

О. В. Зеленський ,
Ю. Л. Смержевський,
А. Ю. Динич

АЛГЕБРАЇЧНІ СТРУКТУРИ І ЇХ ЗАСТОСУВАННЯ

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

ЕЛЕКТРОННЕ ВИДАННЯ



Кам'янець-Подільський
2026

УДК 512.8(075.8)

ББК 22.144я73

З-48

Рекомендувала вчена рада фізико-математичного факультету
Кам'янець-Подільського національного університету імені Івана Огієнка
(протокол № 4 від 27.04.2026 року)

РЕЦЕНЗЕНТИ:

Віталій ІВАНЮК, доктор технічних наук, доцент, завідувач кафедри комп'ютерних наук Кам'янець-Подільського національного університету імені Івана Огієнка;

Ірина КОВАЛЬСЬКА, кандидат фізико-математичних наук, доцент, доцент кафедри математики Кам'янець-Подільського національного університету імені Івана Огієнка;

Олександр ШЕВЧУК, кандидат педагогічних наук, викладач кафедри цифрових, освітніх та соціо-економічних технологій Навчально-реабілітаційного закладу вищої освіти «Кам'янець-Подільський державний інститут».

Зеленський О. В., Смержевський Ю. Л., Динич А. Ю.

З-48 Алгебраїчні структури і їх застосування: навчально-методичний посібник [Електронний ресурс]. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2026. 169 с.

Електронна версія посібника доступна за покликанням:

URL: <http://elar.kpnu.edu.ua/xmlui/handle/123456789/10292>

Метою електронного навчально-методичного посібника є формування, поглиблення та систематизація теоретичних знань і практичних умінь здобувачів освіти з основ сучасної алгебри. Посібник спрямований на ґрунтовне опрацювання таких ключових розділів, як групи, кільця та ідеали, кільце многочленів від однієї і кількох змінних, симетричні многочлени, а також алгебраїчні розширення числових полів. Видання сприяє засвоєнню основних алгебраїчних понять, означень, теорем і методів доведення, розвитку логічного мислення, математичної культури та навичок самостійної роботи. Посібник рекомендовано для студентів фізико-математичних спеціальностей, магістрантів, викладачів, а також для всіх, хто прагне поглибити свої знання з алгебри.

УДК 512.8(075.8)

ББК 22.144я73

© Зеленський О. В.,
Смержевський Ю. Л., Динич А. Ю., 2026

ЗМІСТ

<i>Розділ I. ГРУПИ</i>	5
§1.1. Алгебраїчні структури з однією операцією.....	5
§1.2. Півгрупа	6
§1.3. Означення групи. Найпростіші властивості	8
§1.4. Деякі інші означення групи	13
§1.5. Означення та приклади підгрупи.....	15
§1.6. Циклічні підгрупи.....	17
§1.7. Циклічні групи	20
§1.8. Відношення еквівалентності. Суміжні класи	22
§1.9. Суміжні класи.....	24
 <i>Розділ II. КІЛЬЦЯ ТА ІДЕАЛИ</i>	33
§2.1. Означення кільця.....	33
§2.2. Найпростіші висновки з аксіоматики.....	35
§2.3. Підкільце	38
§2.4. Гомоморфізми та ізоморфізми кілець.....	41
§2.5. Означення ідеалу кільця, приклади ідеалів.....	52
§2.6. Кільця головних ідеалів та евклідові кільця.....	55
§2.7. Подільність в областях цілісності з одиницею.....	57
§2.8. Конгруенції та фактор кільця за ідеалом.....	64
§2.9. Фактор-кільця комутативного кільця за ідеалом I	65
§2.10. Фактор-кільця і гомоморфізми	67
§2.11. Конгруенції та класи лишків за модулем m	69
§2.12. Кільце класів лишків за модулем m	72
§2.13. Застосування конгруенцій до встановлення ознак подільності	75
 <i>Розділ III. КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД ОДНОГО НЕВІДОМОГО</i>	83
§3.1. Подільність многочленів.....	83
§3.2. Ізоморфне вкладення кільця K в алгебру $K[x]$	87
§3.3. Проблема існування та єдиності кільця $K[x]$	88
§3.4. Кільце $K[x]$ як просте трансцендентне розширення кільця K	92
§3.5. Многочлени над полем.....	95
§3.6. Кільце многочленів як евклідове кільце	96
§3.7. Схема Горнера. Розклад многочлена $f(x)$ за степенями $x - \alpha$	99

§3.8. Подільність многочленів. Ідеали кільця $P[x]$	101
§3.9. Найбільший спільний дільник. Алгоритм Евкліда	103
§3.10. Найменше спільне кратне многочленів	105
§3.11. Незвідні многочлени.....	106
§3.12. Корені многочлена.....	110
§3.13. Похідна від многочлена. Відокремлення кратних множників.....	115
 <i>Розділ IV. КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД КІЛЬКОХ ЗМІННИХ</i>	120
§4.1. Побудова кільця многочленів.....	120
§4.2. Різні форми зображення многочленів	122
§4.3. Лексикографічне впорядкування членів многочлена	122
§4.4. Симетричні многочлени. Означення і елементарні властивості	124
§4.5. Основна теорема теорії симетричних многочленів.....	125
§4.6. Основна теорема теорії многочленів.....	128
§4.7. Наслідки з основної теореми теорії многочленів	131
§4.8. Раціональні корені многочленів з раціональними коефіцієнтами	137
 <i>Розділ V. АЛГЕБРАЇЧНІ РОЗШИРЕННЯ ЧИСЛОВИХ ПОЛІВ</i>	139
§5.1. Алгебраїчні числа і скінченні розширення полів.....	139
§5.2. Просте алгебраїчне розширення поля.....	140
§5.3. Алгебраїчні розширення поля.....	142
§5.4. Поняття розв'язності рівняння в квадратних радикалах	146
§5.5. Умови розв'язності рівняння третього степеня в квадратних радикалах....	147
§5.6. Приклади задач, нерозв'язних в квадратних радикалах	148
 <i>Розділ VI. ЕЛЕМЕНТИ СУЧАСНОЇ АЛГЕБРИ</i>	150
§6.1. Обчислювальна алгебра і місце простих чисел.....	151
§6.2. Мала теорема Ферма і ймовірнісна перевірка простоти.....	152
§6.3. Свідки Ферма, лжеці Ферма і числа Кармайкла	154
§6.4. Тест Міллера–Рабіна	156
§6.5. Використання простих чисел у криптографії. Система RSA	157
§6.6. Групи в сучасній криптографії та цифровому підписі	159
§6.7. Алгебраїчні ідеї в блокчейні.....	161
§6.8. Додаткові приклади застосування алгебри.....	163
 ВИСНОВКИ.....	165
 СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	167

Розділ I

ГРУПИ

Як зазначалось в курсі алгебри першого семестру, основним об'єктом вивчення в алгебрі є алгебраїчні структури. Під алгебраїчною структурою розуміють множину M , на якій задана деяка система алгебраїчних операцій, які задовольняють деякі умови-аксіоми структури. Як відомо, алгебраїчні операції діляться на два типи: внутрішні закони композиції і зовнішні закони композиції. В даному розділі під алгебраїчною операцією, означеною на множині M , розумітимемо скрізь бінарний внутрішній закон композиції на M , тобто відображення прямого добутку $M \times M$ в M .

Раніше ми ознайомилися з однією важливою алгебраїчною структурою – полем. Структура поля означається шляхом задання на множині двох алгебраїчних операцій – додавання і множення, які задовольняють відомим дев'яти аксіомам. Але найпростіші серед алгебраїчних структур є структури, які означаються однією алгебраїчною операцією. До вивчення таких структур ми зараз і приступимо.

§1.1. АЛГЕБРАЇЧНІ СТРУКТУРИ З ОДНІЄЮ ОПЕРАЦІЄЮ

Означення 1. Непорожня множина M , на якій означена одна алгебраїчна операція, називається *групоїдом*.

Алгебраїчну операцію що визначає групоїд, будемо найчастіше називати множенням і вживати мультиплікативний запис $a \times b$. Підкреслимо, що операція, яка визначає групоїд M , повинна бути скрізь означеною на множині M , тобто

$$(\forall a, b \in M)(\exists c \in M): ab = c.$$

Щоб відзначити, що групоїд визначається двома компонентами – множиною M і алгебраїчною операцією, означеною на ній, – часом для

групоїда вживають таке позначення: $\langle M, \cdot \rangle$. Як видно з означення, на операцію, яка визначає групоїд, не накладається жодних умов.

Приклади.

1. Множина всіх підстановок n -го степеня з операцією множення підстановок утворює групоїд.
2. Якщо в множині R всіх дійсних чисел розглядати тільки операцію додавання чисел, то сукупність $\langle R, + \rangle$ є групоїдом.

Операція множення підстановок є асоціативною, але не є комутативною, відносно неї існує одиничний елемент і для кожної підстановки – обернена. Операція додавання дійсних чисел є асоціативною і комутативною, відносно неї існує нульовий елемент і для кожного числа – протилежне.

Як бачимо, в деяких групоїдах алгебраїчна операція насправді задовольняє тим чи іншим умовам. Це дає можливість прокласифікувати групоїд в залежності від того, яким умовам задовольняє алгебраїчна операція групоїда. Ми зупинимось тільки на двох класах групоїдів – півгрупах і групах. Півгрупа – це групоїд, алгебраїчна операція якого є асоціативною. Група – це півгрупа, в якій існує одиничний елемент і для кожного елемента – обернений. Зараз дамо детальніші означення цих об'єктів і вивчимо їх деякі властивості.

§1.2. ПІВГРУПА

Означення 2. Непорожня множина M , на якій означена одна алгебраїчна операція, яка є асоціативною, називається *півгрупою*.

Приклади.

1. Множина всіх підстановок n -го степеня з операцією множення підстановок утворює півгрупу.
2. Множина всіх матриць n -го порядку утворює півгрупу відносно операції множення матриць, бо множення матриць є асоціативним. В цій півгрупі існує одиничний елемент – одинична матриця E , але не для кожної матриці існує обернена.

3. Сукупність $\langle N, \cdot \rangle$ і $\langle N, + \rangle$, де N – множина натуральних чисел, утворюють підгрупи, причому в першому випадку нейтральний елемент (1) належить підгрупі, а в другому випадку підгрупа не містить нейтрального елемента (0).

4. Множина P всіх цілих парних чисел утворює підгрупу відносно операції множення (добуток парних чисел – парне число, множення чисел асоціативне), причому ця підгрупа нейтрального елемента (1) не містить.

Наявність асоціативного закону для операції підгрупи M дозволяє однозначно ввести в M поняття добутку 3, 4, ..., n елементів. Оскільки $(a_1 a_2) a_3 = a_1 (a_2 a_3)$, то добуток трьох елементів можна записувати без дужок: $a_1 a_2 a_3$.

Добуток 4, 5, ..., n елементів означимо рекурентно:

$$a_1 a_2 a_3 a_4 = (a_1 a_2 a_3) a_4,$$

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n.$$

Наявність асоціативного закону для операції підгрупи дозволяє в добутках, що містять більше двох співмножників (такі добутки будемо умовно називати складеними), довільно розставляти дужки. Цей факт впливає з такої теореми:

Теорема 1.1. Добуток двох складених добутків дорівнює складеному добутку всіх співмножників, що входять до їх складу, взятих у тому ж порядку [1; 2], тобто

$$(a_1 \dots a_m)(a_{m+1} \dots a_{m+n}) = a_1 \dots a_m a_{m+1} \dots a_{m+n}. \quad (1)$$

Доведення. Доведення проведемо методом математичної індукції за n .

1. Якщо $n = 1$, то формула (1) набуває вигляду $(a_1 \dots a_m) a_{m+1} = a_1 \dots a_m a_{m+1}$, що безпосередньо впливає з означення добутку $m + 1$ елементів.

