $0 \not\equiv f(x) = a_0 + a_1x + \cdots + a_nx^n$ *називається величина* $\deg(f) = \max\{k \in \mathbb{N}: a_k \neq 0\}$. *Старшим коефіцієнтом ненульового многочлена* $f(x)$ *називається число* $\mathrm{coef}(f) = a_n$, *де* $n = \deg(f)$.

Многочлен $f(x) \equiv 0$, у якого всі коефіцієнти нулі, будемо називати нульовим і позначати $\theta(x)$. Степенем нульового многочлена покладемо рівним мінус нескінченності $\deg(\theta) = -\infty$, причому вважаємо, що $\forall a \in \mathbb{K}$

$$\max(a, -\infty) = a\,, a + -\infty = -\infty.$$

Означення 10.2. *Многочлени* $f, g \in \mathbb{K}[x]$ *називаються рівними, якщо* $\deg(f) = \deg(g)$ *і*

$$a_k = b_k, \qquad k = 0,1,2, \ldots$$

Операції в $\mathbb{K}[x]$

Нехай

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \text{ та } g(x) = b_0 + b_1x + \cdots + b_mx^m$$

Тоді

$$f(x) + g(x) = a_0 + b_0 + (a_1 + b_1)x + \cdots,$$

$$f(x) \cdot g(x) = \sum_k c_k x^k,$$

де $c_k = \sum_{i=0}^{k} a_i\, b_{k-i}$.

Твердження 10.1. $\forall f, g \in \mathbb{K}[x]$

1. $\deg(f+g) \le \max\big(\deg(f), \deg(g)\big)$,
2. $\deg(f \cdot g) \le \deg(f) + \deg(g)$, причому $\deg(f \cdot g) < \deg(f) + \deg(g) \Leftrightarrow \operatorname{coef}(f)\operatorname{coef}(g) = 0$.
3. Якщо $\mathbb{K}$ – область цілісності, то $\deg(f \cdot g) = \deg(f) + \deg(g)$, $\operatorname{coef}(f)\operatorname{coef}(g) = \operatorname{coef}(f \cdot g)$.

Вправа 10.1. Довести твердження 10.1.

Теорема 10.1. $(\mathbb{K}[x], +, \cdot)$ – *комутативне кільце з одиницею. Якщо* $(\mathbb{K}, +, \cdot)$ *область цілісності, то* $(\mathbb{K}[x], +, \cdot)$ – *область цілісності, причому* $(\mathbb{K}, +, \cdot)$ *підкільце кільця* $(\mathbb{K}[x], +, \cdot)$.

Доведення. Операції над многочленами зводяться до операцій над елементами кільця $(\mathbb{K}, +, \cdot)$. Безпосередньо перевіряється, що ці операції задовольняють означення асоціативного комутативного кільця з одиницею, тобто $\forall f, g \in \mathbb{K}[x]$

1. $f + g = g + f$;
2. $f + \theta = f$;
3. $f + (-f) = \theta,\ -f(x) = (-1) \cdot f(x)$;
4. $f + (g + h) = (f + g) + h$;
5. $f \cdot g = g \cdot f$;
6. $f \cdot (g + h) = f \cdot h + g \cdot h$;
7. $f \cdot (g \cdot h) = (f \cdot g) \cdot h$.

Нехай $(\mathbb{K}, +, \cdot)$ – область цілісності. Тоді, якщо $f \cdot g = \theta$, то

$$\deg(f \cdot g) = \deg(\theta) + \deg(g) = -\infty,$$

але $\deg(f \cdot g) = \deg(f) + \deg(g)$ і, якщо $f \neq \theta$ та $g \neq \theta$, то $\deg(f \cdot g) \geq 0$. Отримали суперечність. Отже, або $f = \theta$, або $g = \theta$, тобто немає дільників нуля.

Ділення многочленів

Нехай $\mathbb{F}$ поле. Розглянемо кільце многочленів над $\mathbb{F}$: $(\mathbb{F}[x], +, \cdot)$, що є областю цілісності многочленів, оскільки поле – область цілісності. Для стислості кільце $(\mathbb{F}[x], +, \cdot)$ надалі будемо позначати через $\mathbb{F}[x]$.

Означення 10.3. *Многочлен $f \in \mathbb{F}[x]$ ділиться на многочлен $g \in \mathbb{F}[x]$, якщо існує многочлен $h \in \mathbb{F}[x]$ такий, що*

$$f = g \cdot h. \tag{10.1}$$

Наприклад, $f(x) = x^3 - 1$, $g(x) = x^2 + x + 1$,

$$f(x) = x^3 - 1 = (x^2 + x + 1)(x - 1) = g(x)(x - 1).$$

Теорема 10.2 (Ділення з остачею) *Для довільних многочленів $f, g \in \mathbb{F}[x]$, $g \neq \theta$ існує єдина пара многочленів $q, r \in \mathbb{F}[x]$ така, що*

$$f = g \cdot q + r, \tag{10.2}$$

де $\deg(r) < \deg(g)$ *або* $r = \theta$.

Многочлен q називається неповна частка, а r – остача.

Доведення. Спочатку доведемо існування многочленів $q, r \in \mathbb{F}[x]$ Якщо $f(x) = c \in \mathbb{F}$, $\theta \neq g \in \mathbb{F}[x]$, то, якщо $\deg(g) \geq 1$, то

$$f = g \cdot \theta + c.$$

Якщо $\deg(g) = 0$, тобто $g = k \in \mathbb{F}$, причому $k \neq 0$. Тоді $\exists l \in \mathbb{F}$ таке, що

$$c = kl.$$

За індукцією припустимо, що для будь-якого многочлену $f \in \mathbb{F}[x]$ з $\deg(f) < n, n \in \mathbb{N}$ ділення з остачею виконується.

Покажемо, що ділення з остачею виконується і для $\deg(f) = n$. Дійсно, якщо $\deg(g) > n$, то

$$f = g \cdot \theta + f, \qquad \deg(f) = n < \deg(g)$$

Тепер припустимо, що $\deg(g) \leq \deg(f)$. Нехай

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $g(x) = b_0 + b_1 x + \cdots + b_m x^m$, де $m \leq n$.

Розглянемо многочлен

$$p(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = a_n x^n - \frac{a_n}{b_m} x^{n-m} b_m x^m - \cdots$$

Звідки видно, що $\deg(p) < n$. За припущенням індукції існують $q, r \in \mathbb{F}[x]$ такі, що $p = g \cdot q + r$, *де* $\deg(r) < \deg(g)$. Отже,

$$f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = g(x) \cdot q(x) + r(x).$$

Тобто

$$f(x) = g(x) \cdot \left(\frac{a_n}{b_m} x^{n-m} + q(x) \right) + r(x), \qquad \deg(r) < \deg(g).$$

Доведемо єдиність: припустимо, що існують $q_1, r_1 \in \mathbb{F}[x]$ та $q_2, r_2 \in \mathbb{F}[x]$ такі, що $q_1 \neq q_2$ та

$$f = g \cdot q_1 + r_1, \qquad \deg(r_1) < \deg(g),$$

$$f = g \cdot q_2 + r_2, \qquad \deg(r_2) < \deg(g).$$

Звідки

$$0 = g \cdot (q_1 - q_2) + r_1 - r_2.$$

Оскільки $\deg(r_1 - r_2) \leq \deg(r_1)$, то

$$\deg(r_1 - r_2) < \deg(g).$$

Далі, враховуючи властивість степеню $\deg(f \cdot g) = \deg(f) + \deg(g)$ для многочленів над полем та те, що $\deg(q_1 - q_2) \geq 0$, маємо

$$\deg\big(g \cdot (q_1 - q_2)\big) = \deg(g) + \deg(q_1 - q_2) \geq \deg(g) > \deg(r_1 - r_2).$$

Але із того, що $g \cdot (q_1 - q_2) = r_2 - r_1$ випливає, що $\deg\big(g \cdot (q_1 - q_2)\big) = \deg(r_2 - r_1) = \deg(r_1 - r_2)$.

Суперечність виникла із припущення існування двох різних пар $q_1, r_1 \in \mathbb{F}[x]$ та $q_2, r_2 \in \mathbb{F}[x]$, які задовольняють (10.2).

ЛЕКЦІЯ 11. **НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК МНОГОЧЛЕНІВ**

Означення 11.1. *Спільний дільник двох многочленів $f, g \in \mathbb{F}[x]$, який ділиться на будь-який інший спільний дільник цих многочленів, називається їх найбільшим спільним дільником* (НСД).

Позначається $\text{НСД}(f, g)$.

НСД многочленів визначається однозначно з точністю до сталого множника (оскільки, якщо $d(x) = \text{НСД}(f, g)$, то й $c \cdot d(x) = \text{НСД}(f, g)$, $c \neq 0$.

Многочлени $f(x)$ та $g(x)$ називаються взаємно простими, якщо кожний їхній спільний дільник є ненульовою константою, тобто $\text{НСД}(f, g) = c \neq 0$.

Аналогічно алгоритму Евкліда для знаходження НДС двох цілих чисел, алгоритм Евкліда застосовується для знаходження НДС двох многочленів $f, g \in \mathbb{F}[x]$:

$$f(x) = g(x) \cdot q_1(x) + r_1(x), \qquad \deg(r_1) < \deg(g),$$

$$g(x) = r_1(x) \cdot q_2(x) + r_2(x), \qquad \deg(r_2) < \deg(r_1),$$

$$r_1(x) = r_2(x) \cdot q_2(x) + r_3(x), \qquad \deg(r_3) < \deg(r_2),$$

$$- - - - - - - - - - - - - -$$

$$r_{s-1}(x) = r_s(x) \cdot q_s(x) + r_{s+1}(x), \qquad \deg(r_{s+1}) < \deg(r_s),$$

$$r_s(x) = r_{s+1}(x) \cdot q_{s+2}(x).$$

Теорема 11.1. $r_{s+1}(x) = \text{НСД}(f, g)$.

Доведення теореми аналогічне доведенню теореми 2.1 для цілих чисел.

Аналогічно доводиться лінійне зображення $d(x) = \text{НСД}(f, g)$, тобто існують многочлени $u, v \in \mathbb{F}[x]$ такі, що

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x). \qquad (11.1)$$

При цьому, якщо $\deg(g) > 0$ і $\deg(f) > 0$, то $\deg(u) < \deg(g)$, $\deg(v) < \deg(f)$. Доведемо це від супротивного, припустимо, що $\deg(u) \geq \deg(g)$. Тоді існують $q, r \in \mathbb{F}[x]$ такі, що

$$u(x) = g(x) \cdot q(x) + r(x), \qquad \deg(r) < \deg(g).$$

Підставляючи в (11.1), маємо

$$f(x) \cdot r(x) + g(x) \cdot [v(x) + f(x) \cdot q(x)] = d(x).$$

Множник $r(x)$, що стоїть при $f(x)$ має степінь менший степені $g(x)$. Степінь многочлена в квадратних дужках, що стоїть при $g(x)$, у свою чергу менший степеню $f(x)$. Дійсно, якби цей степінь був не менший степеню $f(x)$, то вираз $g(x) \cdot [v(x) + f(x) \cdot q(x)]$ мав би степінь більший степеню $f(x) \cdot r(x)$ і тоді степінь $d(x)$ був би більший або рівний степеню $f(x) \cdot g(x)$, що неможливо з урахуванням зроблених припущень ($\deg(g) > 0$ і $\deg(f) > 0$).

Наслідок 11.1. *Многочлени $f, g \in \mathbb{F}[x]$ взаємно прості тоді і тільки тоді, якщо існують многочлени $u, v \in \mathbb{F}[x]$ такі, що*

$$f(x) \cdot u(x) + g(x) \cdot v(x) = 1.$$

Означення 11.2. *Елемент* $x_0 \in \mathbb{F}$ *називається коренем многочлена* $f \in \mathbb{F}[x]$*, якщо* $f(x_0) = 0$.

Теорема 11.2 (Безу). *Елемент* $x_0 \in \mathbb{F}$ *є коренем многочлена* $f \in \mathbb{F}[x]$ *тоді і тільки тоді, коли многочлен* f *ділиться на* $x - x_0$.

Доведення. Поділимо з остачею f ділиться на $x - x_0$:

$$f(x) = (x - x_0) \cdot q(x) + r(x).$$

Оскільки $\deg(r) < \deg(x - x_0) = 1$, то $r(x) = r$ – константа. Отже,

$$f(x_0) = r.$$

Звідки, якщо x_0 – корінь, то $f(x_0) = 0 = r$, тобто $f(x)$ ділиться на $x - x_0$. Нехай $f(x)$ ділиться на $x - x_0$, тобто $f(x) = (x - x_0) \cdot q(x)$. Звідки $f(x_0) = 0$.

Схема Горнера

Ділення многочлена $f(x) \in \mathbb{F}[x]$ на $x - x_0$ можна здійснити за допомогою схеми Горнера, яка у загальному випадку значно спрощує цю процедуру ділення. Нехай

$$f(x) = (x - x_0) \cdot q(x) + f(x_0),$$

де $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, $q(x) = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$, причому коефіцієнти многочлена $q(x)$ потрібно обчислити.

Отже, $a_0 + a_1 x + \cdots + a_n x^n = (x - x_0) \cdot (b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}) + c$, $c = f(x_0)$.

Прирівнюючи коефіцієнти при відповідних степенях x, маємо

$$a_n = b_{n-1} \qquad \Rightarrow \qquad b_{n-1} = a_n$$

$$a_{n-1} = b_{n-2} - b_{n-1}x_0 \quad \Rightarrow \quad b_{n-2} = a_{n-1} + b_{n-1}x_0$$

$$a_{n-2} = b_{n-3} - b_{n-2}x_0 \quad \Rightarrow \quad b_{n-3} = a_{n-2} + b_{n-2}x_0$$

$$- - - - - - - - - - -$$

$$a_k = b_{k-1} - b_k x_0 \quad \Rightarrow \quad b_{k-1} = a_k + b_k x_0$$

$$- - - - - - - - - - -$$

$$a_1 = b_0 - b_1 x_0 \quad \Rightarrow \quad b_0 = a_1 + b_1 x_0$$

$$a_0 = c - b_0 x_0 \quad \Rightarrow \quad c = a_0 + b_0 x_0$$

Легко бачити, що рекурсивно обчислюються всі коефіцієнти b_k, $k = 0,1, \ldots$, починаючи з $b_{n-1} = a_n$. До того ж, за допомогою схеми Горнера обчислюється $c = f(x_0)$ і у загальному випадку це здійснюється меншою кількістю операцій множення, ніж при безпосередньому обчисленні $f(x_0)$: дійсно, при безпосередньому обчисленні x_0^n здійснюється $(n-1)$ множення плюс n множень на коефіцієнти, тобто усіх $2n-1$ множень, а у схемі Горнера всього n множень, що випливає із n співвідношень справа при обчисленні c.

ЛЕКЦІЯ 12. **ВЛАСТИВОСТІ КОРЕНІВ МНОГОЧЛЕНА. ОСНОВНА ТЕОРЕМА АЛГЕБРИ**

Раціональні корені многочлена з цілими числами

Теорема 12.1. *Нехай* $x_0 = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}$ *нескоротний дріб – корінь многочлена*

$$a_0 + a_1 x + \cdots + a_n x^n = 0,$$

де $a_k \in \mathbb{Z}$. *Тоді* $a_0 \vdots p$, $a_n \vdots q$.

Доведення. Помноживши на q^n рівність

$$a_0 + a_1\frac{p}{q} + a_2\left(\frac{p}{q}\right)^2 \ldots + a_n\left(\frac{p}{q}\right)^n = 0,$$

маємо

$$a_0 q^n + \underline{a_1 p q^{n-1} + \cdots + a_1 q p^{n-1} + a_n p^n} = 0.$$

Оскільки підкреслена знизу частина виразу ділиться на p, а q і p – взаємно прості, то a_0 ділиться на p. Аналогічно, підкреслена зверху частина виразу

$$\overline{a_0 q^n + a_1 p q^{n-1} + \cdots + a_1 q p^{n-1}} + a_n p^n = 0.$$

ділиться на q, отже, a_n ділиться на q, оскільки q і p – взаємно прості.

Теорема 12.2 (Вієта). *Нехай* $\mathbb{F}$ *– поле і* $x_1, x_2, \ldots, x_n \in \mathbb{F}$ *– корені (серед них можуть бути однакові, тобто кратні) многочлена* $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$*, де* $a_k \in \mathbb{F}$*. Тоді*

$$f(x) = (x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_n) \qquad (12.1)$$

і мають місце співвідношення, які називають формулами Вієта:

$$a_{n-1} = -(x_1 + x_2 + \cdots + x_n);$$

$$a_{n-2} = x_1x_2 + x_1x_3 + \cdots x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n;$$

$$a_{n-3} = -(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n);$$

$$- - - - - - - - - - - - - - - -$$

$$a_0 = (-1)^n x_1x_2 \ldots x_n.$$

Доведення. Формула (12.1) є прямим наслідком теореми 11.2 (Безу). Дійсно, оскільки x_1 корінь $f(x)$, то існує многочлен $q(x) \in \mathbb{F}[x]$ такий, що

$$f(x) = (x - x_1) \cdot q_1(x).$$

Далі, многочлен $q(x)$ у свою чергу має корінь x_2 і тоді існує многочлен $q_2(x) \in \mathbb{F}[x]$ такий, що $q_1(x) = (x - x_2) \cdot q_2(x)$, тобто

$$f(x) = (x - x_1) \cdot (x - x_2) \cdot q_2(x).$$

Продовжуємо цей процес поки вичерпаємо всі корені.

Перемножуючи дужки у правій частині (12.1) і прирівнюючи коефіцієнти при однакових степенях змінної x, одержимо формули Вієта.

Якщо головний коефіцієнт a_n многочлена $f(x)$ не дорівнює одиниці, то неважко переконатись, що формули Вієта запишуться з тою різницею, що у лівих частинах замість a_k потрібно поставити $\frac{a_k}{a_n}$, $k = 1, \dots, n-1$.

Основна теорема алгебри

Теорема 12.3 (Основна теорема алгебри комплексних чисел). *Нехай $f(x) \in \mathbb{C}[x]$, тоді існує $x_0 \in \mathbb{C}$ такий, що $f(x_0) = 0$. Іншими словами, будь-який многочлен з комплексними коефіцієнтами має хоча б один корінь у полі комплексних чисел.*

Теорему приймаємо без доведення. Найпростіше доведення теореми 12.3 здійснюється в курсі комплексного аналізу за допомогою теореми Ліувілля.

Наслідок 12.1. *Будь-який многочлен $f(x) \in \mathbb{C}[x]$ степені $n \geq 1$ має рівно n коренів з урахуванням кратності.*

Наслідок 12.2. *Будь-який многочлен $f(x) \in \mathbb{C}[x]$ степені $n \geq 1$ ($f(x) = a_0 + a_1 x + \cdots + a_n x^n$) розкладається в добуток n лінійних множників:*

$$f(x) = a_n(x - x_1) \cdot (x - x_2) \cdot \dots \cdot (x - x_n), \qquad (12.2)$$

причому цей розклад єдиний.

Доведення. Коефіцієнт a_n присутній у розкладі $f(x)$ з тієї причини, що після розкриття дужок у правій частині при x^n має бути коефіцієнт a_n, тобто

$\text{coef}(f) = a_n$. Покажемо єдиність розкладу (12.2): припустимо, що існує інший розклад многочлена

$$f(x) = a_n(x - y_1) \cdot (x - y_2) \cdot \ldots \cdot (x - y_n) \qquad (12.3)$$

Із (12.2) та (12.3) випливає, що

$$(x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_n) = (x - y_1) \cdot (x - y_2) \cdot \ldots \cdot (x - y_n). \quad (12.4)$$

Якби якийсь корінь x_k у лівій частині (12.4) був відмінний від усіх коренів y_l, $l = 1, \ldots, n$ у правій частині (12.4), то, підставляючи його у (12.4) ми отримали б зліва нуль, а справа число, відмінне від нуля. Аналогічно для якби якийсь корінь y_l у правій частині (12.4) не збігався з жодним x_i, $i = 1, \ldots, n$ у лівій частині (12.4). Отже, будь-який x_k рівний деякому y_l і навпаки.

Звідси ще не випливає єдиність розкладу (12.2), оскільки аргументи вище не заперечують, що якійсь однакові корені справа і зліва в (12.4) можуть мати різну кратність. Покажемо, що це також не можливо. Дійсно, припустимо, що кратність якогось кореня, наприклад x_1 зліва більша ніж справа, а саме $(x - x_1)^l$ знаходиться зліва і $(x - x_1)^m$ знаходиться справа при цьому $l > m$. Тоді, скоротивши праву і ліву частини (12.2) на $(x - x_1)^m$ отримаємо рівність, де справа немає множника $(x - x_1)$, а зліва є множник $(x - x_1)^{l-m}$, що не можливо згідно вищеописаних аргументів.

Лема 12.1. *Якщо многочлени* $f, g \in \mathbb{C}[x]$ *такі, що* $\deg(g) \leq n$, $\deg(f) \leq n$, *мають рівні значенні у більш ніж* n *різних точках, то* $f(x) = g(x)$.

Доведення. Розглянемо многочлен $f(x) - g(x)$. За припущеннями леми він має більш ніж n коренів і при цьому його степінь не більший n, а це можливо, коли $\forall x \in \mathbb{C}$, $f(x) - g(x) = 0$.

Отже, многочлен степені не більше n однозначно визначається своїми значеннями у $(n + 1)$ різних точках.