2. Припустимо, що формула (1) справедлива для деякого n . Доведемо її для $n + 1$:

$$(a_1 \cdots a_m)(a_{m+1} \cdots a_{m+n} a_{m+n+1}).$$

Використовуючи означення добутку $m + n + 1$ елементів і асоціативність алгебраїчної операції, послідовно матимемо:

$$\begin{aligned} (a_1 \cdots a_m)(a_{m+1} \cdots a_{m+n} a_{m+n+1}) &= ((a_1 \cdots a_m)(a_{m+1} \cdots a_{m+n})) a_{m+n+1} = \\ &= (a_1 \cdots a_m a_{m+1} \cdots a_{m+n}) a_{m+n+1} = a_1 \cdots a_m a_{m+1} \cdots a_{m+n} a_{m+n+1}. \end{aligned}$$

Отже, якщо формула (1) справедлива для n , то вона справедлива і для $n + 1$. За принципом математичної індукції формула (1) справедлива для будь-якого натурального n .

Наслідок. У складеному добутку можна вільно розставляти дужки.

Справді, якщо у формулі (1) послідовно брати $m = 1, 2, \dots, n - 1$, то дістанемо:

$$a_1 a_2 \cdots a_n = (a_1 a_2) a_3 \cdots a_n = ((a_1 a_2) a_3) \cdots a_n = \cdots = (a_1 a_2 \cdots a_{n-1}) a_n.$$

У кожній із одержаних дужок на підставі теореми 1.1 знову можна довільно розставляти дужки, наприклад: $(a_1 a_2)(a_3 a_4 \dots a_k)(a_{k+1} \dots a_n)$.

§1.3. ОЗНАЧЕННЯ ГРУПИ. НАЙПРОСТІШІ ВЛАСТИВОСТІ

Означення 3. Непорожня множина G називається групою, якщо на ній означена одна алгебраїчна операція, яка задовольняє таким умовам:

- 1) алгебраїчна операція асоціативна, тобто $(\forall a, b, c \in G) a(bc) = (ab)c$;
- 2) в G існує одиничний елемент e такий, що $(\forall a \in G) ae = ea = a$;
- 3) для кожного елемента $a \in G$ існує обернений елемент $a^{-1} \in G$ такий, що $aa^{-1} = a^{-1}a = e$.

Якщо алгебраїчна операція, означена в групі, є додатково комутативною, то група називається комутативною або абелевою.

Приклади.

1. Система $\langle R_+, \cdot \rangle$, де R_+ – множина додатних дійсних чисел утворює групу, бо $\forall a, b \in R_+, a \cdot b \in R_+$ і операція множення задовольняє аксіомам групи:

- 1) множення дійсних чисел асоціативне;
- 2) в R_+ існує одиничний елемент – число 1;
- 3) для кожного числа $a \in R_+$ обернене число існує і належить R_+ .

2. Множина R_0 всіх дійсних чисел без нуля теж утворює групу відносно операції множення дійсних чисел. В цьому переконуємось так само як і в прикладі 1.

3. Множина R всіх дійсних чисел утворює групу відносно операції додавання дійсних чисел. Справді, операція «+» в R задовольняє аксіомам групи:

- 1) операція «+» асоціативна.
- 2) в R існує нейтральний елемент – число 0;
- 3) для всякого числа a існує симетричний елемент – протилежне число $-a$.

4. З аналогічних міркувань система $\langle Z, + \rangle$, де Z – множина усіх цілих чисел є групою.

5. Множина M_n всіх невідроджених матриць n -го порядку над полем P утворює групу відносно операції множення матриць. Дійсно $\forall A, B \in M_n : AB \in M_n$, бо за теоремою про визначник добутку матриць $|AB| = |A| \cdot |B| \neq 0$. Крім того,

- 1) множення матриць асоціативне;
- 2) в M_n існує одиничний елемент – одинична матриця E ;
- 3) всяка неособлива матриця має обернену, яка, крім того ж належить M_n , бо на підставі теореми про визначник добутку матриць із рівності $AA^{-1} = E$ випливає $|A||A^{-1}| = 1$ і значить, $|A^{-1}| \neq 0$.

6. Множина $K_n = \{ \varepsilon_k \mid \varepsilon_k^n = 1 \}$ всіх значень кореня n -ого степеня з 1 утворює групу відносно операції множення комплексних чисел. Справді, якщо $\varepsilon_k, \varepsilon_j \in K_n$, то $\varepsilon_k \cdot \varepsilon_j \in K_n$, бо $(\varepsilon_k \cdot \varepsilon_j)^n = \varepsilon_k^n \cdot \varepsilon_j^n = 1$. Операція множення задовольняє аксіомам групи:

- 1) множення комплексних чисел асоціативне;
- 2) одиниця належить $K_n : \varepsilon_0 = 1$;
- 3) $(\forall k)(\varepsilon_k \neq 0) \text{ і } \varepsilon_k^{-1} \in K_n$, бо $(\varepsilon_k^{-1})^n = (\varepsilon_k^n)^{-1} = 1$.

7. Множина S_n всіх підстановок n -ого степеня очевидним чином утворює групу відносно операції множення підстановок.

Зауважимо, що групи в прикладах 1-4 і в 6 є абелевими, а групи в прикладах 5 і 7 – неабелеві. Зауважимо також, що алгебраїчні операції в конкретних групах є або операціями множення, або операціями додавання. Групи, в яких алгебраїчні операції є множення називаються мультиплікативними, а групи, в яких алгебраїчні операції є додавання, називаються адитивними. З наведених прикладів видно, також, що одні групи мають безліч елементів – нескінченні групи (групи прикладів 1-5), інші мають скінченну кількість елементів – скінченні групи (групи прикладів 6 і 7). Кількість елементів у скінченній групі G називається порядком цієї групи і позначається $Or(K_n) = n$, а в прикладі 7 $Or(S_n) = n!$. В скінченних множинах групову операцію зручно задавати за допомогою таблиць множення, так званих таблиць Келі. В множині P_2 , що складається з двох поворотів площини навколо нерухомої точки O – точки повороту l на кут 0° і повороту π на кут 180° – операцією множення задамо такою таблицею Келі:

	l	π
l	l	π
π	π	l

Легко перевірити, що множина P_2 із заданою операцією є групою.

Вправи.

I. Дослідити, чи утворює групу:

- 1) множина N всіх натуральних чисел відносно додавання і відносно множення чисел;
- 2) множина Q всіх раціональних чисел відносно додавання і відносно множення чисел;
- 3) множина $\{-1; 1\}$ відносно операції множення чисел;
- 4) множина всіх парних підстановок n -ого степеня відносно операції множення підстановок;

5) множина всіх непарних підстановок n -ого степеня відносно операції множення підстановок.

II. Скласти таблицю Келі для симетричної групи S_3 .

Відзначимо декілька найпростіших властивостей груп, які безпосередньо випливають з означення аксіоматики групи.

1°. В усякій групі $\langle G, \cdot \rangle$ одиничний елемент e є єдиним і для всякого елемента $a \in G$ обернений елемент a^{-1} теж єдиний.

Ця властивість є безпосереднім наслідком теорем, доведених у курсі алгебри першого семестру, про єдиність нейтрального елемента і симетричного елемента в множині з асоціативною алгебраїчною операцією.

2°. Для всяких елементів $a, b \in G$ рівняння $ax = b$ та $ya = b$ мають єдині розв'язки відповідно $x = a^{-1}b$ та $y = ba^{-1}$.

Доведення цієї властивості проводиться точно так само, як і доведення відповідної властивості полів.

3°. $\forall a, b \in G: (ab)^{-1} = b^{-1}a^{-1}$, тобто елемент обернений до добутку, дорівнює добутку обернених елементів, взятих у зворотному порядку.

Доведення. Щоб показати, що елемент $b^{-1}a^{-1}$ є оберненим до ab треба показати на підставі означення оберненого елемента, що і $(ab)(b^{-1}a^{-1}) = e$ і $(b^{-1}a^{-1})(ab) = e$. Покажемо справедливості першої рівності (друга – аналогічно): $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$.

Подібно до того, як вводиться степінь з цілим показником для дійсного числа, поняття степеня з цілим показником можна ввести для будь-якого елемента групи.

Означення 4. Нехай G – група і n – ціле число. Тоді

$$\forall a \in G, a^n = \begin{cases} \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ раз}}, \text{ якщо } n > 0 \\ e, \text{ якщо } n = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{|n| \text{ раз}}, \text{ якщо } n < 0 \end{cases}.$$

Правила дій над степенями елементів групи ті ж, що і над степенями дійсних чисел:

4°. Якщо G – група, то для всіх $a \in G$ і $m, n \in \mathbb{Z}$ виконується рівність $a^m a^n = a^{m+n}$.

Доведення. Розглянемо можливі знаки чисел m і n .

1. Якщо $m \geq 0$ і $n \geq 0$, то на підставі означення степеня та теореми 1.1 маємо

$$a^m a^n = (a \cdot a \cdots a)(a \cdot a \cdots a) = a^{m+n}.$$

2. Якщо один із показників від'ємний, то використовуємо означення $a^{-k} = (a^{-1})^k$ і скорочення $aa^{-1} = a^{-1}a = e$. Після скорочення однакових взаємно обернених множників знову одержуємо $a^m a^n = a^{m+n}$.

3. Випадок $m \leq 0$, $n \geq 0$ розглядається аналогічно попередньому.

4. Якщо $m \leq 0$ і $n \leq 0$, то твердження випливає з означення від'ємного степеня та вже доведеного випадку для невід'ємних показників.

5. $m \leq 0$, $n \leq 0$. Розглядається аналогічно випадку 1).

Наслідок. У групі G для всіх $a \in G$ і $n \in \mathbb{Z}$ виконується $(a^n)^{-1} = a^{-n}$, тобто елементом, оберненим до a^n , є a^{-n} .

Справді, $a^n a^{-n} = a^{n-n} = a^0 = e$, $a^{-n} a^n = a^{-n+n} = a^0 = e$.

Методом математичної індукції властивість 4° можна поширити на довільну скінченну кількість співмножників.

5°. У групі G для всіх $a \in G$ і $m, n \in \mathbb{Z}$ виконується рівність $(a^m)^n = a^{mn}$.

Доведення. Якщо $n \geq 0$, то $(a^m)^n$ є добутком n однакових множників a^m , тому за властивістю 4° маємо $(a^m)^n = a^{mn}$.

Якщо $n < 0$, то за означенням від'ємного степеня та наслідком із властивості 4° одержуємо той самий результат:

$$(a^m)^n = \left((a^m)^{-1} \right)^{-n} = (a^{-m})^{-n} = a^{mn}.$$

Вправа. Перефразувати властивості 3-5 для адитивних груп.

Зауважимо, що при переході до адитивних груп поняття n -ого степеня елемента a замінюється поняттям n -кратного елемента na елемента a :

$$na = \begin{cases} a + a + \dots + a, & n > 0 \\ 0, & n = 0 \\ |n| \cdot (-a) = (-a) + (-a) + \dots + (-a), & n < 0 \end{cases}$$

§1.4. ДЕЯКІ ІНШІ ОЗНАЧЕННЯ ГРУПИ

В літературі даються часто означення групи відмінні від означення 3 [1]. Зараз ми ознайомимося з цими означеннями та доведемо їх еквівалентність означенню 3, тобто, покажемо, що всяка множина, яка задовольняє умови означення 3, задовольняє і умови означення 3' та 3'' і навпаки.

Означення 3'. Непорожня множина G називається групою, якщо на ній означена одна алгебраїчна операція, яка задовольняє таким умовам:

- 1) алгебраїчна операція асоціативна;
- 2) в G існує ліва одиниця e_l , така, що

$$\forall a \in G: e_l a = a \quad (1)$$

3) для довільного елемента $a \in G$ відносно лівої одиниці e_l існує лівий обернений елемент $a' \in G$, такий, що

$$a' a = e_l. \quad (2)$$

Означення 3''. Непорожня множина G називається групою, якщо на ній означена одна алгебраїчна операція, яка задовольняє таким умовам:

- 1) алгебраїчна операція асоціативна;
- 2) для будь-яких $a, b \in G$ рівняння $ax = b$ та $ya = b$ мають розв'язки.