Інтерполяційна формула Лагранжа

Припустимо, що перед нами стоїть задача побудови многочлена степені не вище n, який при різних значеннях змінної $x_1, x_2, \dots, x_{n+1}$ приймають відповідні значення $c_1, c_2, \dots, c_{n+1}$. Такий многочлен f визначається формулою

$$f(x) = \sum_{k=1}^{n+1} \frac{c_k(x - x_1) \dots (x - x_{k-1})(x - x_{k+1}) \dots (x - x_{n+1})}{(x_k - x_1) \dots (x_k - x_{k-1})(x_k - x_{k+1}) \dots (x_k - x_{n+1})}.$$

Дійсно, безпосередньою підстановкою неважко переконатись, що $f(x_k) = c_k$, $k = 1, \dots, n+1$.

ЛЕКЦІЯ 13. **РОЗШИРЕННЯ КІЛЕЦЬ І ПОЛІВ**

Означення 13.1. *Якщо кільце* $(\mathcal{R}_1, +, \cdot)$ *є підкільцем кільця* $(\mathcal{R}, +, \cdot)$, *то* $(\mathcal{R}, +, \cdot)$ *називається розширенням кільця* $(\mathcal{R}_1, +, \cdot)$. *Якщо* $(\mathcal{R}_1, +, \cdot)$ та $(\mathcal{R}, +, \cdot)$ – *поля, то* $(\mathcal{R}, +, \cdot)$ *називається розширенням поля* $(\mathcal{R}_1, +, \cdot)$.

Через $\mathcal{R}/\mathcal{R}_1$ позначається розширенням кільця (поля) $(\mathcal{R}_1, +, \cdot)$ до кільця (поля) $(\mathcal{R}, +, \cdot)$.

Приклади

1. Кільце $(\mathbb{Z}[i], +, \cdot)$, $(\mathbb{Z}[i] = \{n + mi\ , n, m \in \mathbb{Z}\}$ – множина гауссових чисел) є розширенням кільця $(\mathbb{Z}, +, \cdot)$.
2. $\mathbb{Z}[\omega] = \{n + m\omega\ | n, m \in \mathbb{Z}\}$, де $\omega = \sqrt[3]{1}$ – множина чисел Ейзенштейна. $(\mathbb{Z}[\omega], +, \cdot)$ – розширення кільця $(\mathbb{Z}, +, \cdot)$.
3. Поле комплексних чисел $(\mathbb{C}, +, \cdot)$ є розширенням поля дійсних чисел $(\mathbb{R}, +, \cdot)$.

Лінійний простір

Означення 13.2. *Лінійним (або векторним) простором над полем* $\mathbb{F}$ *називається непорожня множина* L *з операціями додавання* $+$ *та множення на елементи поля* $\mathbb{F}$, *які задовольняють умови* $\forall a, b, c \in L, \forall \lambda, \mu \in \mathbb{F}$:

I. $a + b = b + a$;

II. $(a + b) + c = a + (b + c)$;

III. $\exists 0 \in L: a + 0 = a$;

IV. $\exists(-a) \in L: a + (-a) = 0$;

V. $1a = a$;

VI. $\lambda(a + b) = \lambda a + \lambda b$;

VII. $\lambda(\mu a) = (\lambda\mu)a$;

VIII. $(\lambda + \mu)a = \lambda a + \mu a$.

Легко перевірити, що будь яке розширення $\mathbb{P}/\mathbb{F}$ поля $(\mathbb{F}, +, \cdot)$ до поля $(\mathbb{P}, +, \cdot)$ є векторним простором $\mathbb{P}$ над полем $\mathbb{F}$. Розмірність цього векторного простору позначається $[\mathbb{P}: \mathbb{F}]$.

Означення 13.3. *Розширення* $\mathbb{P}/\mathbb{F}$ *називається скінченним, якщо векторний простором* $\mathbb{P}$ *над полем* $\mathbb{F}$ *є скінченновимірним, тобто* $[\mathbb{P}: \mathbb{F}] < \infty$. *У противному випадку розширення* $\mathbb{P}/\mathbb{F}$ *називається нескінченним. При цьому* $[\mathbb{P}: \mathbb{F}]$ *називають степенем розширення.*

По іншому, розширення $(\mathbb{P}, +, \cdot)$ поля $(\mathbb{F}, +, \cdot)$ є скінченним, якщо існують елементи $a_0, a_1, \dots, a_n \in \mathbb{P}$ такі, що кожен елемент $b \in \mathbb{P}$ єдиним чином зображується у вигляді

$$b = \beta_1 a_1 + \cdots + \beta_n a_n,$$

де $\beta_k \in \mathbb{F}$, $k = 1,2, \dots, n$.

Приклади

1) Поле $\left(\mathbb{Q}[\sqrt{2}], +, \cdot\right)$, де $\mathbb{Q}\left[\sqrt{2}\right] = \left\{x + y\sqrt{2} \,|x, y \in \mathbb{Q}\right\}$ є скінченим розширенням поля $\mathbb{Q}$, оскільки $\left[\mathbb{Q}\left[\sqrt{2}\right]: \mathbb{Q}\right] = 2$.
2) Поле комплексних чисел $(\mathbb{C}, +, \cdot)$ є скінченим розширенням поля дійсних чисел $(\mathbb{R}, +, \cdot)$, оскільки $\mathbb{C} = \mathbb{R}[i] = \{x + yi \,|x, y \in \mathbb{R}\}$ і $[\mathbb{C}: \mathbb{R}] = 2$.
3) Поле дійсних чисел $(\mathbb{R}, +, \cdot)$ є нескінченним розширенням поля раціональних чисел $(\mathbb{Q}, +, \cdot)$.

4) Поле гаусових чисел $(\mathbb{Q}[i], +, \cdot)$, де $\mathbb{Q}[i] = \{x + yi \mid x, y \in \mathbb{Q}\}$ є скінченим розширенням поля $\mathbb{Q}$

Означення 13.4. *Нехай* $(\mathbb{F}, +, \cdot)$, $(\mathbb{P}, +, \cdot)$, $(\mathbb{H}, +, \cdot)$ *– поля. Тоді співвідношення* $\mathbb{F} \subset \mathbb{P} \subset \mathbb{H}$ *називають вежею полів.*

Лема 13.1. *Для вежі полів* $\mathbb{F} \subset \mathbb{P} \subset \mathbb{H}$ *має місце*

$$[\mathbb{P}: \mathbb{F}] = [\mathbb{H}: \mathbb{P}][\mathbb{P}: \mathbb{F}].$$

Доведення. Нехай E – базис в $\mathbb{P}/\mathbb{F}$, а B – базис в $\mathbb{H}/\mathbb{P}$. Тоді множина

$\{x \cdot y \mid x \in E, y \in B\} \subset \mathbb{P}$ – базис в $\mathbb{P}$.

Нехай $\mathbb{F}$ – деяке числове поле і $a_1, \dots, a_n \in \mathbb{C}$ – довільні числа.

Означення 13.5. *Найменше поле, яке містить одночасно* $\mathbb{F}$ *і* $a_1, \dots, a_n$ *називається розширенням, породженим числами* $a_1, \dots, a_n$.

Це поле існує, оскільки серед таких полів є поле $\mathbb{C}$ і перетин усіх полів, що містять $\mathbb{F}$ та $a_1, \dots, a_n$, є полем. (Переконатись самостійно!).

Розширення поля $\mathbb{F}$, породжене числами $a_1, \dots, a_n$ позначається через $\mathbb{F}[a_1, \dots, a_n]$.

Означення 13.6. *Число* a *називається алгебраїчним над полем* $(\mathbb{F}, +, \cdot)$, *якщо* a *є коренем деякого ненульового многочлена з коефіцієнтами із* $\mathbb{F}$. *Неалгебраїчні числа називаються трансцедентними.*

Наприклад, $\sqrt{2}$ є алгебраїчним над полем раціональних чисел, оскільки $\sqrt{2}$ є коренем рівняння $x^2 - 2 = 0$, а $\sqrt[4]{3}i$ – алгебраїчне над полем дійсних чисел, як корінь рівняння $x^2 + \sqrt{3} = 0$.

Якщо будь-яке алгебраїчне число над полем $(\mathbb{F}, +, \cdot)$ належить $\mathbb{F}$, то поле називається *алгебраїчно замкнутим*.

Із основної теореми алгебри комплексних чисел випливає, що поле комплексних чисел є алгебраїчно замкнутим.

Означення 13.7. *Розширення* $(\mathbb{P}, +, \cdot)$ *поля* $(\mathbb{F}, +, \cdot)$ *називається алгебраїчно породженим, якщо існують алгебраїчні над полем* $\mathbb{F}$ *числа* $a_1, \dots, a_n$ *такі, що* $\mathbb{P} = \mathbb{F}[a_1, a_2, \dots, a_n]$. *Якщо* $n = 1$, *то* $\mathbb{P} = \mathbb{F}[a_1]$ *називається простим алгебраїчним розширенням.*

Означення 13.8. *Розширення* $(\mathbb{P}, +, \cdot)$ *поля* $(\mathbb{F}, +, \cdot)$ *називається складово алгебраїчним розширенням, якщо існує такий ланцюжок підполів*

$$\mathbb{F} = L_1 \subset L_2 \subset \cdots \subset L_r = \mathbb{P},$$

що для довільного $k = 2, \dots, r$ *поле* L_k *є простим алгебраїчним розширенням поля* L_{k-1}.

Означення 13.9. *Розширення* $(\mathbb{P}, +, \cdot)$ *поля* $(\mathbb{F}, +, \cdot)$ *називається алгебраїчним, якщо будь-який елемент поля* $\mathbb{P}$ *є алгебраїчним над полем* $\mathbb{F}$.

Алгебраїчність скінченних розширень

Теорема 13.1. *Будь-яке скінченне розширення є алгебраїчним.*

Доведення. Нехай $\mathbb{P}/\mathbb{F}$ – скінченне розширення і $[\mathbb{P}: \mathbb{F}] = n \in \mathbb{N}$. Для довільного $b \in \mathbb{P}$ вектори 1, b,…, b^n – лінійно залежні як $n + 1$ вектор в n-вимірному просторі. Отже, існують числа $\beta_0, \beta_1, \dots, \beta_n$ такі, що

$$\beta_0 + \beta_1 b + \cdots + \beta_n b^n = 0.$$

Тобто b – є алгебраїчним числом як корінь многочлена $\beta_0 + \beta_1 x + \cdots + \beta_n x^n$.

Наслідок 13.1. *Поле дійсних чисел не є скінченним розширенням поля раціональних чисел, оскільки числа* π *та* e *– неалгебраїчні, тобто трансцедентні* (*приймається без доведення*).

Означення 13.10. *Розширення, що містить трансцендентні елементи називається трансцендентним розширенням.*

Очевидно, що поле дійсних чисел є трансцедентним розширенням раціональних чисел.

Поле алгебраїчних чисел

Означення 13.11. *Підмножина A комплексних чисел називається множиною цілих алгебраїчних чисел, якщо будь-яке $x \in A$ є коренем ненульового многочлена $f(x) = a_0 + a_1x + \cdots + a_nx^n$ над полем раціональних чисел, тобто є розв'язком рівняння*

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0, \qquad (13.1)$$

де $a_k \in \mathbb{Q}$, $a_n \neq 0$, $n \in \mathbb{N}$.

Наприклад, будь-яке раціональне число r є алгебраїчним, оскільки це число – розв'язок рівняння

$$x - r = 0.$$

Інший приклад: i, $-i$ є алгебраїчними числами, оскільки вони розв'язки рівняння

$$x^2 + 1 = 0.$$

Будь-яке неалгебраїчне комплексне число називається *трансцедентним*.

Твердження 13.1. *Якщо $t \in A$, то $-t \in A$.*

Доведення. Дійсно, якщо $t \in A$, то існує многочлен $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, де $a_k \in \mathbb{Q}$, $a_n \neq 0$, $n \in \mathbb{N}$ такий, що t є його корінь, тобто

$$a_nt^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0 = 0.$$

Якщо n парне, то легко бачити, що $-t$ задовольняє рівняння

$$a_nx^n - a_{n-1}x^{n-1} + a_{n-2}t^{n-2} - \cdots + a_2x^2 - a_1x + a_0 = 0.$$

Отже, $-t$ є також алгебраїчним числом.

Вправа 13.1. Розглянути випадок, коли $n \in \mathbb{N}$ непарне.

Вправа 13.2. Довести, що якщо $t, s \in A$, то $t + s \in A$, $t \cdot s \in A$, а коли $s \neq 0$, то $\frac{t}{s} \in A$. Тобто $(A, +, \cdot)$ є полем, яке називається *полем алгебраїчних чисел*.

Вправа 13.3. Довести, що не існує власного підполя поля раціональних чисел $\mathbb{Q}$.

ЛЕКЦІЯ 14. **МНОГОЧЛЕНИ ВІД ДЕКІЛЬКОХ ЗМІННИХ**

Означення 14.1. *Многочленом $f(x_1, x_2, \dots, x_n)$ від n невідомих $x_1, x_2, \dots, x_n$ над полем $\mathbb{F}$ називається сума скінченного числа членів виду $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$, де $k_i \geq 0$ з коефіцієнтами із $\mathbb{F}$.*

Позначається $f \in \mathbb{F}[x_1, x_2, \dots, x_n]$.

Означення 14.2. *Многочлени від n невідомих $x_1, x_2, \dots, x_n$ над полем $\mathbb{F}$ $f(x_1, x_2, \dots, x_n)$ та $g(x_1, x_2, \dots, x_n)$ називаються рівними, якщо рівні їх коефіцієнти при однакових членах.*

Степенем члена $x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$ називається число $k_1 + k_2 + \dots + k_n$.

Означення 14.3. *Степенем многочлена $f(x_1, x_2, \dots, x_n)$ називається найбільший степінь його членів. Якщо многочлен містить декілька членів з найбільшим степенем, то для визначення старшого члена многочлена використовується лексикографічне правило.*

Наприклад, член $x_1^2 x_2$ вважається старшим від $x_1 x_2^2$. Член $x_1^3 x_2 x_3^2$ старший від $x_1^3 x_3^3$.

Означення 14.4. *Сумою многочленів $f(x_1, x_2, \dots, x_n)$ та $g(x_1, x_2, \dots, x_n)$ називається многочлен, коефіцієнти якого отримуються додаванням відповідних коефіцієнтів многочленів f і g,якщо при цьому деякий член входить лиш в один із многочленів f і g, то коефіцієнт при ньому в іншому многочлені вважається рівним нулю.*

Добуток двох одночленів $ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ та $bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}$ визначається рівністю

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}\cdot bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}=(ab)x_1^{k_1+l_1}x_2^{k_2+l_1}\dots x_n^{k_n+l_1}.$$

Означення 14.5. *Добутком многочленів $f(x_1,x_2,\dots,x_n)$ та $g(x_1,x_2,\dots,x_n)$ називається многочлен, який отримується у результаті почленного перемноження і зведення подібних одночленів.*

Неважко переконатись, що за цих операцій $\mathbb{F}[x_1,x_2,\dots,x_n]$ є комутативним кільцем, що не містить дільників нуля.

Симетричні многочлени

Нехай M – скінченна множина, що містить n елементів. Для спрощення викладок припустимо, що $M=\{1,2,\dots,n\}$. Перестановкою (або підстановкою) множини M називається довільна бієкція $\varphi\colon M\to M$. Очевидно, що існує $n!$ перестановок множини M.

Сукупність усіх перестановок множини M позначимо через S_n.

Означення 14.6. *Многочлен $f\in\mathbb{F}[x_1,x_2,\dots,x_n]$ називається симетричним, якщо*

$$f\left(x_{\varphi(1)},x_{\varphi(2)},\dots,x_{\varphi(n)}\right)=f(x_1,x_2,\dots,x_n),\qquad\forall\varphi\in S_n.$$

Приклади

1. $x_1x_2x_3$;
2. $x_1x_2+x_1^2x_2^2+x_1^3x_2^3$;
3. $x_1^2+x_2^2+x_3^2+2x_1x_2x_3$;
4. $S_k=x_1^k+x_2^k+\dots+x_n^k$, $k\in\mathbb{N}$ – степеневі суми;
5. $V(x_1,x_2,\dots,x_n)=\prod_{1\le i<j\le n}\left(x_j-x_i\right)^2$.
6. Прикладом несиметричного многочлена є многочлен $x_1x_2+x_2x_3$. Дійсно, при підстановці $\varphi\in S_3$:

$$\varphi=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

тобто $\varphi(1) = 2, \varphi(2) = 1, \varphi(3) = 3$, маємо

$$x_2x_1 + x_1x_3 \neq x_1x_2 + x_2x_3.$$

Елементарні симетричні многочлени

Елементарними симетричними многочленами від n невідомих $x_1, x_2, \dots, x_n$ є многочлени виду:

1. $\sigma_1(x_1, x_2, \dots, x_n) = x_1 + x_2 + \cdots + x_n$;
2. $\sigma_2(x_1, x_2, \dots, x_n) = x_1x_2 + x_1x_3 + \cdots x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n$;
3. $\sigma_3(x_1, x_2, \dots, x_n) = -(x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n)$;

– – – – – – – – – – –

4. $\sigma_n(x_1, x_2, \dots, x_n) = x_1x_2 \dots x_n$.

Загальний вигляд такого многочлена такий

$$\sigma_k(x_1, x_2, \dots, x_n) = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} x_{i_1}x_{i_2} \dots x_{i_k}, k = 1,2, \dots, n.$$

Інколи для повноти вводять многочлен $\sigma_0(x_1, x_2, \dots, x_n) = 1$.

Важливою властивістю симетричних многочленів є така:

Твердження 14.1. *Якщо* $f_1(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n)$ – *набір симетричних многочленів із* $\mathbb{F}[x_1, x_2, \dots, x_n]$ *і* $G(y_1, y_2, \dots, y_k)$ – *довільний многочлен від невідомих* $y_1, y_2, \dots, y_k$, *то* $G\big(f_1(x_1, x_2, \dots, x_n), \dots, f_k(x_1, x_2, \dots, x_n)\big)$ – *симетричний многочлен.*

Вправа 14.1. Довести твердження 14.1.

Основна теорема про симетричні многочлени

Теорема 14.1. *Для будь-якого симетричного многочлена* $h(x_1, x_2, \dots, x_n) \in \mathbb{F}[x_1, x_2, \dots, x_n]$ *існує єдиний многочлен* $G(y_1, y_2, \dots, y_n) \in \mathbb{F}[y_1, y_2, \dots, y_n]$ *такий, що*

$$h(x_1, x_2, \dots, x_n) = G\big(\sigma_1(x_1, x_2, \dots, x_n), \sigma_2(x_1, x_2, \dots, x_n), \dots, \sigma_n(x_1, x_2, \dots, x_n)\big),$$

де G не обов'язково симетричний.

Приклад 14.1. Нехай $h(x_1, x_2, \dots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$. Тоді легко бачити, що

$$x_1^2 + x_2^2 + \cdots + x_n^2 = (x_1 + x_2 + \cdots + x_n)^2 - 2(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n)$$
$$= \big(\sigma_1(x_1, x_2, \dots, x_n)\big)^2 - 2\sigma_2(x_1, x_2, \dots, x_n).$$

Тобто

$$G(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2.$$

Вправа 14.2. Переконайтесь, що якщо $h(x_1, x_2, \dots, x_n) = x_1^3 + x_2^3 + \cdots + x_n^3$, то $h = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$.

Доведення. Спочатку доведемо дві допоміжні леми:

Лема 14.1. *Нехай $ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n}$ – старший член симетричного многочлена $f(x_1, x_2, \dots, x_n)$. Тоді $k_1 \geq k_2 \geq \cdots \geq k_n$.*

Доведення леми 14.1. Від супротивного, нехай для деякого $1 \leq i \leq n$, $k_i < k_{i+1}$. Оскільки f – симетричний, то, помінявши місцями $x_i^{k_i}$ та $x_{i+1}^{k_{i+1}}$ отримаємо одночлен, який також входить у суму многочлена f і при цьому за лексикографічним правилом цей одночлен старший від початкового, що суперечить припущенню.

Лема 14.2. *Для будь-якого члена $g = x_1^{k_1}x_2^{k_2} \dots x_n^{k_n}$, у якого $k_1 \geq k_2 \geq \cdots \geq k_n$, існує єдиний набір невід'ємних цілих чисел $l_1, l_2, \dots, l_n$ таких, що старший член многочлена $\sigma_1^{l_1}\sigma_2^{l_2} \dots \sigma_n^{l_n}$ збігається з g.*

Доведення леми 14.2. Легко бачити, що старшим членом σ_k є $x_1x_2 \dots x_k$. Звідки випливає, що старшим членом многочлена $\sigma_1^{l_1}\sigma_2^{l_2} \dots \sigma_n^{l_n}$ є $x_1^{l_1}(x_1x_2)^{l_2} \dots (x_1x_2 \dots x_n)^{l_n} = x_1^{l_1+l_2+\cdots+l_n}x_2^{l_2+\cdots+l_n} \dots x_n^{l_n}$. Порівнюючи цей старший член з g, маємо

$$\begin{cases} l_1 + l_2 + \cdots + l_n = k_1 \\ l_2 + \cdots + l_n = k_2 \\ - - - - - - - - - \\ l_n = k_n \end{cases}$$

Ця система має єдиний невід'ємний розв'язок:

$$l_i = k_i - k_{i+1} \geq 0, i = 1, \dots, n-1,$$

$$l_n = k_n.$$

Перейдемо до *доведення теореми*. Якщо симетричний многочлен $h = 0$, то $G = 0$.