Теорема 1.2. Означення 3 і 3' еквівалентні [1; 4].

Доведення. Якщо множина є групою за означенням 3, тобто задовольняє умови означення 3, то вона задовольняє умови означення 3', тобто є групою за означенням 3'. Одиничний елемент відіграє при цьому роль лівої одиниці, а обернений відіграє роль лівого оберненого.

Нехай, навпаки, задовольняє умовам означення 3'. Щоб довести, що вона задовольняє умовам означення 3, досить, очевидно, показати, що ліва одиниця є одночасно і правою, тобто для

$$\forall a \in G: a e_l = a \quad (3)$$

і лівий обернений a' є одночасно і правим оберненим, тобто

$$\forall a \in G: a a' = e_l \quad (4)$$

Покажемо спочатку справедливість співвідношення (4). Для цього домножимо рівність (2) справа на елемент a' . Внаслідок однозначності

операції множення (добуток двох елементів єдиний) рівність при цьому не порушується:

$$a'(aa') = a'.$$

В силу умови 3) означення 3' елемент a' має лівий обернений a'' . Домноживши останню рівність зліва на елемент a'' і скориставшись асоціативністю, одержимо:

$$(a''a')(aa') = a''a'.$$

Оскільки a'' – лівий обернений елемент до a' , тобто $a''a' = e_l$, то остання рівність перепишеться так:

$$e_l(aa') = e_l \text{ або, інакше, } aa' = e_l,$$

чим справедливості співвідношення (4) доведено.

Переконаємось зараз в справедливості співвідношення (3). Для цього перетворимо ліву частину, використавши послідовно формулу (2), асоціативність множення, формули (4) і (1): $ae_l = a(a'a) = (aa')a = e_la = a$.

Отже, множина G є групою і за означенням 3.

Теорема 1.3. Означення 3 і 3'' еквівалентні [1; 4].

Доведення. Якщо множина G задовольняє умови означення 3, то, як це безпосередньо впливає з означення 3 і властивості 2', вона задовольняє і умови означення 3''.

Навпаки, нехай множина G задовольняє умови означення 3''. Ми покажемо, що множина при цьому задовольняє умови означення 3', звідки на підставі теореми 1.2 буде виходити, що множина G задовольняє і умови означення 3. Отже, треба показати, що в G існує ліва одиниця, по відношенні до якої кожен елемент має лівий обернений елемент.

Щоб довести існування в G лівої одиниці, тобто такого елемента e_l , який задовольняє співвідношення (1), зауважимо, що за умовою рівняння $u \cdot a = a$ має розв'язок який позначимо через e_a : $e_a a = a$. покажемо, що e_a є лівою одиницею, тобто, що для $(\forall b \in G): e_a \cdot b = b$. З цією метою приймемо до уваги, що рівняння $ax = b$ має розв'язок $x_0 : ax_0 = b$, внаслідок чого

$$e_a b = e_a (ax_0) = (e_a a) x_0 = ax_0 = b.$$

Отже, для $(\forall b \in G): e_a \cdot b = b$, тобто e_a – ліва одиниця в G . Внаслідок того, що за умовою для всякого $b \in G$ рівняння $ub = e_a$, має розв'язок по відношенні до лівої одиниці e_a кожен елемент $b \in G$ має лівий обернений.

Таким чином, множина G є групою згідно з означення $3'$, а в силу теореми 1.2 і згідно з означенням 3.

Вправи.

1. Чи еквівалентні означення $3'$ і $3''$?
2. Якщо множина G є групою відносно до означення $3''$, то чи є розв'язки рівнянь $ax = b$ і $ya = b$ єдиними?

§1.5. ОЗНАЧЕННЯ ТА ПРИКЛАДИ ПІДГРУПИ

Досі ми говорили про групи взагалі і не цікавилися їх будовою та частинами з яких вони складаються. Однак, вивчення структури групи, зокрема, їх підмножин представляє значний інтерес. Серед усіх підмножин групи G особливо виділяються ті множини, які самі є групами відносно операції, заданої в G , такі підмножини називаються підгрупами, їх вивчення ми і ознайомимось зараз.

Означення 5. Підмножина H групи G , яка сама є групою відносно операції, заданої в G , називається підгрупою групи G .

Оскільки групова операція, будучи асоціативною на всій групі G , є асоціативною і на всякій підмножині групи G , та одиничний елемент групи G єдиний, то підмножина H групи G є підгрупою тоді і тільки тоді, коли справджуються такі умови:

- 1) $(\forall a, b \in H): ab \in H$;
- 2) одиничний елемент e групи G належить підмножині H ;
- 3) $(\forall a \in H): a^{-1} \in H$.

Зауважимо, що умова 2) є наслідком умов 1) і 3). Справді, якщо непорожня підмножина H групи G задовольняє умови 1) і 3), то разом із довільним своїм елементом a підмножина H містить a^{-1} (умова 3) і елемент $a^{-1}a = e$ (умова 1).

Отже, одиничний елемент $e \in H$. Таким чином, справедливий такий критерій.

Теорема 1.4. Підмножина H групи G є підгрупою групи G тоді і тільки тоді, коли виконуються умови а) і б) [1; 2; 4].

а) $(\forall a, b \in H): ab \in H$;

б) $(\forall a \in H): a^{-1} \in H$.

Приклади.

1. Група $\langle Z, + \rangle$ є підгрупою групи $\langle Q, + \rangle$, остання є підгрупою групи $\langle R, + \rangle$, а ця в свою чергу є підгрупою групи $\langle C, + \rangle$. В цьому легко переко-
натись перевіряючи умови а) та б) теореми 1.4.

Множина C_1 всіх комплексних чисел, модуль яких дорівнює 1, є підгру-
пою групи $\langle C_0, \times \rangle$, де C_0 – множина комплексних чисел відмінних від нуля.

Справді, оскільки модуль добутку двох комплексних чисел дорівнює
добутку модулів, добуток двох чисел із C_1 належить C_1 . Крім того, якщо
 $z \in C_1$, то $z \neq 0$ і, значить існує z^{-1} , причому $|z^{-1}| = \left| \frac{1}{z} \right| = \frac{1}{|z|}$, тобто $z^{-1} \in C_1$.

Множина P_n всіх парних підстановок є підгрупою симетричної групи
 $\langle S_n, \cdot \rangle$.

Справді для $(\forall \varphi, \psi \in P_n): (\varphi\psi \in P_n)$, бо φ і ψ розкладаються в парне
число транспозицій. Крім того, як відомо, підстановка, обернена до пар-
ної, є парною.

Отже, $\langle P_n, \cdot \rangle$ є підгрупою симетричної групи $\langle S_n, \cdot \rangle$. Підгрупа $\langle P_n, \cdot \rangle$ на-
зивається знакозмінною групою n -го степеня. З деякими іншими група-
ми підстановок ми ознайомились на практичних заняттях.

§1.6. ЦИКЛІЧНІ ПІДГРУПИ

Вище були наведені приклади підгруп в конкретних групах. В цьому пункті будуть вказані підгрупи довільної групи, детально зупинимося на так званих циклічних підгрупах.

1. Тривіальні підгрупи. Якщо в групі G взяти підмножину $\varepsilon = \{e\}$, що складається з одного одиничного елемента e , то вона є підгрупою G , бо $e \times e = e$ і $e^{-1} = e$. Ця підгрупа називається одиничною підгрупою групи G .

Очевидно також, що вся група G є підгрупою самої себе. Підгрупи ε та G називаються тривіальними підгрупами групи G . Якщо група G відмінна від одиничної групи ε , то в ній підгрупи, відмінні від ε і G , які називаються нетривіальними.

2. Перетин підгруп. Якщо H_1 і H_2 – підгрупи групи G , то їх перетин $H = H_1 \cap H_2$ теж є підгрупою групи G .

Дійсно, якщо $a, b \in H = H_1 \cap H_2$, то $a, b \in H_1$ і $a, b \in H_2$. Оскільки H_1 і H_2 – підгрупи, то внаслідок умови а) теореми 1.4 $a, b \in H_1$ і $a, b \in H_2$, звідки $a, b \in H_1 \cap H_2 = H$. Аналогічно якщо $a \in H = H_1 \cap H_2$, то $a \in H_1$ і $a \in H_2$ і на підставі того, що H_1 і H_2 – підгрупи $a^{-1} \in H_1$, і $a^{-1} \in H_2$ (умова б) теореми 1.4), тобто $a^{-1} \in H_1 \cap H_2 = H$. Таким чином, підмножина $H \in G$ задовольняє умовам теореми 1.4, і, значить є підгрупою.

3. Циклічна підгрупа. Нехай a – довільний елемент групи G і $(a) = \{a^n \cdot n \in \mathbb{Z}\}$ – сукупність всіх степенів елемента a з цілими показниками. Множина (a) є підгрупою групи G . Справді, для $(\forall a^n, a^m \in (a)): a^n a^m = a^{n+m} \in (a)$ і для $(\forall a^n \in (a)): (a^n)^{-1} \in (a)$. Елементи a^{n+m} і a^{-n} є степенями елемента a і тому належить (a) . Таким чином, множина (a) задовольняє умовам теореми 1.4 і тому є підгрупою групи G . Ця підгрупа називається циклічною підгрупою, породженою елементом (a) .

Означення 6. Сукупність всіх степенів з цілими показниками елемента $a \in G$, де G – довільна група називається циклічною підгрупою групи G , породженою елементом a і позначається (a) .

Нехай G – група і a – довільний її елемент.

Тоді можуть мати місце такі випадки:

1. Будь-які два степені елемента a при різних показниках не рівні, тобто

$$(\forall n, m \in \mathbb{Z}, m \neq n): a^n \neq a^m.$$

Елемент a при цьому називається елементом нескінченного порядку. Наприклад, число 2, в групі $\langle R_0, \times \rangle$ є елементом нескінченного порядку: $2^n \neq 2^m$.

Зрозуміло, що циклічна група (2) , породжена елементом 2, є в даному випадку нескінченною.

2. Існують такі $n, m \in \mathbb{Z}, m \neq n$, що $a^n = a^m$. Якщо для означеності прийняти $m < n$, то матимемо $a^{n-m} = e$, причому $n - m$ натуральне число. Отже, в даному випадку існують такі натуральні числа s , що $a^s = e$. Найменше з чисел s , таких що $a^s = e$, називається порядком елемента a . Точніше, якщо $(s \in \mathbb{N}): a^s = e$, що елемент a називається елементом скінченного порядку, а саме порядку n , якщо найменше з чисел s , таких що $a^s = e$.

Для прикладу візьмемо число i (уявна одиниця) в групі $\langle C_0, \cdot \rangle$ і розглянемо його степені. Матимемо: $i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1, i^5 = i, i^6 = -1, i^7 = -i, i^8 = 1, \dots$

Як бачимо, існують натуральні числа s , а саме $s = 4, 8, \dots$, при яких $i^s = 1$. Найменшим з них є 4. Отже, i – число порядку 4.

Циклічна підгрупа (i) , породжена елементом i , є скінченною – має 4 різні числа $1, i, -1, -i$. Отже, її порядок (кількість елементів) співпадає з порядком породжуючого числа i .

Тільки що наведені два приклади дозволяють сподіватися, що справедливим є таке твердження:

Теорема 1.5. Порядок циклічної підгрупи (a) групи G співпадає з порядком породжуючого її елемента a .

Доведення. Якщо елемент a є елементом нескінченного порядку, тобто при різних показниках степені елемента a різні, то підгрупа (a) містить безліч різних елементів, тобто її порядок теж нескінченний.

Нехай тепер елемент a має скінченний порядок n . Треба довести, що кількість елементів в групі (a) дорівнює n . З цієї метою з підгрупи

$$(a) = \{ \dots a^{-n} \dots a^{-2}, a^{-1}, a^0, a^1, a^2, \dots, a^{n-1}, a^n \dots \}.$$

Виберемо елементи $a^0, a^1, a^2, \dots, a^{n-1}$ (1) і покажемо, що 1) всі елементи системи (1) різні, 2) будь-який інший елемент a^m , ($m \neq 0, 1, 2, \dots, n-1$) підгрупи (a) співпадає з деякими елементами системи (1).

Щоб довести, що будь-які два елементи системи (1) різні, припустимо, що деякі з цих елементів співпадають, тобто, припустимо, що

$$a^m = a^k, \quad (0 \leq k < m \leq n-1).$$

Домноживши останню рівність справа на a^{-k} , матимемо $a^{m-k} = e$.

Оскільки $0 < m - k < n$, то остання рівність означає, що знайшлося натуральне число $s = m - k < n$, при якому $a^s = e$. Останнє не можливе, бо a – елемент n -го порядку. Отже, всі елементи системи (1) різні.

Нехай тепер a^m , ($m \neq 0, 1, 2, \dots, n-1$) – довільний елемент, що не ввійшов в систему (1). За теоремою про ділення з остачею ми матимемо, що

$$\exists q, r \in \mathbb{Z} : (m = nq + r) \wedge (0 \leq r < n).$$

$$\text{Тоді } a^m = a^{nq+r} = a^{nq} * a^r = (a^n)^q * a^r = e * a^r = a^r.$$

Отже, $a^m = a^r$, $0 \leq r < n$, тобто елемент a^m співпадає з котримось з елементів системи (1).

Таким чином ми показали, що в підгрупі (a) є n різних елементів $a^0, a^1, a^2, \dots, a^{n-1}$ і це означає, що $Or(a) = n = Ora$.

§1.7. ЦИКЛІЧНІ ГРУПИ

Є випадки, коли вся група G співпадає із деякою із своїх циклічних підгруп, тобто із сукупністю всіх степенів з цілими показниками деякого із своїх елементів a . Така група називається циклічною, елемент a – її твірним елементом.

Приклади. 1. Мультиплікативна група K_n всіх коренів n -го степеня з 1 є циклічною. Справді, група K_n складається з чисел $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ ($k = 0, 1, 2, \dots, n-1$). Очевидно, що на підставі формули Муавра $\varepsilon_k = \varepsilon_1^k$ ($k = 0, 1, 2, \dots, n-1$).

2. Адитивна група $Z, +$ є циклічною.

Пригадаємо, що у випадку адитивної групи замість n -го степеня елемента a , a^n , розглядають елемент, n -кратний a , $na = \underbrace{a + a + \dots + a}_n$. Тоді

$$(\forall n \in Z): n = \begin{cases} \underbrace{1 + 1 + \dots + 1}_n, & n > 0 \\ 0 * 1, & n = 0 \\ \underbrace{(-1) + (-1) + \dots + (-1)}_{|n|} = -(|n| * 1) = n * 1, & n < 0 \end{cases}$$

Це означає, що $Z, +$ – циклічна і твірним елементом її є 1, тобто $Z = (1)$.

Характерною властивістю циклічних груп є те, що можна легко описати всі їх підгрупи.

Теорема 1.6. Кожна підгрупа циклічної групи є циклічною.

Доведення. Нехай $G = (a)$ – циклічна група з твірним елементом a і H – довільна її підгрупа. Треба довести, що H – циклічна підгрупа.

Внаслідок того, що кожен елемент групи G є степенем елемента a , то елементи підгрупи H є теж степенями елемента a . Зауважимо, що коли H – тривіальна група, то вона, очевидно, циклічна, а якщо H – нетривіальна група, то серед її елементів обов'язково є степінь з натуральним показником. Дійсно, H містить елемент $a^k \neq e$. Якщо $k > 0$, то H містить степінь елемента a з натуральним показником. Якщо $k < 0$, то

$a^{-k} = (a^k)^{-1} \in H$ і знову H містить степінь a з натуральним показником $-k$.

Таким чином, множина всіх степенів елемента a з натуральними показниками, які належать підгрупі H , непорожня. Оскільки всяка підмножина множини натуральних чисел має найменше число, то і серед натуральних показників степенів елемента a , які належать підгрупі H , є найменший показник k_0 .

Покажемо, що елемент a^{k_0} є породжуючим елементом підгрупи H . Для цього візьмемо довільний елемент a^k підгрупи H і на підставі теореми про ділення з остачею запишемо співвідношення $k = k_0q + r$, де $q, r \in \mathbb{Z}$ і $0 \leq r < k_0$, звідки, зокрема, $r = k - k_0q$. Тоді $a^r = a^{k-k_0q} = a^k \cdot (a^{k_0})^{-q}$. Якщо $-q > 0$, то $(a^{k_0})^{-q} \in H$, як добуток елемента $a^{k_0} \in H$ самого на себе $-q$ раз, якщо $-q = 0$, то $(a^{k_0})^{-q} = e \in H$, якщо ж $-q < 0$, то $(a^{k_0})^{-q} = (a^{-k_0})^{|-q|}$ і знову належить H , як добуток елемента a^{-k_0} оберненого до $a^{k_0} \in H$, самого на себе $|-q|$ раз. Оскільки $a^k \in H$, то $a^r \in H$, як добуток елементів $a^k, (a^k)^{-q} \in H$. Якби $r \neq 0$, то в силу нерівності $r < k_0$ в H знайшовся би елемент a^r із натуральним показником, меншим за k_0 , що суперечить вибору k_0 . Отже, $r = 0$. Тоді $k = k_0q$ і $a^k = (a^{k_0})^q$. Внаслідок довільності елемента $a_k \in H$, підгрупа H є циклічною.

§1.8. ВІДНОШЕННЯ ЕКВІВАЛЕНТНОСТІ. СУМІЖНІ КЛАСИ

Як уже підкреслювалося, основними об'єктами сучасної математики є математичні структури – множини з одним або декількома відношеннями. Алгебраїчні операції – окремий вид відношень, точніше, функціональних відношень. Зрозуміло, що можуть існувати структури, яких поряд з алгебраїчною операцією задано деякі інші відношення, зокрема, відношення еквівалентності. Зараз зупинимось на розгляді груп, в яких додатково введено деяке відношення еквівалентності. Інтерес становлять тільки ті відношення еквівалентності, які певним способом узгоджені з груповою операцією. Оскільки операція в групі, взагалі кажучи, некомутативна, то приходить розглядати відношення еквівалентності, узгоджені з груповою операцією зліва, і відношення еквівалентності, узгоджені з груповою операцією справа.

Означення 7. Говорять, що відношення еквівалентності $\sim$ означене на групі G , узгоджується з груповою операцією зліва, якщо

$$\forall a \in G, \forall b, b' \in G : b \sim b' \rightarrow ab \sim ab'.$$

і справа, якщо

$$\forall a \in G, \forall b, b' \in G : b \sim b' \rightarrow ba \sim b'a.$$

Наведемо приклади відношень еквівалентності, узгоджених з груповою операцією зліва і справа.

Означення 8. Нехай H – довільна підгрупа групи G . Елементи $a, b \in G$ будемо називати конгруентними за модулем H зліва і записувати $a \equiv b \pmod{H}$ якщо $a^{-1}b \in H$, і справа та записувати $a \equiv b \pmod{H}$, якщо $ab^{-1} \in H$.

Теорема 1.7. Відношення конгруентності зліва (справа) за модулем підгрупи H є відношенням еквівалентності на G , узгодженим з груповою операцією зліва (справа).

Доведення. Теорему доведемо для відношення конгруентності зліва (для конгруентності справа доведення аналогічне).

Перевіримо спочатку, що відношення конгруентності зліва за модулем підгрупи є відношенням еквівалентності.

$$\forall a \in G : a \equiv a \pmod{H}, \text{ бо } a^{-1}a = e \in H.$$

1. Якщо $a \equiv b \pmod{H}$, то елемент $x = a^{-1}b \in H$. Тоді підгрупі належить і елемент $x^{-1} = (a^{-1}b)^{-1} = b^{-1}a$, тобто $b^{-1}a \in H$. Це і означає, що $b \equiv a \pmod{H}$.

2. Якщо $a \equiv b \pmod{H}$ і $b \equiv c \pmod{H}$, то елементи $a^{-1}b, b^{-1}c \in H$. Тоді їх добуток $(a^{-1}b)(b^{-1}c) = a^{-1}(bb^{-1})c = (a^{-1}e)c = a^{-1}c$, тобто елемент $a^{-1}c$ належить H .

Значить, $a \equiv c \pmod{H}$.

Залишилося показати, що дане відношення еквівалентності узгоджене з груповою операцією зліва, тобто, що

$$(\forall a, b, c \in G) : (a \equiv b \pmod{H}) \rightarrow (ca \equiv cb \pmod{H}).$$

Щоб довести справедливості останньої конгруенції, треба показати, що

$$(ca)^{-1}(cb) = (a^{-1}c^{-1})(cb) = a^{-1}(c^{-1}c)b = (a^{-1}e)b = a^{-1}b \in H$$

а остання належність очевидна, бо $a \equiv b \pmod{H}$.

Отже, відношення конгруентності зліва (справа) за модулем є відношенням еквівалентності на G , узгодженим з груповою операцією зліва (справа).

Виявляється, що відношень еквівалентності на групі G , узгоджених з груповою операцією зліва (справа), які були б відмінними від відношення конгруентності зліва (справа) за модулем підгрупи H взагалі немає. Інакше кажучи, відношення конгруентності зліва (справа) за модулем підгрупи H є універсальним відношенням еквівалентності, узгодженим зліва (справа) з груповою операцією. Точніше така теорема, яку приймемо без доведення.

Теорема 1.8. Для всякого відношення еквівалентності $\sim$ на групі G , узгодженою з груповою операцією зліва (справа) існує підгрупа H групи G така, що відношення $\sim$ є відношенням конгруентності зліва (справа) за модулем підгрупи H .

§1.9. СУМІЖНІ КЛАСИ

Відомо що всяке відношення еквівалентності на множині визначає розбиття цієї множини на класи еквівалентних між собою елементів. Відношення конгруентності зліва за модулем підгрупи H групи G , як відношення еквівалентності розбиває множину G на класи еквівалентності. Ці класи еквівалентності називають в даному випадку лівими суміжними класами.

Означення 9. Лівим суміжним класом K_a групи G за підгрупою $H \in G$, породженим елементом $a \in G$, називається клас еквівалентності відношення конгруентності зліва за модулем H , якому належить a , тобто сукупність усіх елементів $b \in G$, конгруентності зліва із a за модулем H .

Аналогічно запроваджуються поняття правого суміжного класу. Нам треба встановити вигляд лівих суміжних класів, дати їх чіткіше опис. З цією метою введемо спочатку поняття добутку підмножин групи G і відзначимо його деякі властивості, що будуть використані далі.

Означення 10. Добутком підмножин A та B групи G називається підмножина AB цієї групи, яка складається із усіх, тих і тільки тих, елементів $x \in G$, які можна записати у вигляді $x = ab$, де $a \in A, b \in B$. Отже, $AB = \{ab \mid a \in A, b \in B\}$.

У випадку, коли $A = \{a\}$, тобто, множина A складається тільки з одного елемента a , добуток AB записується так aB . Відзначимо деякі властивості:

1. Множення підмножини групи G асоціативне:

$$(\forall A, B, C \in G): A(BC) = (AB)C. \quad (1)$$

Справді, на підставі асоціативності групової операції

$$(\forall x \in A(BC)): x = a(bc) = (ab)c \in (AB)C$$

і навпаки, $(\forall x \in (AB)C): x = (ab)c = a(bc) \in A(BC)$, звідси і випливає рівність (1).