Нехай $h \neq 0$, а $g_1 = ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n}$ – його старший член. Згідно леми 14.1 $k_1 \geq k_2 \geq \cdots \geq k_n$, а за лемою 14.2 існує $G_1 \in \mathbb{F}[x_1, x_2, \dots, x_n]$ такий, що старший член $G_1(\sigma_1, \sigma_2, \dots, \sigma_n)$ дорівнює $g_1 = ax_1^{k_1}x_2^{k_2} \dots x_n^{k_n}$.

Розглянемо многочлен

$$h_1 = h - G_1(\sigma_1, \sigma_2, \dots, \sigma_n).$$

Якщо $h_1 = 0$, то $G = G_1$ – шуканий многочлен. Якщо ж $h_1 \neq 0$ і g_2 – його старший член, то за лексикографічним правилом $g_1 > g_2$.

Крім цього, існує $G_2 \in \mathbb{F}[x_1, x_2, \dots, x_n]$ такий, що старший член $G_2(\sigma_1, \sigma_2, \dots, \sigma_n)$ дорівнює g_2. Розглянемо многочлен $h_2 = h_1 - G_2(\sigma_1, \sigma_2, \dots, \sigma_n)$.

Якщо $h_2 = 0$, то, оскільки $h_1 = h - G_1$, шуканий многочлен G має вигляд $G = G_1 + G_2$. Якщо ж $h_2 \neq 0$ і g_3 – його старший член, то за лексикографічним правилом $g_2 > g_3$. Продовжуємо цей процес допоки за лемою 14.1, з урахуванням $g_1 > g_2 > \cdots$, на певному кроці m ми отримаємо $h_m = 0$. Звідки

$$G = G_1 + G_2 + \cdots + G_m.$$

Доведемо, що многочлен G єдиний. Нехай існує інший многочлен $H \in \mathbb{F}[y_1, y_2, \dots, y_n]$ такий, що

$$h(x_1, x_2, \dots, x_n) = H\big(\sigma_1(x_1, x_2, \dots, x_n), \sigma_2(x_1, x_2, \dots, x_n), \dots, \sigma_n(x_1, x_2, \dots, x_n)\big).$$

Розглянемо многочлен $P = G - H$. За припущенням $P \neq 0$ але при цьому $P(\sigma_1, \sigma_2, \dots, \sigma_n) = 0$. Нехай $P_1(\sigma_1, \sigma_2, \dots, \sigma_n)$, …, $P_s(\sigma_1, \sigma_2, \dots, \sigma_n)$ – одночлени, які

входять як доданки в P, а $p_1, \ldots, p_s$ їх старші члени відповідно. За лемою 14.2 без урахування сталих коефіцієнтів $p_1, \ldots, p_s$ лексикографічно різні. Без обмеження загальності припустимо, що p_1 є старший серед них. Тоді p_1 старший за усі члени не тільки P_1, а й усі члени многочленів $P_1(\sigma_1, \sigma_2, \ldots, \sigma_n), \ldots, P_s(\sigma_1, \sigma_2, \ldots, \sigma_n)$. Тому після зведення подібних він залишиться у сумі

$$P_1(\sigma_1, \sigma_2, \ldots, \sigma_n) + \cdots + P_s(\sigma_1, \sigma_2, \ldots, \sigma_n).$$

Звідки випливає, що $P(\sigma_1, \sigma_2, \ldots, \sigma_n) \neq 0$. Отримали суперечність через припущення, що многочлен G не єдиний.

Напишемо теорему 12.2 (Вієта) з використанням елементарних симетричних многочленів:

Нехай $\mathbb{F}$ *– поле і* $x_1, x_2, \ldots, x_n \in \mathbb{F}$ *– корені (серед них можуть бути кратні) многочлена* $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n$, *де* $a_k \in \mathbb{F}$. *Тоді мають місце співвідношення*:

$$\sigma_k(x_1, x_2, \ldots, x_n) = (-1)^k \frac{a_{n-k}}{a_n}, \qquad k = 1,2, \ldots, n. \tag{14.1}$$

Вправа 14.3. Переконатись у правильності формули (14.1).

За допомогою формул (14.1) та основної теореми про симетричні многочлени можна виразити довільний симетричний многочлен від коренів многочлена через коефіцієнти a_k, $k = 0,1, \ldots, n$ цього многочлена, не знаючи при цьому самих коренів.

Приклад 14.2. Нехай $f(x) = 1 + x + \sqrt{7}x^2 + 3x^3 + 4x^4 + x^5$. Знайдемо суму квадратів коренів $x_1, x_2, x_3, x_4, x_5 \in \mathbb{C}$ цього многочлена. Із прикладу 14.1 відомо, що сума цих квадратів виражається через елементарні симетричні многочлени так:

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = \big(\sigma_1(x_1, x_2, x_3, x_4, x_5)\big)^2 - 2\sigma_2(x_1, x_2, x_3, x_4, x_5).$$

З урахуванням формул (15.1) $\sigma_1(x_1, x_2, x_3, x_4, x_5) = -\frac{a_4}{a_5} = -4$, а $\sigma_2(x_1, x_2, x_3, x_4, x_5) = \frac{a_3}{a_5} = 3$. Отже,

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = 16 - 6 = 10.$$

Відзначимо, що самих коренів ми навіть не можемо обчислити, оскільки корені цього рівняння 5-го степеню не виражаються у радикалах через свої коефіцієнти.

Вправа 14.4. Знайти суму кубів коренів многочлена

$$f(x) = 1 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 6x^6.$$

Приклад 14.3. Розв'язати систему рівнянь

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1^2 + x_2^2 + x_3^2 = 0 \\ x_1^3 + x_2^3 + x_3^3 = 3 \end{cases} \tag{14.2}$$

де $x_1, x_2, x_3 \in \mathbb{C}$.

Розв'язання. Маємо

$$x_1 + x_2 + x_3 = \sigma_1 = 0,$$

$$x_1^2 + x_2^2 + x_3^2 = \sigma_1^2 - 2\sigma_2 = 0,$$

$$x_1^3 + x_2^3 + x_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 3.$$

Звідки $\sigma_1 = \sigma_2 = 0$, $\sigma_3 = 1$.

З використанням формул (14.1), побудуємо многочлен, для якого x_1, x_2, x_3 є коренями, за умови, що головний коефіцієнт $a_3 = 1$, маємо

$$f(x) = x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = x^3 - 1.$$

Корені цього многочлена 1, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Всього система (14.2) має $3! = 6$ розв'язків, які одержуємо перестановками значень x_1, x_2, x_3.

ІІ ЕЛЕМЕНТИ АЛГЕБРИ

ЛЕКЦІЯ 15. АЛГЕБРАЇЧНІ ОПЕРАЦІЇ. АЛГЕБРАЇЧНІ СТРУКТУРИ

Нехай $X \neq \emptyset$ деяка множина. Через X^n будемо позначати декартовий добуток множини X на себе n разів, тобто $X^n = \underbrace{X \times X \times \ldots \times X}_{n}$, де $n \in \mathbb{Z}_+ = \mathbb{N} \cup \{0\}$.

Означення 15.1. *Відображення $f: X^n \to X$ називається n-арною алгебраїчною операцією на X.*

Зауваження 15.1. Надалі під n-арною операцією будемо мати на увазі саме внутрішню n-арну операцію, тобто, коли результат операції має ту ж природу, що і множники. Наприклад, векторний добуток векторів. Скалярний же добуток векторів не є внутрішньою бінарною операцією, оскільки у цьому випадку результат добутку векторів є скаляр, а не вектор.

Домовимось також надалі використовувати такі позначення : $\mathbb{Z}^* = \mathbb{Z}\backslash\{0\}$, $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$, $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$, $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$.

Приклади

1. Якщо $n = 2$, то операція називається бінарною. Це одна з найбільш вживаних в математиці операцій і такими є, наприклад, множення та додавання на множині дійсних чисел.
2. При $n = 1$ операція називається унарною і до таких операцій належить, наприклад, існування протилежного числа $(-n)$ для $n \in \mathbb{Z}$ чи оберненого r^{-1} для $r \in \mathbb{R}^*$.
3. Прикладами 0-арної операції є існування нейтрального елементу при додаванні дійсних чисел (нуль) та при їх множенні (одиниця).
4. При $n = 3$ операцію називають тернарною і в якості прикладу можна навести подвійний векторний добуток $[a, [b, c]]$ векторів простору a, b, c.

Із означення випливає, що бінарна операцію двох елементів $x, y \in X$ позначається як $f(x, y)$, але частіше у загальних випадках для бінарних

операцій використовуються символи *, °. Також, щоб підкреслити близькість операції до адитивних властивостей іноді використовується символ $+$, а для близькості до мультиплікативних властивостей використовується символ $\times$ та вживається відповідно адитивна та мультиплікативна термінологія.

Означення 15.2. *Алгебраїчною структурою називається непорожня множина X з довільною кількістю внутрішніх операцій довільної арності.*

Будемо позначати алгебраїчні структури у вигляді упорядкованого набору $(X, f, g, h, \dots)$, де $f, g, h, \dots$ – внутрішні операції.

Приклади

1. $(\mathbb{Z}, +)$ – алгебраїчна структура з операцією додавання на множині цілих чисел.
2. $(\mathbb{R}, -, \times)$ – алгебраїчна структура з операціями віднімання та множення на множині дійсних чисел.
3. $(\mathbb{N}, +, \uparrow)$ – алгебраїчна структура з операціями додавання та піднесення до степеню на множині натуральних чисел.

Вправа 15.1. Навести власні приклади алгебраїчних структур.

Означення 15.3. *Бінарна операція * на множині X називається*

1. *<u>Комутативною</u>, якщо* $\forall x, y \in X$,

$$x * y = y * x.$$

2. *<u>Асоціативною</u>, якщо* $\forall x, y \in X$,

$$x * (y * z) = (x * y) * z.$$

Означення 15.4. *Елемент $e_r \in X$ називається правим нейтральним елементом бінарної операції * якщо* $\forall x \in X$,

$$x * e_r = x.$$

Елемент $e_l \in X$ називається лівим нейтральним елементом бінарної операції $*$ якщо $\forall x \in X$,

$$e_l * x = x.$$

Елемент $e \in X$ називається нейтральним елементом бінарної операції $*$ якщо $\forall x \in X$,

$$x * e = e * x = x.$$

В адитивній термінології нейтральний елемент називають *нулем* операції, а в мультиплікативній *одиницею* операції.

Твердження 15.1. *Якщо існують правий нейтральний $e_r \in X$ та лівий нейтральний $e_l \in X$ елементи операції $*$, то існує нейтральний елемент $e \in X$ цієї операції, причому*

$$e_r = e_l = e.$$

Доведення. Дійсно, із означення правого і лівого елементів випливає

$$e_l = e_l * e_r = e_r.$$

Звідки випливає, що e_r (чи e_l) є нейтральним елементом операції $*$.