2. Якщо $A, B \in G$ і $A = B$, то $(\forall c \in G): cA = cB$.

Дійсно, всякий елемент $x \in cA$ має вигляд $x = ca$, $a \in A$.

Оскільки $A = B$, то $a \in B$. Тому $x = ca$ $a \in B$ тобто $x \in cB$.

Таким чином, $cA \subset cB$. Аналогічно навпаки: $cB \subset cA$.

3. Якщо H – підгрупа групи G , то $H * H = H$.

Всякий елемент x множини $H * H$ має вигляд $x = ab, a \in H, b \in H$.

Оскільки H – підгрупа, то $ab \in H$, тобто, $H * H \in H$. Навпаки, для $\forall x \in H: x = xe, x \in H, e \in H$, тобто $HH * H$.

Наступна теорема дає зручний для багатьох випадків опис лівих суміжних класів.

Теорема 1.9. Підмножина K групи G є лівим суміжним класом групи G за підгрупою H тоді і тільки тоді, коли, де a – деякий елемент групи G . $K = aH$.

Доведення: Нехай K – лівий суміжний клас групи G за підгрупою H . Треба довести, що $\exists a \in G: K = aH$.

Нехай a – довільний елемент класу K . Тоді за означенням класу K як класу еквівалентності зліва за модулем H .

Покажемо, що $K = aH$. Оскільки ця рівність є рівністю двох множин, то і доводити її будемо відповідним чином.

Якщо $b \in K$, то $a \equiv b \pmod{H}$, тобто, елемент $x = a^{-1}b \in H$, звідки $b = ax, x \in H$, звідки елемент $a^{-1}b = x \in H$. Це значить, що $a \equiv b \pmod{H}$ тобто, $b \in K$. Цим рівність $K = aH$ доведена, тобто, доведено, що для всякого суміжного класу K існує елемент $a \in G$, такий що $K = aH$.

Покажемо тепер, що, навпаки, всяка підмножина aH , де a – довільний елемент групи G , є лівим суміжним класом групи G за підгрупою H .

Нехай b – довільний елемент підмножини aH . Тоді $(\exists x \in H): b = ax$, звідки $a^{-1}b = x \in H$, тобто, $a \equiv b \pmod{H}$.

Зворотне включення доводиться точно так само, як і вище. Отже, $aH = Ka$, тобто, aH – лівий суміжний клас групи G за підгрупою H . **Теорема доведена.**

Як бачимо, всякий лівий суміжний клас групи G за підгрупою H співпадає з множиною aH , де a – довільний елемент цього класу, і, навпаки, множина aH , де a – довільний елемент групи G , є лівим суміжним класом групи G за підгрупою H . Тому скрізь далі лівий суміжний клас групи G за підгрупою H ми будемо записувати у вигляді aH , де a – елемент групи G .

Аналогічні міркування справедливі і по відношенні до правих суміжних класів і тому далі скрізь правий суміжний клас групи G за підгрупою H , ми будемо записувати у вигляді Ha , де a – елемент групи G .

Відзначимо деякі властивості лівих суміжних класів (для правих суміжних класів властивості аналогічні).

Різні суміжні класи aH і bH групи G взаємно неперерізні і об'єднання всіх лівих суміжних класів утворює групу G

Цей факт безпосередньо впливає із того, що сукупність лівих суміжних класів групи G за підгрупою H утворює розбиття групи G .

1. Серед лівих суміжних класів групи G за підгрупою H є сама підгрупа H , бо $H = eH$

2. Якщо $a \notin H$, то aH не є підгрупою групи G .

Справді, якби aH була підгрупою, то одиничний елемент e належав би aH , тобто $e \in aH$, тобто існував би такий елемент $x_0 \in H$, що $e = ax_0$, звідки, $a = x_0^{-1} \in H$, тобто $a \in H$ всупереч умові.

3. Якщо підгрупа H групи G скінченна і містить точно m елементів, то і кожен лівий суміжний клас aH теж містить точно m різних елементів.

Дійсно, якщо $H = \{a_1, a_2, \dots, a_m\}$, то $aH = \{aa_1, aa_2, \dots, aa_m\}$.

Якби для деяких i, j було $aa_i = aa_j$, то домноживши цю рівність на a^{-1} зліва, ми одержали б $a_i = a_j$, всупереч умові ($a_1, a_2, \dots, a_m$ – різні елементи підгрупи H).

В теорії груп часто приходить розглядати множини, елементами яких служать ліві чи праві суміжні класи.

Означення 11. Сукупність M_l усіх лівих суміжних класів групи G за підгрупою H називається лівостороннім розкладом групи за підгрупою H , а сукупність M_r , всіх правих суміжних класів – правостороннім розкладом G за H .

Таким чином,

$$M_l = \{H, aH, bH, \dots\}, M_r = \{H, Ha, Hb, \dots\}.$$

Якщо група G абелева, то

$$(\forall a, b \in G): (a \equiv b \pmod{H}) \Leftrightarrow (a \equiv b \pmod{H})$$

Справді,

$$(a \equiv b \pmod{H}) \Leftrightarrow (a^{-1}b \in H) \Leftrightarrow (ba^{-1} \in H) \Leftrightarrow (b \equiv a \pmod{H}) \Leftrightarrow (a \equiv b \pmod{H}).$$

Тому у випадку абелевої групи не розрізняють конгруенції зліва і справа за модулем H , а просто говорять про конгруентність за модулем H . Оскільки у випадку абелевої групи $(\forall a \in G)(aH = Ha)$ і, очевидно, $M_l = M_r$, то для абелевих груп вживають тільки терміни суміжний клас і розклад групи G за підгрупою H .

Цією домовленістю щодо термінології ми скористуємось зараз при розгляді прикладів.

Приклади 1. Знайдемо суміжні класи абелевої групи $\langle C_0, \times \rangle$, де C_0 – множина не рівних нулю комплексних чисел, за підгрупою $H = \{z \in C_0 \mid |z| = 1\}$.

Оскільки суміжний клас – це сукупність всіх елементів, конгруентних між собою за модулем підгрупи H , то для опису цієї сукупності треба знайти необхідну і достатню умову того, щоб 2 елементи групи $\langle C_0, \times \rangle$, були конгруентні за модулем H .

За означенням $a \equiv b \pmod{H}$, тоді і тільки тоді, коли $a^{-1}b = \frac{b}{a} \in H$, тобто коли $\left| \frac{b}{a} \right| = 1$ інакше, $|b| = |a|$.

Отже, два числа $a, b \in C_0$ конгруентні за модулем H тоді і тільки тоді, коли $|b| = |a|$. Це означає, що довільний суміжний клас групи C_0 за підгрупою H є сукупність всіх комплексних чисел, які мають один і той же модуль. Сукупність всіх комплексних чисел з одним і тим же модулем r геометрично являє собою коло, радіуса r з центром в початку координат. Отже, геометрично суміжний клас групи $\langle C_0, \cdot \rangle$ за підгрупою H – коло з центром в початку координат, а сукупність всіх таких концентричних кіл – розклад групи C_0 за підгрупою H .

Приклади 2. Нехай $\langle \mathbb{Z}, + \rangle$ адитивна група цілих чисел і $m\mathbb{Z} = (m)$ – її підгрупа, що складається із усіх цілих чисел кратних m . Оскільки група $\mathbb{Z}$

абелева, то умова конгруентності $a \equiv b \pmod{m}$ виглядає так: $(-a) + b = b - a \in m\mathbb{Z}$, тобто $a \equiv b \pmod{m}$, тоді і тільки тоді, коли $a - b : m$ (ділиться без остачі на m).

Зауважимо, що різниця чисел a і b ділиться на m без остачі тоді і тільки тоді, коли при діленні на m a і b дають однакові остачі. Справді, нехай $a = mq_1 + r_1$, $b = mq_2 + r_2$, тоді $a - b = m(q_1 - q_2) + (r_1 - r_2)$. Якщо, $r_1 = r_2$, то $a - b = m(q_1 - q_2) : m$.

Якщо ж $(a - b) : m$, то ліва частина рівності $(a - b) - m(q_1 - q_2) = r_1 - r_2$ ділиться на m . Тоді на m повинна ділитись і права $r_1 - r_2 : m$. Оскільки $0 \leq r_1, r_2 < m$ то $|r_1 - r_2| < m$. Тому подільність $r_1 - r_2 : m$ можлива тоді і тільки тоді, коли $r_1 - r_2 = 0$ тобто, $r_1 = r_2$.

Таким чином, два цілі числа a і b конгруентні за модулем $m\mathbb{Z}$ підгруп тоді і тільки тоді, коли при діленні на m числа a і b дають однакові остачі. З цього виходить, що будь-який суміжний клас групи Z за модулем $m\mathbb{Z}$, як множина всіх чисел, конгруентних між собою, є сукупністю всіх цілих чисел, які при діленні на m дають одну і ту ж саму остачу r . Зрозуміло, що всіх різних класів групи Z за підгрупою $m\mathbb{Z}$ є стільки, скільки є різних остач при діленні на m , бо кожна остача Z належить до одного і тільки одного класу. Всіх різних остач при діленні на $m \in m$, а саме: $0, 1, 2, \dots, m - 1$. Тому всіх різних суміжних класів за модулем $m\mathbb{Z}$ теж є m . Відповідно за теоремою 1.9 суміжний клас K , який є сукупністю всіх цілих чисел, що при діленні на m дають остачу r , можна записати у вигляді $r + m\mathbb{Z}$, бо $r = m * 0 + r$ і, значить, $r \in K$. Внаслідок цього розкладу групи Z підгрупою $m\mathbb{Z}$ запишеться так:

$$M = \{m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \dots, (m - 1) + m\mathbb{Z}\}.$$

3. Наведемо ще приклад відношення конгруентності та суміжних класів за цим відношенням в неабелевій групі. Для цього в симетричній групі S_n всіх підстановок n -го степеня розглянемо підгрупу H , що складається із усіх підстановок n -го степеня, які елемент n залишають незмінним, тобто переводять його в себе:

$$H = \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_{n-1}, n \end{pmatrix} \right\}.$$

Оскільки всі перестановки $k_1, k_2, \dots, k_{n-1}$ з чисел $1, 2, \dots, n-1 \in (n-1)!$
 $OrH = (n-1)!$

Нехай для підстановок τ, s, S_n справедливо $\tau \equiv s \pmod{eH}$, $r^{-1}s \in H$ і якщо $r^{-1} = \begin{pmatrix} 1, 2, \dots, n-1, n \\ t_1, t_2, \dots, t_{n-1}, t \end{pmatrix}$, внаслідок того, що $r^{-1}(n) = t_n$ і добуток $r^{-1}s$ пере-

водить число n в n , остання рівність справедлива тоді і тільки тоді, коли $r(t_n) = n$, $s(t_n) = n$. Це означає, що лівий суміжний клас групи S_n за підгрупою H є сукупністю всіх підстановок, які в число n переводять один і той же елемент t_n . Інакше кажучи, лівий суміжний клас групи S_n за підгрупою H є сукупністю всіх підстановок, в яких n має один і той же прообраз.

Із аналогічних міркувань, правий суміжний клас групи S_n за підгрупою H є сукупністю всіх підстановок, в яких n має один і той же образ.

$$H = \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_{n-1}, n \end{pmatrix} \right\}.$$

Внаслідок довільності елемента $a^k \in H$ всякий елемент із H є степенем елемента a , тобто H – циклічна підгрупа породжена елементом a .

Вправи:

1. Навести приклад підгруп деяких конкретних груп.
2. Якщо $a \in G$ – елемент порядку n , то для яких натуральних чисел s кратних n справедлива рівність $a^s = e$?
3. Показати, що коли H – підгрупа групи G , то для всякого цілого $s \in \mathbb{Z}$ та елемента $a \in H$ елемент a^s теж належить H .
4. Визначити порядок підстановок і групи.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ і } \psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ групи } S_3.$$

5. Знайти всі підгрупи симетричної групи S_3 .
6. Описати всі підгрупи адитивної групи $\mathbb{Z}$ цілих чисел.

Оскільки всі перестановки $k_1, k_2, \dots, k_{n-1}$ з чисел $1, 2, \dots, n-1 \in (n-1)!$
то $OrH = (n-1)!$

Нехай для підстановок τ, s, S_n справедливо $\tau \equiv s \pmod{H}$. Тоді $r^{-1}s \in H$ і якщо

$$\tau^{-1} = \begin{pmatrix} 1, 2, \dots, n-1, n \\ t_1, t_2, \dots, t_{n-1}, t_n \end{pmatrix}, \quad s = \begin{pmatrix} 1, 2, \dots, n-1, n \\ s_1, s_2, \dots, s_{n-1}, s_n \end{pmatrix}$$

то належність $\tau^{-1}s \in H$ рівносильна рівності:

$$\begin{pmatrix} 1, 2, \dots, n-1, n \\ t_1, t_2, \dots, t_{n-1}, t_n \end{pmatrix} \begin{pmatrix} 1, 2, \dots, n-1, n \\ s_1, s_2, \dots, s_{n-1}, s_n \end{pmatrix} = \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_{n-1}, k_n \end{pmatrix}.$$

Внаслідок того, що $\tau^{-1}(n) = tn$ і добуток $r^{-1}s$ переводить n в n , остання рівність справедлива тоді і тільки тоді, коли $s(t_n) = n$. Отже, конгруєнція $\tau \equiv s \pmod{H}$ справедлива тоді і тільки тоді, коли $\tau(t_n) = n$ і $s(t_n) = n$. Це означає, що лівий суміжний клас групи S_n за підгрупою є сукупність всіх підстановок, які в число n переводять один і той же елемент t_n . Інакше кажучи, лівий суміжний клас групи S_n за підгрупою H є сукупністю всіх підстановок, в яких n має один і той же прообраз.

Із аналогічних міркувань, правий суміжний клас групи S_n за підгрупою H є сукупністю всіх підстановок, в яких n має один і той же образ.

Лівосторонній і правосторонній розклади групи S_n за підгрупою H мають відповідно вигляд:

$$\psi_l = \left\{ \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ n, k_2, \dots, k_{n-1}, k_n \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, n, \dots, k_{n-1}, k_n \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, n-1, n \end{pmatrix} \right\} \right\}$$

$$\psi_r = \left\{ \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_{n-1}, 1 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_{n-1}, 2 \end{pmatrix} \right\}, \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_n, n \end{pmatrix} \right\} \right\}.$$

Ці два розклади мають спільним тільки один суміжний клас підгрупу $H = \left\{ \begin{pmatrix} 1, 2, \dots, n-1, n \\ k_1, k_2, \dots, k_{n-1}, n \end{pmatrix} \right\}$. Інші суміжні класи в цих розкладах, мають як легко бачити, різні. Тому розклади ψ_l і ψ_k теж різні.

Закінчимо даний параграф однією простою, але важливою теоремою, яку встановив ще у XVIII ст. Відомий французький математик Лагранж для випадку груп підстановок.

Теорема 1.10. (Лагранжа). Якщо група G скінчена і має порядок n , то порядок m всякої підгрупи H є дільником числа n .

Доведення. Оскільки різні суміжні класи групи G взаємно неперерізні, то в силу скінченності групи G кількість різних лівих суміжних класів цієї групи за підгрупою H скінчена і нехай дорівнює k . за властивістю 4° в кожному лівому суміжному класі є m елементів. Внаслідок цього і того, що різні суміжні класи групи G за підгрупою H спільних елементів не мають, а об'єднання їх співпадає з G , кількість елементів в групі дорівнює mk . За умовою кількість елементів групи G дорівнює n . Отже, $n = mk$, звідки m – дільник числа n . **Теорема доведена.**

Вправи:

1. Довести теорему 1.7 для відношення конгруентності справа.
2. Чи є операція множення підмножин абелевої групи комутативною?
3. Нехай H – підгрупа групи G . Довести, що сукупність всіх підмножин виду aH , де a – довільний елемент групи G , утворює розбиття групи G .
4. Довести, що коли $Or\ G = p$, де p – просте число, то група є циклічною.

Означення 12: Гомоморфізмом груп $(G, *)$ і $(G', \circ)$ називається відображення $\varphi: G \rightarrow G'$, яке зберігає операцію: $\forall a, b \in G$ виконується рівність $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Твердження 1.1. Якщо e одиниця G а e' одиниця G' то $\varphi(e) = e'$, де φ – гомоморфізм G та G' .

Означення 13. Бієктивний гомоморфізм груп G та G' називається ізоморфізмом цих груп і пишуть $G \approx G'$. Ізоморфізм групи G на себе називають автоморфізмом і позначають $AutG$.

Приклади. Відображення $\varphi: (R, +) \rightarrow (R, +)$, яке діє за правилом $\varphi(a) = r^a, \forall a \in R$, r – фіксоване додатне число, $r \neq 1$, є ізоморфізмом.

2. Якщо група G Абелева, то відображення $\varphi: G \rightarrow G, \varphi(a) = a - 1$, є ізоморфізмом групи G в себе.

Означення 14. Ядром гомоморфізму φ груп G та G' називають множину $ker\varphi := \{g \in G \mid \varphi(g) = e'\}$. Образ гомоморфізму φ – множина

$$\text{im } \varphi := \{g' \in G' \mid \exists g \in G: \varphi(g) = g'\}.$$

Означення 15. Кількість лівих (правих) суміжних класів групи G за підгрупою H називається індексом підгрупи H в групі G і позначається $(G : H)$.

Означення 16. Підгрупа $H \subseteq G$ називається нормальною (нормальним дільником) в групі G , якщо $\forall a \in G$ виконується $aH = Ha$.

Позначатимемо: $H \triangleright G$.

Твердження 1.2. Нехай H – підгрупа групи G . Тоді еквівалентними є такі умови:

- 1) $H \triangleright G$;
- 2) $gHg^{-1} = H$ для довільного $g \in G$;
- 3) $gHg^{-1} \subseteq H$ для довільного $g \in G$.

Зауваження. Зауважимо, що якщо $A \triangleright B$ та $B \triangleright C$, то A не обов'язково є нормальною в C .

Розділ II

КІЛЬЦЯ ТА ІДЕАЛИ

Як уже не раз відзначалось, основним об'єктом в сучасній алгебрі є алгебраїчні структури, тобто множини, в яких введено одну чи декілька алгебраїчних операцій, які задовольняють тим чи іншим умовам (аксіомам структури). В алгебрі на першому семестрі вивчалися дві важливі алгебраїчні структури – групи і поля. Вивчення алгебри на другому курсі розпочалося із встановлення ряду властивостей цілих чисел. В множині $\mathbb{Z}$ цілих чисел введені дві алгебраїчні операції – додавання і множення. Відносно операції додавання множина $\mathbb{Z}$ утворює адитивну абелеву групу, але, оскільки в ній є ще одна алгебраїчна операція – множення, її структура не є структурою групи. Множина $\mathbb{Z}$ цілих чисел не є і полем, бо жодне ціле число, крім 1 і -1 , не має в $\mathbb{Z}$ оберненого до себе. Таким чином, в математиці є множини з двома алгебраїчними операціями (внутрішніми законами композиції), які не є полями. Найважливіший клас серед них утворюють кільця.

§2.1. ОЗНАЧЕННЯ КІЛЬЦЯ

Означення 1. Непорожня множина K називається кільцем, якщо на ній означені дві алгебраїчні операції (внутрішні закони композиції) – додавання і множення, що задовольняють таким умовам:

1) асоціативність додавання:

$$\forall a, b, c \in K: (a + b) + c = a + (b + c);$$

2) комутативність додавання:

$$\forall a, b \in K: a + b = b + a;$$

3) в K існує нулевий елемент 0 такий, що

$$\forall a \in K: a + 0 = a;$$

4) для всякого елемента $a \in K$ існує протилежний елемент $-a$ такий, що

$$a + (-a) = 0;$$

5) асоціативність множення:

$$\forall a, b, c \in K: (ab)c = a(bc);$$

6) операція множення дистрибутивна по відношенню до додавання

$$\forall a, b, c \in K: a(b + c) = ab + ac, (b + c)a = ba + ca.$$

Якщо в кільці K операція множення є комутативна, тобто

$$\forall a, b \in K: ab = ba$$

то кільце K називається комутативним.

Якщо в кільці існує елемент 1 такий, що $\forall a \in K: a * 1 = 1 * a = a$, то кільце K називається кільцем з одиницею. Якщо для кожного не нульового елемента $a \in K$ існує обернений елемент, тобто, такий елемент $a^{-1} \in K$, що

$$aa^{-1} = a^{-1}a = 1,$$

то таке комутативне кільце K з 1 називається полем. Як бачимо, поле є кільцем. Наведемо приклади кілець, що не є полями.

Приклади.

1. Множина Z усіх цілих чисел утворює комутативне кільце з 1 , якщо за внутрішні закони композиції в Z взяти звичайні операції додавання і множення цілих чисел.

2. Множина M_n усіх матриць n -того порядку з елементами із даного числового поля утворює некомутативне кільце з одиницею, якщо за внутрішні закони композиції прийняти звичайні операції додавання і множення матриць. Виконання аксіом 1)-6) перевірилось при вивченні матриць на першому курсі.

3. Множина C усіх неперервних функцій на сегменті $[a, b]$ утворює комутативне кільце з 1 , якщо для довільних $f(x), g(x) \in C$, $(f + g)$ і (fg) означити так:

$$\forall x \in [a, b]: (f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x),$$

Той факт, що $(f + g)(x), (fg)(x) \in C$, відомий з аналізу (сума і добуток неперервних функцій – функції неперервні). Виконання аксіом 1), 2), 3),

б) впливає із справедливості цих умов для додавання і множення дійсних чисел (при всякому $x \in [a, b]$, $f(x)$ – дійсне число), наприклад,

$$(\forall f(x), g(x) \in C): (f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x).$$

Аналогічно перевіряється комутативність множення. Очевидно, роль нулевого елементу виконує функція $f(x) = 0$ ($x \in [a, b]$), протилежною до $f(x)$ є функція $-f(x)$, при всякому $x \in [a, b]$ приймає значення, протилежні до відповідних значень $f(x)$. Одиничним елементом служить функція $f(x) = 1$ ($x \in [a, b]$).

Зауважимо, що множина C не є полем, тому, що для всякої функції $f(x) \in C$, яка має в точці $x_0 \in [a, b]$ корінь, обернена функція має в точці x_0 розрив, і значить не належить C .

Відзначимо, що деякі автори, наприклад, А. Г. Курош (3), в означення кільця не включають аксіому 5), тобто, не ставлять вимоги щоб множення було асоціативним. Тоді серед кілець є неасоціативні кільця (наприклад, кільця Лі і кільця Жордана, див. (3)).

§2.2. НАЙПРОСТІШІ ВИСНОВКИ З АКСІОМАТИКИ

Означення 2. Всяке кільце K відносно операції додавання, означеної в ньому, утворює адитивну абелеву групу – адитивну групу кільця K .

Внаслідок цього всі властивості, які мають адитивні абелеві групи справедливі і у випадку довільного кільця K . Відзначимо деякі з них.

– Нулевий елемент кільця K є єдиним і всякий елемент кільця K має єдиний протилежний.