Означення 15.5. *Нехай e – нейтральний елемент відносно операції $*$. Елемент $x_r^{-1} \in X$ називається правим симетричним елементом до елемента $x \in X$, якщо*

$$x * x_r^{-1} = e.$$

Елемент $x_l^{-1} \in X$ називається лівим симетричним елементом до елемента $x \in X$, якщо

$$x_l^{-1} * x = e.$$

Одночасно правий і лівий симетричний елемент $x^{-1} \in X$ до елемента $x \in X$ називається симетричним елементом до x, тобто

$$x * x^{-1} = x^{-1} * x = e.$$

В адитивній термінології симетричний елемент називається протилежним, а у мультиплікативній обернений елемент.

Твердження 15.2. *Нехай $*$ асоціативна операція на X і існують правий симетричний елемент $x_r^{-1} \in X$ та лівий симетричний елемент $x_l^{-1} \in X$ до $x \in X$. Тоді існує єдиний симетричний до x елемент x^{-1}, причому*

$$x_r^{-1} = x_l^{-1} = x^{-1}.$$

Доведення. Із означення 4 випливає, що

$$x * x_r^{-1} = e = x_l^{-1} * x.$$

Помноживши рівність $x * x_r^{-1} = e$ зліва на x_l^{-1} отримаємо

$$x_l^{-1} * (x * x_r^{-1}) = x_l^{-1} * e = x_l^{-1}.$$

З іншого боку, використовуючи асоціативність, маємо

$$x_l^{-1} * (x * x_r^{-1}) = (x_l^{-1} * x) * x_r^{-1} = e * x_r^{-1} = x_r^{-1},$$

тобто $x_r^{-1} = x_l^{-1}$. Звідки випливає єдиність x_r^{-1} та x_l^{-1}. Дійсно, якщо припустити існування ще одного правого симетричного елемента $\tilde{x}_r^{-1}$ до x, то має виконуватись рівність $\tilde{x}_r^{-1} = x_l^{-1}$, а, отже, $\tilde{x}_r^{-1} = x_r^{-1}$. Аналогічно для лівого симетричного елемента.

Отже, існує і єдиний симетричний до x *елемент* x^{-1}: $x^{-1} = x_r^{-1}$ (або $x^{-1} = x_l^{-1}$).

Приклади

1. В алгебраїчній структурі $(\mathbb{R}, -)$ 0 – тільки правий нейтральний елемент.
2. В алгебраїчній структурі векторів простору із векторним добутком не існує ні правого, ні лівого нейтрального елемента.
3. В алгебраїчній структурі $(2^X, \cup)$ $\emptyset$ – нейтральний елемент, але для жодного $2^X \ni A \neq \emptyset$ не існує симетричного.

ОСНОВНІ АЛГЕБРАЇЧНІ СТРУКТУРИ З БІНАРНОЮ ОПЕРАЦІЄЮ

Означення 15.6. *Алгебраїчна структура* $(X,*)$ *називається* <u>*оперативом*</u>, *якщо* $\forall x, y \in X,\ x * y \in X$.

Приклади

1. $(\mathbb{Z}, +)$, $(\mathbb{Q},\times)$, $(\mathbb{R}, -)$ – оперативи.
2. $(\mathbb{Z}, -)$ – оператив, тоді як $(\mathbb{N}, -)$ не оператив, оскільки, наприклад, $3 - 5 = -2 \notin \mathbb{N}$.
3. $(\mathbb{Q}^*, :)$ – оператив, а $(\mathbb{Z}^*, :)$ не оператив, оскільки, наприклад, $\frac{1}{2} \notin \mathbb{Z}^*$.

Півгрупи

Означення 15.7. *Оператив* $(X,*)$ *з асоціативною операцією* $*$ *називається* <u>*півгрупою*</u>.

Приклади

1. $(\mathbb{N}, +)$, $(\mathbb{N},\cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{R},\cdot)$ – півгрупи.
2. Нехай $M_{n\times n}$ – квадратні дійсні матриці розмірності n із звичайною операцією добутку $\cdot$ цих матриць, тоді $(M_{n\times n},\cdot)$ – півгрупа.
3. Множина перехідних ймовірностей марковського процесу на вимірному просторі утворюють півгрупу (наслідок рівняння Чепмена-Колмогорова).
4. Алгебраїчна структура векторів простору із векторним добутком не є півгрупою оскільки векторний добуток не асоціативний.

Моноїди

Означення 15.8. *Півгрупа* $(X,*)$ *яка містить нейтральний елемент* e *відносно операції* $*$ *називається* <u>*моноїдом*</u>.

Позначається $(X,*,e)$.

Приклади

1. $(\mathbb{N},\cdot,1)$, $(\mathbb{Q}, +,0)$, $(\mathbb{R},\cdot)$, $(2^X,\cup,\emptyset)$, $(2^X,\cap,X)$ – моноїди.

2. $(\mathbb{N}, +)$ – не моноїд, оскільки не містить нейтрального елемента 0, але є півгрупою.
3. $(\mathbb{N}, НСК, 1)$, де НСК – це найменше спільне кратне, є моноїдом.

Вправа 15.2. Навести власні приклади моноїдів та півгруп, що не є моноїдами.

ЛЕКЦІЯ 16. **ГРУПИ**

Групи та деякі їх базові властивості

Означення 16.1. *Групою називається моноїд* $(X,*,e)$*, кожен елемент якого має симетричний, тобто* $\forall x \in X$ *існує* $x^{-1} \in X$.

Як правило для позначення груп на місці X використовують символ G.

Повне описання групи як математичної структури має вигляд: $(G, e, inv,*)$, де G – множина елементів групи, e – це 0-арна операція, яка позначає існування нейтрального елемента e групи, inv – це 1-арна операція взяття симетричного елемента, тобто $inv: G \to G$, $inv(x) = x^{-1}$, $*$ це – бінарна операція групи.

Для спрощення запису для позначення групи $(G, e, inv,*)$ будемо використовувати позначення $(G,*,e)$. Через $|G|$ позначають кількість елементів групи, яке називається порядком групи. Група $(G,*,e)$ з комутативною операцією $*$ називається абелевою. Часто для підкреслювання близькості бінарної операції групи до операції додавання (множення) групу називають адитивною (мультиплікативною).

Приклади

1. $(\mathbb{Z}, +)$ – група нескінченна (адитивна, абелева).
2. $(\mathbb{R}^*,\cdot)$ – група нескінченна (мультиплікативна, абелева).
3. $(2^X, \Delta)$, де Δ операція симетричної різниці, – абелева група.
4. $(\{+1, -1\},\cdot)$ – скінченна група 2-го порядку (мультиплікативна, абелева).

5. $(GL_{n\times n}(\mathbb{R}),\cdot)$ (де $GL_{n\times n}(\mathbb{R})$ – множина невироджених дійсних матриць розміру $n \times n$) – група (мультиплікативна, некомутативна при $n > 1$).
6. Множина комплексних чисел з модулем одиниця і операцією множення комплексних чисел – мультиплікативна абелева група.
7. Група поворотів правильного n-кутника навколо його центру, яка складається із елементів: $R_{\frac{360}{n}k}$, $k = 0,1,\dots,n-1$, де R_α – поворот -кутника на α градусів з операцією «композиція поворотів». Легко бачити, що $e = R_0$ – нейтральний елемент цієї групи.
8. Діедральна група – це група симетрій правильного n-кутника, у якій, крім поворотів навколо центру n-кутника, розглядаються відображення відносно осей симетрії цього n-кутника.

Вправа 16.1. Переконатись, що у прикладі 3 $(2^X, \Delta)$ є група (вказати нейтральний елемент, симетричний елемент до $A \in 2^X$, перевірити, що операція Δ асоціативна).

Вправа 16.2. Описати елементи діедральної групи правильного трикутника та виписати таблицю множення цих елементів (таблицю Келі).

Вправа 16.3. Нехай $(G,*,e)$ – група, $a,b \in G$. Показати, що

$$(a*b)^{-1} = b^{-1}*a^{-1}.$$

Вправа 16.4. Показати, що для тіла усі ненульові елементи утворюють групу щодо множення .

Теорема 16.1. Алгебраїчна структура $(G,*)$ є групою тоді і тільки тоді, коли виконуються умови:

1. Операція $*$ є асоціативною,
2. $\forall a,b \in G$ існують єдиний елемент $g \in G$ та єдиний елемент $h \in G$ такі, що $a*g = b$ та $h*b = a$.

Доведення. Необхідність випливає із означення групи. Дійсно, помножимо рівняння $a * g = b$ зліва на a^{-1} отримаємо $g = a^{-1} * b$. Аналогічно, помножимо рівняння $h * b = a$ справа на b^{-1} отримаємо $h = a * b^{-1}$. Тобто, g та h, які задовольняють умову 2, існують і єдині.

Достатність. Покажемо, що за умов теореми існує нейтральний елемент. Дійсно, для $\forall x \in G$ існує єдина пара елементів $g_0, h_0 \in G$ така, що $x * g_0 = x$ та $h_0 * x = x$.

Далі, із 2 випливає, що $\forall y \in G$ існує k таке, що $k * x = y$. Отже, з урахуванням умови 1, маємо

$$y * g_0 = (k * x) * g_0 = k * (x * g_0) = k * x = y.$$

Тобто, g_0 є правим нейтральним елементом алгебраїчної структури $(G,*)$. Аналогічно доводиться, що h_0 – лівий нейтральний елемент, а значить за твердженням 1.1 $g_0 = h_0 = e$ – нейтральний елемент.

Для довільного a, із рівняння $a * g = e$ (тут у якості b взято нейтральний елемент e) одержуємо, що $g = a_r^{-1}$. Аналогічно, покладаючи $b = a$ та $a = e$ у рівнянні $h * b = a$ одержуємо $h = a_l^{-1}$. Звідки за твердженням 1.2 $a^{-1} = a_r^{-1} = a_l^{-1}$.

Отже, $(G,*)$ є групою.

Наслідок 16.1. Із теореми 1 випливає правило скорочення у групі, тобто, якщо $a * g_1 = a * g_2$, то $g_1 = g_2$ і, якщо $h_1 * b = h_2 * b$, то $h_1 = h_2$.

Вправа 16.4. Довести наслідок 2.1.

Гомоморфізм груп

Означення 16.2. *Нехай* $(G_1,*)$ *та* $(G_2,\circ)$ *- групи. Гомоморфізмом групи* $(G_1,*)$ *у групу* $(G_2,\circ)$ *називається відображення* $\varphi: G_1 \to G_2$, *для якого виконується властивість* $\forall x, y \in G_1$

$$\varphi(x * y) = \varphi(x) \circ \varphi(y).$$

Приклади

1. Розглянемо відображення $\varphi: GL_{n\times n}(\mathbb{R}) \to \mathbb{R}^*$, при якому $\forall A \in GL_{n\times n}(\mathbb{R})$, $\varphi(A) = \det(A)$. Оскільки $\forall A, B \in GL_{n\times n}(\mathbb{R})$ $\varphi(AB) = \det(AB) = \det(A)\det(B)$, то φ – гомоморфізм.
2. Нехай $(G,*)$ – група. Покладемо $\forall g \in G$ $\varphi(g) = 0$. Очевидно, що φ є гомоморфізм групи $(G,*)$ у групу $(\mathbb{Z},+)$ (або у групу $(\mathbb{Q},+)$, або у групу $(\mathbb{R},+)$).