– Які б не були елементи $a, b \in K$ рівняння $a + x = b$ має єдиний розв'язок $x = b + (-a)$, який називають різницею елементів b та a і позначають $x = b - a$.

$$- \forall a, b \in K: -(a + b) = -a - b.$$

Аналогічно, як і для адитивних абелевих груп, вводиться поняття n -кратного елемента na до a :

$$na = \begin{cases} a + a + \dots + a, & n > 0 \\ 0, & n = 0 \\ |n| \cdot (-a) = (-a) + (-a) + \dots + (-a), & n < 0 \end{cases}$$

Нагадаємо, що n -кратний елемент на задовольняє співвідношення:

$$\forall a \in K, \forall m, n \in \mathbb{Z}: ma + na = (m + n)a, m(na) = (mn)a.$$

Означення 6. Всяке кільце K відносно операції множення, означеної в ньому, утворює мультиплікативну підгрупу.

Наявність асоціативного закону для множення дозволяє ввести поняття n -го степеня елемента a :

$$(\forall a \in K)(\forall n \in \mathbb{N}): a^n = \underbrace{a \cdot a \cdot a \cdot \dots \cdot a}_n$$

Означення 7. $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$ (для $m, n \in \mathbb{N}$; відповідні формули також справедливі для цілих показників у групі).

Відзначимо ще 4 властивості, при доведенні яких використовується дистрибутивність множення відносно додавання.

Означення 8. $(\forall a, b \in K): a(b - c) = ab - ac$ (дистрибутивний закон для різниці).

На підставі означення досить показати, що

$$ac + a(b - c) = ab.$$

В справедливості останньої рівності пересвідчуємось, використовуючи аксіому 6) і означення різниці $b - c$:

$$ac + a(b - c) = a(c + (b - c)) = ab.$$

Означення 9. $(\forall a \in K): a * 0 = 0$.

Справді, який би не був елемент $x \in K$:

$$a * 0 = a(x + (-x)) = a(x - x) = ax - ax = ax + (-ax) = 0.$$

Як відомо, в довільному полі і в кільці $\mathbb{Z}$ цілих чисел справедливе обернене твердження:

$$(\forall a, b \in K): (ab = 0) \text{ звідси } (a = 0) \text{ або } (b = 0).$$

У випадку довільного кільця це твердження, взагалі кажучи, невірне. Існують кільця, в яких із рівності $ab = 0$ не випливає, що a або b дорівнюють 0.

Наприклад, в кільці M_2 матриць 2-го порядку:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Це зауваження дозволяє ввести нове поняття, поняття дільника нуля.

Означення 10. Якщо для деяких елементів $a, b \in K, a \neq 0, b \neq 0$, справедлива рівність $ab = 0$, то елементи a , та b називають дільниками нуля (точніше, a – лівим дільником, b – правим дільником 0).

В кільці M_2 дільниками нуля є, наприклад, матриці

$$\begin{pmatrix} \alpha & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & \beta \end{pmatrix}, (\alpha, \beta \neq 0).$$

Вивчення кілець, в яких є дільники 0, дещо ускладнюється. В подальшому ми будемо займатися вивченням тільки тих кілець, в яких немає дільників 0. Комутативне кільце, в якому нема дільників нуля, називається **областю цілісності**.

Означення 11. Перша рівність означає. Що елемент $(-a)b$ має бути протилежним до ab , тобто, має виконуватись рівність: $ab + (-a)b = 0$.

Ця рівність легко випливає із аксіом 6) і 4) та властивості 9:

$$ab + (-a)b = (a + (-a))b = 0b = 0.$$

Аналогічно доводиться, що $a(-b) = -ab$.

Справедливість останньої рівності легко виводиться із перших двох $(-a)(-b) = -a(-b) = -(-ab) = ab$, бо із рівності $a + (-a) = 0$ в аксіомі 4) виходить, що $(-a) + a = 0$, тобто елементом, протилежним до $(-a) \in a - (-a) = a$.

Означення 12. Якщо ненулевий елемент $a \in K$ не є дільником нуля, то із рівності $ab_1 = ab_2$ ($b_1, b_2 \in K$) випливає: $b_1 = b_2$. Це означає, що рівності можна скорочувати на ненульовий елемент, який не є дільником нуля.

Справді, додавання до обох частин рівності $ab_1 = ab_2$ елемент $-ab_2$, ми одержимо:

$$ab_1 - ab_2 = 0,$$

або в силу властивості

$$a(b_1 - b_2) = 0.$$

Оскільки елемент a не є дільником нуля, то $b_1 - b_2 = 0$, тобто $b_1 = b_2$.

Зауважимо, що скорочувати рівності на дільники нуля не можна. Справді, як легко пересвідчитись, в кільці M_2 справедлива рівність

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 3 & 0 \end{pmatrix},$$

в той час, як

$$\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

§2.3. ПІДКІЛЬЦЕ

Одним із важливих напрямків в теорії кілець є вивчення кілець підмножин кільця. Серед усіх підмножин кільця особливо виділяються ті підмножини, які самі є кільцями відносно операцій, означених в усьому кільці.

Означення 14. Підмножина K_0 кільця K , яка сама є кільцем відносно операцій, означених в K , називається підкільцем кільця K .

Наступна теорема дозволяє спростити фактичну перевірку того, чи утворює певна підмножина кільця його підкільце.

Теорема 2.1. Підмножина K_0 кільця K є підкільцем кільця K тоді і тільки тоді, коли

- 1) $(\forall a, b \in K_0): a + b \in K_0$,
- 2) $(\forall a \in K_0): -a \in K_0$,
- 3) $(\forall a, b \in K_0): ab \in K_0$.

Доведення. Якщо підмножина $K_0 \subset K$ є підкільцем K , то виконання умов 1)-3) гарантоване означенням кільця K .

Якщо підмножина K_0 кільця K , навпаки, задовольняє умовам 1)-3), то із умов 1) і 3) випливає, що вона замкнена відносно операції додавання і множення кільця K , тобто, що на K задані операції додавання і множення, причому K_0 можна розглядати незалежно від включення $K_0 \subset K$. Оскільки

все ж таки $K_0 < K$ і в K_0 задані ті ж операції, що і в усьому кільці K , то підмножина K_0 задовольняє аксіомам 1), 2), 5), 6) із означення кільця.

Із умови 2 випливає, що для всякого $a \in K_0$ елемент $-a \in K_0$. Тоді із умови 1) випливає, що $a + (-a) = 0$ належить K_0 . Отже в K_0 існує нулевий елемент 0 і для всякого $a \in K_0$ існує $-a$ що теж належить K_0 . Отже, підмножина K_0 задовольняє всім аксіомам із означення кільця, тобто вона є підкільцем кільця K .

Приклади.

1. Підмножина P усіх парних цілих чисел є підкільцем кільця Z цілих чисел.

Справді, сума, добуток, парних чисел і число, протилежне до парного, є парними. Це означає що P задовольняє умовам теореми 2.1, значить P є підкільцем кільця Z .

Множина P усіх парних неперервних функцій утворює підкільце кільця C усіх неперервних функцій на $[-1, 1]$.

Дійсно, для довільних функцій $f(x), g(x) \in P$ справедливо:

$$(f + g)(x) = f(-x) + g(-x) = f(x) + g(x) = (f + g)(x),$$

$$(fg)(x) = f(-x)g(-x) = f(x)g(x) = (fg)(x),$$

$$(-f)(-x) = -f(-x) = -f(x) = (-f)(-).$$

Отже,

$$(\forall f, g \in P): f + g, fg, -f \in P.$$

Тобто, множина P на підставі теореми 2.1, є підкільцем кільця C .

3. Множина D_n усіх діагональних матриць n -го порядку є підкільцем кільця M_n усіх матриць n -го порядку над полем P , бо сума, добуток діагональних матриць, і матриця, протилежна до діагональної, є діагональними.

Зауваження. Умова 2) у формулюванні теореми 2.1 може бути замінена умовою:

$$2') (\forall a, b \in K): a - b \in K.$$

Справді, якщо умова 2') виконується, то для всякого елемента $b \in K_0$ існує $-b \in K_0$ і тоді на підстав умови 1) ми матимемо:

$$a - b = a + (-b) \in K_0.$$

Навпаки, якщо справджується умова 2'), то

$$(\forall a, \in K): -a = 0 - a \in K_0,$$

бо $0 = a - a$ і значить, належить K_0 .

Закінчемо параграф переліком деяких підкілець довільного кільця.

1. Множина $O = \{0\}$, яка складається тільки з одного нульового елемента кільця K , утворює, очевидно, підкілець кільця K . Це підкілець називають **нульовим підкілєм** K .

2. Кільце K є, очевидно, підкілєм самого себе. Підкілець O і K називають **тривіальними** підкілцями кільця K , а всі інші підкілця – нетривіальними або власними підкілцями.

Якщо K_α – деякі підкілця кільця K , то їх перетин $K_0 = \bigcap_{\alpha} K_\alpha$ теж є підкілєм кільця K .

Дійсно, якщо $a \in K_0$, то $a \in K_\alpha$ при всякому α . Оскільки K_α – підкілець, то $-a \in K_\alpha$. Значить, при всякому α елемент $-a \in K_\alpha$. Тому $-a \in \bigcap_{\alpha} K_\alpha = K_0$.

Якщо $a, b \in K_\alpha$, то при всякому α : $a, b \in K_\alpha$ і отже, внаслідок того, що K_α підкілець, $a + b, ab \in K_\alpha$ при всякому α . Таким чином, $a + b, ab \in \bigcap_{\alpha} K_\alpha = K_0$. Як

бачимо, задовольняє умови теореми 2.1 і тому є підкілєм кільця K .

Відомо, яку важливу роль в теоремі груп відіграють циклічні підгрупи (a) , породжені елементом a . В наступному пункті побудоване підкілець, яке є аналогом циклічної підгрупи.

1. Нехай K – деяке кільце, a – елемент кільця K . Тоді множина $K\alpha$ усіх можливих сум

$$n_1 a^{m_1} + n_2 a^{m_2} + \dots + n_k a^{m_k},$$

де $n_1, n_2, \dots, n_k$ – довільні цілі числа, $m_1, m_2, \dots, m_k$ довільні натуральні числа, утворює підкілець кільця K , яке називається підкілєм, породженим елементом a . За означенням

$$K\alpha = \{n_1 a^{m_1} + n_2 a^{m_2} + \dots + n_k a^{m_k} \mid n_i \in \mathbb{Z}, m_i \in \mathbb{N}, i = 1, 2, 3, \dots, k\}$$

Щоб показати, що множина $K\alpha$ – підкілець кільця K , досить перевірити виконання 1.-3. Із теореми 2.1. В силу асоціативності додавання ви-

конання умови 1. Очевидне, бо скінчених сумах можна довільно розставляти дужки, зокрема, їх опускати:

$$\begin{aligned} & (n_1 a^{m_1} + n_2 a^{m_2} + \dots + n_k a^{m_k}) + (n'_1 a^{m'_1} + n'_2 a^{m'_2} + \dots + n'_k a^{m'_k}) = \\ & = (n_1 n'_1) a^{m_1+m'_1} + \dots + (n_2 n'_2) a^{m_2+m'_2} + \dots + (n_k n'_k) a^{m_k+m'_k} \in K\alpha. \end{aligned}$$

§2.4. ГОМОМОРФІЗМИ ТА ІЗОМОРФІЗМИ КІЛЕЦЬ

1. Як відомо, одним із основних понять математики є поняття, функції, відображення. Це поняття вивчається і в математичному аналізі, і в геометрії, і в алгебрі. При вивченні алгебраїчних структур найбільший інтерес становлять ті відображення, які певним способом узгодженні із алгебраїчною структурою, що вивчається. В теорії груп такими відображеннями є гомоморфізми, тобто, такі ж відображення f групи G в групу G' що

$$(\forall a, b \in G): f(ab) = f(a)f(b).$$

В теорії кілець вивчаються відображення, які аналогічним способом узгоджені з алгебраїчними операціями, означеними в кільці. Такі відображення називаються кільцевими гомоморфізмами.