Означення 16.3. *Нехай φ – гомоморфізмом групи $(G_1,*,i)$ у групу $(G_2,\circ,e)$. Ядро гомоморфізму φ — це підмножина всіх елементів G_1, що відображаються в нейтральний елемент e групи $(G_2,\circ,e)$:*

$$\ker\varphi = \{x \in G_1 | \varphi(x) = e\}.$$

Легко бачити, що $\ker\varphi \neq \emptyset$ оскільки нейтральний елемент i групи $(G_1,*,i)$ належить до ядра, тобто $\varphi(i) = e$.

Дійсно, $\forall x \in G_1$ $\varphi(x) = \varphi(x * i) = \varphi(x) \circ \varphi(i)$, звідки $\varphi(i) = e$.

Означення 16.3. *Ізоморфізмом φ групи $(G_1,*)$ на групу $(G_2,\circ)$ називається бієктивний гомоморфізм, тобто гомоморфізм, для якого виконується умови:*

1. *якщо $x \neq y$ то $\varphi(x) \neq \varphi(y)$,*
2. $\varphi(G_1) = G_2$.

Приклади

1. Функція $\varphi(x) = e^x$ є ізоморфізмом адитивної групи $(\mathbb{R},+,0)$ на мультиплікативну групу $(\mathbb{R}_{>0},\cdot,1)$. Дійсно,
$$e^{x+y} = e^x \cdot e^y.$$
2. Функція $\varphi(x) = \ln x$ є ізоморфізмом групи $(\mathbb{R}_{>0},\cdot,1)$ на групу $(\mathbb{R},+,0)$. Дійсно,
$$\ln(x \cdot y) = \ln x + \ln y.$$

3. Функція $\varphi(a+bi)=\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ є ізоморфізмом групи $(\mathbb{C},\cdot,0)$, де $\mathbb{C}$ – комплексні числа, на групу матриць $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix},+,\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right\}$, де $a,b\in\mathbb{R}$, а $+$ – операція додавання матриць.
4. Функція $\varphi(a+bi)=\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ є ізоморфізмом групи $(\mathbb{C},\cdot,1)$, де $\mathbb{C}$ – комплексні числа, на групу матриць $\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix},\times,\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$, де $a,b\in\mathbb{R}$, а $\times$ – операція множення матриць.

Вправа 16.3. Навести свої приклади гомоморфізмів та ізоморфізмів.

Квазігрупи

Латинський квадрат n-го порядку – це таблиця $L=(l_{ij})$ розміру $n\times n$, заповнена n елементами множини M таким чином, що в кожному рядку і в кожному стовпці таблиці кожен елемент з M зустрічається рівно один раз.

Означення 16.4. *Квазігрупою називається оператив* $(X,*)$, *такий що* $\forall a,b\in X$, *існує єдиний* $x\in X$ *такий, що* $a*x=b$ *та існує єдиний* $y\in X$ *такий, що* $y*a=b$.

Будь-латинський квадрат є таблицею множення (таблицею Келі) квазігрупи.

Зауваження 16.1. Слід відзначити, що означення квазігрупи не передбачає існування нейтрального елементу.

Приклади

1. $(\mathbb{Z},-)$, $(\mathbb{R}^*,:)$ – квазігрупи без нейтрального елементу (існує тільки правий нейтральний елемент).
2. $(2^X,\Delta)$ – квазігрупа з нейтральним елементом $\emptyset$.

Вправа 16.4. Переконайтесь, що $(2^X,\Delta)$ – квазігрупа.

Вправа 16.5. Наведіть свої приклади квазігруп, у яких не існує нейтрольного елементу.

Твердження 16.1. *Якщо* $(X,*)$ *– півгрупа і квазігрупа, то* $(X,*)$ *– група.*

Доведення. Нехай $x \in X$, тоді за означенням 2.4 існує і єдиний $e \in X$ такий, що $e * x = x$. Звідки $(x * e) * x = x * (e * x) = x * x$. Позначимо $a = x * x$. Із єдності розв'язку

$$(x * e) * x = a = x * x$$

випливає, що $x * e = x$.

Аналогічно, для $\forall y \in X$, маємо $(y * e) * x = y * (e * x) = y * x$. Позначимо $b = y * x$. Із єдності розв'язку $(y * e) * x = b = y * x$. Звідки $y * e = y$.

Отже, e – нейтральний елемент. Залишилось довести існування оберненого для кожного елемента множини X.

Розглянемо довільне $a \in X$. Рівняння $a * x = e$ має розв'язок $x = a_r^{-1}$, а рівняння $x * a = e$ має розв'язок $x = a_l^{-1}$. Звідки, з урахуванням асоціативності $a_r^{-1} = a_l^{-1} = a^{-1}$.

Отже, $\forall a \in X$ існує обернений a^{-1}.

Вправи

1. Дослідити, чи є півгрупою, моноїдом, групою такі алебраїчні структури:
   a) $(\mathbb{N}, -)$;
   b) $(\mathbb{N}, +)$;
   c) $(\mathbb{Z}, +)$;
   d) $(\mathbb{R}, +)$
   e) $(\mathbb{C}, \cdot)$
2. Дослідити, чи є алгебраїчна структура $(\mathbb{R},*)$ моноїдом за операцією $a * b = a + b + ab$. Чи є $(\mathbb{R},*)$ групою?

3. Чи утворюють матриці $G = \left\{\begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}, x \in R\right\}$ групу за операцією множення матриць?

ЛЕКЦІЯ 17. **ПІДГРУПА. СИМЕТРИЧНА ГРУПА. ЦИКЛІЧНІ ГРУПИ**

Означення 17.1. *Підгрупою групи* $(G,*)$ *називається група* $(H,*)$ *щодо тої ж операції* $*$, *де* $H \subset G$.

Позначається $H \lhd G$.

Очевидно, що кожна група $(G,*,i)$ в якості півгрупи має $(i,*,i)$, тобто групу, яка складається тільки з нейтрального елементу i.

Приклади.

1. $(\mathbb{R}_{>0},\cdot)$ – підгрупа групи $(\mathbb{R}^*,\cdot)$;
2. $(\mathbb{P},+,0)$ ($\mathbb{P}$ – множина парних цілих чисел) є підгрупа групи $(\mathbb{Z},+,0)$.

Вправа 17.1. Навести свої приклади підгруп.

Теорема 17.1. *Нехай* $H \subset G$ *– непорожня підмножина, де* $(G,*,e)$ *– група.* Для того, щоб $(H,*)$ була б підгрупою групи $(G,*,e)$, необхідно і достатньо, щоб:

1. $\forall x,y \in H, x * y \in H$;
2. $\forall x \in H, x^{-1} \in H$.

Доведення. Необхідність очевидна.

Достатність. Асоціативність $*$ випливає із того, що $(G,*,e)$ – група. Оскільки $\forall x \in H, e = x * x^{-1} \in H$. Отже, $(H,*,e)$ – група, а, значить, півгрупа групи $(G,*,e)$.

Симетрична група

Нехай M – скінченна множина, що містить n елементів. Не зменшуючи загальності, припустимо, що $M = \{1,2,\dots,n\}$. Нехай φ та ψ перестановки множини M.

Композицією перестановок φ та ψ називається перетворення $\varphi \circ \psi: M \to M$ таке, що $\forall k \in M$

$$\varphi \circ \psi(k) = \varphi\big(\psi(k)\big).$$

Твердження 17.1. *Композиція перестановок φ та ψ множини M є перестановкою множини M.*

Доведення. Покажемо, що $\varphi \circ \psi$ є ін'єкцією. Дійсно, якщо $k, l \in M$ і $k \neq l$, то $\psi(k) \neq \psi(l)$, звідки $\varphi\big(\psi(k)\big) \neq \varphi\big(\psi(l)\big)$, тобто $\varphi \circ \psi$ інєкція.

Залишилось довести, що $\varphi \circ \psi$ сюр'єкція. Нехай $m \in M$, тоді, оскільки ψ бієкція існує $l \in M$ таке, що $\psi(l) = m$. Аналогічно існує $k \in M$ таке, що $\varphi(k) = l$. Звідки випливає, що $\varphi\big(\psi(k)\big) = m$ і, отже, $\varphi \circ \psi$ є бієкцією, тобто перестановкою множини M.

Означення 17.2. *Множенням $\circ$ перестановок φ* та *ψ будемо називати перестановку $\varphi \circ \psi: M \to M$, де $\varphi \circ \psi(k) = \varphi\big(\psi(k)\big)$, $\forall k \in M$.*

Особливе місце займає тотожна перестановка ε, яка кожен елемент множини M переводить в самого себе, тобто $\forall k \in M\ \varepsilon(k) = k$. Легко бачити, що для довільної перестановки φ множини M має місце

$$\varphi \circ \varepsilon = \varepsilon \circ \varphi = \varphi.$$

Із математичного аналізу добре відомо, що бієкція має обернене відображення, яке також є бієкцією. Припустимо, що перестановка φ множини M задається формулою $\varphi(k) = i_k$, $k = 1, \dots, n$. Оберненою перестановкою до перестановки φ називається перестановка

$$\varphi^{-1}(i_k) = k.$$

Неважко переконатись, що

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \varepsilon.$$

Вправа 17.1. Довести, що операція композиція перестановок асоціативна.

Позначимо через $S(M)$ – множину усіх перестановок скінченної множини M.

Означення 17.3. *Симетричною групою (або групою підстановок (перестановок)) називається група* $(S(M),\circ,\varepsilon)$.

У випадку, коли $|M| = n$, симетричну групу позначають через S_n.

Якщо n невелике, елементи групи S_n зручно зображати у вигляді таблиць. Наприклад, при $n = 3$

$$\varepsilon = \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix}, \varphi_1 = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \varphi_2 = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}, \varphi_3 = \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix},$$

$$\varphi_4 = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 1\end{pmatrix}, \varphi_5 = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}.$$

Вправа 17.2. Довести, що діедральна група трикутника (див. вправу 2.2) ізоморфна групі S_3.

Циклічні групи

Нехай $(G,*,e)$ – група, а $g \in G$ деякий її елемент. Через g^n, $n \in \mathbb{N}$ будемо позначати елемент $\underbrace{g * g * \ldots * g}_{n \text{ разів}}$, а через g^{-n} – елемент, симетричний до g^n.

Вправа 17.3. Показати, що $g^{-n} = \underbrace{g^{-1} * g^{-1} * \ldots * g^{-1}}_{n \text{ разів}}$.

Підмножину елементів G, що складається із $g^0 = e$, g, g^{-1}, g^2, g^{-2}, ... позначимо через $\langle g\rangle$. Структура $(\langle g\rangle,*,e)$ є підгрупою групи $(G,*,e)$.

Дійсно, якщо $g^l, g^m \in \langle g\rangle$, то $g^l * g^m = g^{l+m} \in \langle g\rangle$, а із $g^m \in \langle g\rangle$ випливає $g^{-m} \in \langle g\rangle$.

При цьому група $(\langle g\rangle,\circ,e)$ називається породженою твірним елементом g, а її порядок *порядком* елемента g.

Означення 17.4. *Група* $(G,*,e)$ *називається циклічною, якщо існує* $g \in G$ *такий, що* $\langle g\rangle = G$, *тобто* $G = \{g^n | n \in \mathbb{Z}\}$.

Іншими словами, *група називається циклічною, якщо вона збігається з однією із своїх циклічних підгруп.*

Вправа 17.4. Нехай $(G,*,e)$ – циклічна група, довести, що вона абелева.

Зауваження. У наведеному вище означенні циклічної групи було використано мультиплікативну термінологію. В адитивній термінології циклічна група, породжена елементом g записується так:

$$G = \langle g \rangle = \{ng | n \in \mathbb{Z}\}.$$

Приклади.

1. $(\mathbb{Z},+,0)$ – циклічна адитивна група нескінченного порядку;
2. Нехай $(G,*,e)$ – група, причому $G = e$. Тоді $(G,*,e)$ циклічна група порядку 1.
3. Множина комплексних коренів n-го степеню із 1: $e^{\frac{2\pi k}{n}}$, $k = 0,1,\dots,n-1$ з операцією множення комплексних чисел – циклічна група порядку n.

Вправа 17.5. Навести власні приклади циклічних груп та вказати їх твірні елементи.

ЛЕКЦІЯ 18. **СУМІЖНІ КЛАСИ. ТЕОРЕМА ЛАГРАНЖА**

Означення 18.1. *Якщо $(H,*,e)$ – підгупа групи $(G,*,e)$, то правими суміжними класами суміжності за підгрупою H називаються множини*

$$Hg = \{h * g | h \in H\}, \qquad g \in G.$$

Відповідно лівими суміжними класами суміжності за підгрупою H називаються множини

$$gH = \{g * h | h \in H\}, \qquad g \in G.$$

Будь-який елемент суміжного класу (правого чи лівого) називається представником цього класу.

Твердження 18.1. *Нехай a і b представники правого суміжного класу Hg, тобто $a \in Hg$ і $b \in Hg$. Тоді $a * b^{-1} \in H$.*

Доведення. Оскільки $a \in Hg$, то $\exists h_1 \in H$, такий що $a = h_1 * g$. Аналогічно $\exists h_2 \in H$, такий що $b = h_2 * g$. Звідки

$$a * b^{-1} = (h_1 * g) * (g^{-1} * h_2^{-1}) = h_1 * h_2^{-1} \in H.$$

Вправа 18.1. Довести, що коли a і b представники лівого суміжного класу gH, тобто $a \in gH$ і $b \in gH$, то $a^{-1} * b \in H$.

На групі $(G,*,e)$ введемо відношення $\sim_R$ пов'язане з підгрупою $(H,*,e)$ для правого суміжного класу Hg:

$$a \sim_R b \Leftrightarrow a * b^{-1} \in H$$

та для лівого суміжного класу gH:

$$a \sim_L b \Leftrightarrow a^{-1} * b \in H.$$

Вправа 18.2. Довести, що відношення $\sim_R$ та $\sim_L$ є відношеннями еквівалентності на G, а, отже, розбивають G на класи еквівалентності, що не перетинаються.

Твердження 18.2. *Класи еквівалентності відношення $\sim_R$ є правими класами суміжності за підгрупою H.*

Доведення. Дійсно, якщо $a \sim_R b$, то $a * b^{-1} \in H$, тобто $\exists h \in H$ таке, що $h = a * b^{-1}$ або $a = h * b$. Звідки $a \in Hb$ і, оскільки $b = e * b$, то $b \in Hb$.

Вправа 18.3. Нехай $H_1, H_2, \dots, H_n$ – класи еквівалентності відношення $\sim_L$. Показати, що якщо $a_i \in H_i$, $i = 1,2, \dots, n$, то $H_i = a_i H$, тобто класи еквівалентності відношення $\sim_L$ є лівими класами суміжності за підгрупою H. А також, що коли $H_1, H_2, \dots, H_n$ – класи еквівалентності відношення $\sim_R$, тоді, якщо $a_i \in H_i$, $i = 1,2, \dots, n$, то $H_i = Ha_i$.

Теорема 18.1. *Нехай група $(G,*)$ — скінченна, тобто $|G| < +\infty$. Тоді*

I. *Якщо $H, H_1, H_{2,\dots}, H_n$ – класи еквівалентності відношення $\sim_L$ і $a_i \in H_i$, $i = 1,2, \dots, n$,* то

$$G = H \sqcup a_1H \sqcup a_2H \sqcup \ldots \sqcup a_nH,$$

де знак $\sqcup$ *означає об'єднання множин, які не перетинаються.*

II. Якщо $H, H_1, H_{2,\ldots}, H_n$ *– класи еквівалентності відношення* $\sim_R$ *і* $a_i \in H_i$, $i = 1,2, \ldots, n$, то

$$G = H \sqcup Ha_1 \sqcup Ha_2 \sqcup \ldots \sqcup Ha_n.$$

Доведення. Покажемо, що справедлива частина I. Дійсно, із того, що

$$G = H \sqcup H_1 \sqcup H_2 \sqcup \ldots \sqcup H_n$$

та вправи 4.3 ($H_i = a_iH, i = 1, \ldots, n$) випливає доведення теореми. Частина II доводиться аналогічно.

Твердження 18.2. *Будь-який клас суміжності* (*правий чи лівий*) *за підгрупою* H *містить* $|H|$ *елементів.*

Доведення. Для будь-якого представника g правого класу суміжності Hg за підгрупою H відображення $f: H \ni h \xrightarrow{f} h * g \in Hg$ є бієктивним (взаємно однозначним відображенням H на всю множину Hg). Дійсно, для всіх $h_1, h_2 \in Hg$ таких, що $h_1 \neq h_2$ маємо, що $h_1 * g \neq h_2 * g$. Крім цього, із означення правого класу суміжності Hg випливає, що f відображає H на всю множину Hg. Отже, H та Hg мають однакову потужність, тобто $|Hg| = |H|$.

Для лівого класу суміжності gH твердження доводиться аналогічно.

Теорема 18.2 (Лагранж). *Для будь-якої скінченної групи* $(G,*)$ *її порядок* $|G|$ *ділиться на порядок* $|H|$ *підгрупи* $(H,*)$ *цієї групи.*

Доведення. Нехай $|G| = k$, а $|H| = m$. Тоді, за твердженням 4.2, будь-який суміжний клас (правий чи лівий) містить рівно m. Якщо таких класів l, то за теоремою 4.1, $k = ml$.

Якщо група комутативна, то очевидно, що її праві та ліві класи суміжності збігаються. Для некомутативних груп у загальному випадку такі об'єкти відрізняються.

Означення 18.1. *Якщо* $(H,*)$ *підгрупа групи* $(G,*)$ *така, що праві і ліві суміжні класи за підгрупою* H *збігаються, тобто* $Hg = gH$ *для всіх* $g \in G$*, то* $(H,*)$ *називається нормальним дільником групи* $(G,*)$.

Твердження 18.3. *Підгрупа* $(H,*)$ *є нормальним дільником групи* $(G,*)$ *тоді і тільки тоді, коли* $\forall g \in G$ *та* $\forall h \in H$ *маємо*

$$g^{-1}hg \in H.$$

Доведення. Достатність. Нехай $\forall g \in G \ \ та \ \ \forall h \in H \ \ g^{-1}hg \in H$. Звідси випливає, що $hg \in gH$. З іншого боку, $hg \in gH$ і оскільки це виконується для $\forall h \in H$, то для фіксованого $g \in G$, $Hg = gH$. Далі, оскільки з попереднього $Hg = gH$ для будь-якого $g \in G$, то $(H,*)$ – нормальний дільник $(G,*)$.

Необхідність. Нехай підгрупа $(H,*)$ є нормальним дільником групи $(G,*)$. Тоді $Hg = gH$ для всіх $g \in G$. Звідки $\forall g \in G$ та $\forall h \in H$ існує $h_1 \in H$ таке, що $hg = gh_1$, тобто $g^{-1}hg = h_1 \in H$. Отже, $g \in G$ та $\forall h \in H$ маємо $g^{-1}hg \in H$.

Нехай $(H,*)$ є нормальним дільником групи $(G,*)$. На класах суміжності g_1H та g_2H введемо операцію $g_1H * g_2H$, яка є множиною всіх добутків елементів із g_1H на елементи g_2H, тобто

$$g_1H * g_2H := \{x * y | x \in g_1H, y \in g_2H\}. \qquad (4.1)$$

Оскільки $(H,*)$ – нормальний дільник, то неважко переконатись, що

$$g_1H * g_2H = (g_1 * g_2)H.$$

Враховуючи це, неважко переконатись, що операція $g_1H * g_2H$ є груповою, тобто вона асоціативна, в якості нейтрального елементу виступає множина H та для будь-якого gH існує обернений $g^{-1}H$.

Означення 18.2. *Множина класів суміжності* gH *за нормальним дільником* $(H,*)$ групи $(G,*)$ з операцією (4.1) *називається фактор-групою.*

Література

1. Бондаренко Є. В. Теорія кілець. К.: ВПЦ “Київський університет”, 2012.
2. Гаврилків В. М. Елементи теорії груп та теорії кілець: навчальний посібник. Івано-Франківськ: Голіней, 2016. 148 с.
3. Вища математика: навчальний посібник для студентів вищ. навч. зак. 4-те вид. / колектив авторів: В. П. Дубовик, І. І. Юрик, І. П. Вовкодав та ін. К. : Ігнатекс-Україна, 2013. 648 с.
4. Оглобліна О. І., Сушко Т. С., Шрамко С. В. Елементи теорії чисел: навчальний посібник. Міністерство освіти і науки України. Сумський державний університет, 2015. 185 с.
5. Пилипів В. М., Заторський Р. А., Ліщинський І. І. Кільце поліномів: навчально-методичний посібник. Івано-Франківськ: Плай, 2014. 100 с.
6. Пилипів В. М., Заторський Р. А., Ліщинський І. І. Класичні основи теорії чисел: навчально-методичний посібник. Івано-Франківськ: Плай, 2014. 68 с.
7. Андрійчук В. І., Забавський Б. В. Алгебра і теорія чисел: навч. посібник. Львів: ЛНУ імені Івана Франка, 2009. 266.

Навчальне видання

Погоруй Анатолій Олександрович
Фонарюк Олена Василівна

АЛГЕБРА І ТЕОРІЯ ЧИСЕЛ

Навчально-методичний посібник