Означення 15. Відображення f кільця K в кільце K' називається гомоморфізмом, якщо

$$(\forall a, b \in K): f(a + b) = f(a) + f(b), f(ab) = f(a)f(b).$$

Перша з цих умов означає, що кільцевий гомоморфізм f в груповим гомоморфізмом адитивної групи кільця K в адитивну групу кільця K' . Внаслідок цього всі властивості групових гомоморфізмів справедливі і для кільцевих гомоморфізмів. Зокрема:

1. $f(0) = 0'$;
2. $(\forall a \in K): f(-a) = -f(a)$.

Аналогічно, як і випадку груп, гомоморфізм $f: K \rightarrow K'$, який є ін'єктивним відображенням, називається **мономорфізмом**: гомоморфізм $f: K \rightarrow K'$, який є сур'єктивним відображенням, називається **епіморфізмом**: гомоморфізм $f: K \rightarrow K'$, який є бієктивним відображенням, називається **ізоморфізмом**.

У зв'язку із властивостями 1 і 2. Виникає питання, чи не будуть аналогічні властивості справедливі відносно операцій множення. Виявляється, що будуть, але при деяких обмеженнях на кільця або на відображення f . Сформулюємо їх:

1. Якщо в кільці K існує 1 і f є епіморфізмом кільця K в кільці K' , то в кільці K' теж існує $1'$ і $f(1)=1'$.

Справді, внаслідок сур'єктивності відображення f :

$$(\forall a \in K') (\exists a \in K): a' = f(a).$$

Тоді

$$(\forall a \in K'): a' f(1) = f(a) f(1) = f(a * 1) = f(a) = a'$$

$$(\forall a \in K'): f(1) a' = f(1) f(a) = f(1 * a) = f(a) = a'.$$

Звідси виходить, що елемент $f(1)$ відіграє роль одиниці в кільці K' , тобто $f(1) = 1'$. Зауважимо, що одиничні елементи в кільцях K і K' є єдиними.

2. Якщо в кільці K існує 1 , кільце K' є областю цілісності з одиницею $1'$, то для всякого ненульового гомоморфізму $f: K \rightarrow K'$ справедливо $f(1) = 1'$.

Дісно,

$$(\forall a \in K) f(a) = f(a \cdot 1) = f(a) f(1)$$

і з другого боку, $f(a) = f(a) 1'$, звідси $f(a) f(1) = f(a) 1'$ або інакше $f(a)[f(1) - 1'] = 0$.

Оскільки в K' нема дільників нуля і a можна підібрати так, щоб $a \in K$ ми включаємо тривіальний випадок: $(\forall a \in K): f(a)=0$, то з наступної рівності виходить, що $f(1) = 1'$, відповідно, і відображення $f: K \rightarrow K'$ є таким, що $f(1) = 1'$. Якщо існує обернений елемент для a^{-1} для елемента $a \in K$, то існує обернений елемент для $f(a)$ і при цьому

$$f(a^{-1}) = (f(a))^{-1}.$$

Твердження випливає із рівностей:

$$f(a) f(a^{-1}) = f(a a^{-1}) = f(1) = 1',$$

$$f(a^{-1}) f(a) = f(a^{-1} a) = f(1) = 1'.$$

Для групового гомоморфізму вводять поняття ядра $Ker f$ і області значень $Im f$. Аналогічні поняття вводяться і для кільцевого гомоморфізму.

Означення 16. Ядром гомоморфізму $f: K \rightarrow K'$ називається множина $Ker f$ всіх тих елементів $f \in K$, які відображенням f переводяться в нулевий елемент 0 кільця K' :

$$Ker f = \{x' \in K' \mid \exists x \in K : f(x) = x'\}.$$

Областю значень або образом гомоморфізму $f: K \rightarrow K'$ називається множина $Im f$ всіх тих елементів в K' , для яких існують такі елементи $x \in K$, що $x' = f(x)$, тобто,

$$Im f = \{x' \in K' \mid \exists x \in K : f(x) = x'\}.$$

Як відомо, у випадку групового гомоморфізму $f: G \rightarrow G'$ множини $Ker f$ і $Im f$ є підгрупами груп G і G' відповідно. Неважко перевірити, що у випадку кільцевого гомоморфізму $f: K \rightarrow K'$ множини $Ker f$ і $Im f$ є підкільцем кільця K і K' відповідно. До цього питання ми ще повернемося в параграфі 3.

Приклад. Розглянемо кільце D_3 усіх діагональних матриць 3-го порядку.

$$D_3 = \left\{ A = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix} \mid \alpha_1, \alpha_2, \alpha_3 \in R \right\}$$

і кільце R_3 усіх трьохвимірних векторів

$$R_3 = \{a = (\alpha_1, \alpha_2, \alpha_3) \mid \alpha_1, \alpha_2, \alpha_3 \in R\},$$

в якому операції задані так:

$$(\alpha_1, \alpha_2, \alpha_3) + (\alpha'_1, \alpha'_2, \alpha'_3) = (\alpha_1 + \alpha'_1, \alpha_2 + \alpha'_2, \alpha_3 + \alpha'_3),$$

$$(\alpha_1, \alpha_2, \alpha_3)(\alpha'_1, \alpha'_2, \alpha'_3) = (\alpha_1\alpha'_1, \alpha_2\alpha'_2, \alpha_3\alpha'_3).$$

Задамо відображення $f: D \rightarrow D'$ таким способом: якщо

$$A = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}, \text{ то } f(A) = (\alpha_1, \alpha_2, 0).$$

Відображення f є гомоморфізмом, Якщо

$$A = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}, B = \begin{pmatrix} \beta_1 & 0 & 0 \\ 0 & \beta_2 & 0 \\ 0 & 0 & \beta_3 \end{pmatrix},$$

то

$$A + B = \begin{pmatrix} \alpha_1 + \beta_1 & 0 & 0 \\ 0 & \alpha_2 + \beta_2 & 0 \\ 0 & 0 & \alpha_3 + \beta_3 \end{pmatrix}, f(A) = (\alpha_1, \alpha_2, 0), f(B) = (\beta_1, \beta_2, 0)$$

і значить

$$f(A + B) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, 0) = (\alpha_1, \beta_1, 0) + (\alpha_2, \beta_2, 0) = f(A) + f(B);$$

$$AB = \begin{pmatrix} \alpha_1\beta_1 & 0 & 0 \\ 0 & \alpha_2\beta_2 & 0 \\ 0 & 0 & \alpha_3\beta_3 \end{pmatrix},$$

$$f(AB) = (\alpha_1\beta_1, \alpha_2\beta_2, 0) = (\alpha_1, \beta_1, 0)(\alpha_2, \beta_2, 0) = f(A)f(B).$$

Очевидно, що

$$\text{Ker } f = \left\{ A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \alpha \end{pmatrix} \mid \alpha \in R \right\},$$

$$\text{Im } f = \{a = (\alpha_1, \alpha_2, 0) \mid \alpha_1, \alpha_2 \in R\}.$$

II. Серед гомоморфізмів особлива роль належить ізоморфізмам. Якщо існує ізоморфне відображення кільця K на кільце K' , то кільця K та K' називають **ізоморфними**. Ізоморфні кільця мають цілком однакові алгебраїчні властивості і фактично їх можна не розрізняти. З цієї точки зору цікавим є наступне твердження.

Теорема 2.2. Якщо кільце K ізоморфне множині M з двома алгебраїчними операціями – додавання та множення, то множина M теж є кільцем.

Доведення. Нехай кільце K ізоморфне множині M , на якій означено операції додавання і множення. Нам треба довести, що множина M є кі-

льцем. Оскільки на множині M операції вже означено, то залишається тільки показати, що ці операції задовольняють аксіоми кільця.

Оскільки кільце K ізоморфне M , то відображення ізоморфне $f: K \rightarrow M$. Відображення f зокрема є сур'єктивним і, значить:

$$(\forall a', b', c' \in M) (\exists a, b, c \in K): a' = f(a), b' = f(b), c' = f(c).$$

Тоді, в силу гомоморфності відображення f і справедливості аксіом кільця для операцій, означених на K , ми матимемо:

$$(a' + b') + c' = (f(a) + f(b)) + f(c) = f(a + b) + f(c) = f((a + b) + c);$$

$$f(a + (b + c)) = f(a) + f(b + c) = f(a) + (f(b) + f(c)) = a' + (b' + c');$$

$$\begin{aligned} (a'b')c' &= (f(a)f(b))f(c) = f(ab)f(c) = f((ab)c) = f(a(bc)) = \\ &= f(a)f(bc) = f(a)(f(b)f(c)) = a'(b'c'); \end{aligned}$$

$$a' + b' = f(a) + f(b) = f(a + b) = f(b) + f(a) = b' + a';$$

$$a'(b' + c') = f(a)(f(b) + f(c)) = f(a)f(b + c) = f(a(b + c)) = f(ab + ac) =$$

$$= f(ab) + f(ac) = f(a)f(b) + f(a)f(c) = a'b' + a'c'.$$

Таким чином, операції, означені на множині M , задовольняють аксіоми 1), 2), 5) і 6) означення кільця. Роль нулевого елемента в M виконує $f(0)$:

$$a' + f(0) = f(a) + f(0) = f(a + 0) = f(a) = a',$$

протилежним елементом до елемента $a' = f(a)$ є елемент $f(-a)$:

$$a' + f(-a) = f(a) + f(-a) = f(a + (-a)) = f(0) = 0'.$$

Отже, множина M є кільцем.

Як бачимо, ізоморфізм переносить алгебраїчні властивості з однієї множини на другу. При допомозі ізоморфізму можна розв'язати і питання про існування обернених елементів. Цим займемося в наступному пункті.

ІІІ. Поле дробів області цілісності. Якщо кільце K є кільцем з одиницею, то деякі елементи цього кільця мають обернені до себе. Постараємося з'ясувати, для яких елементів кільця існують обернені елементи. Справді, якщо a – дільник нуля кільця K , тобто, існує такий елемент

$b \in K, b \neq 0$, що $ab = 0$, то припустивши існування елемента a^{-1} і домноживши останню рівність на a^{-1} , дістанемо:

$$a^{-1}(ab) = a^{-1} * 0, (a^{-1}a)b = 0, b = 0, \text{ всупереч умові } b \neq 0.$$

Отже, шукати елементи, що мають обернені, треба серед недільників нуля. Виникає питання: чи кожен елемент, що не є дільником нуля, має обернений? Відповідь одержується, коли з цього погляду розглянути кільце Z цілих чисел. В кільці Z обернені елементи мають тільки 1 і -1 . Інші числа обернених елементів не мають і в той же час вони не є дільниками нуля. Отже, не всі недільники нуля мають обернені елементи. Однак, для кільця Z цілих чисел існує більш широке кільце – поле раціональних чисел, яке містить кільце Z і в якому кожне ненульове ціле число має обернене число. Тоді можна поставити питання: чи не має місце аналогічна ситуація у випадку довільного кільця K ? Виявляється, що має і це можна обґрунтувати ввівши поняття ізоморфного вкладення кільця в кільце.

Означення 17. Говорять, що кільце K ізоморфно вкладається в кільце K' , якщо існує ізоморфне відображення кільця K на деяке підкільце K' .

Виявляється, що кожне кільце K можна ізоморфно вкласти в кільце K' , в якому всякий ненульовий елемент, що не є дільником нуля, має обернений. Обґрунтуємо зараз це твердження тільки для того випадку, коли K – область цілісності. Кільце K' виявиться при цьому полем. Отже, доведемо таку теорему.

Теорема 2.3. Всяка область цілісності K ізоморфно вкладається в поле $\bar{K}$.

Доведення. Щоб виробити підхід до доведення даної теореми, зауважимо, що поле раціональних чисел, яке містить в собі кільце цілих чисел і в якому кожне ненульове ціле число має обернене, одержується із кільця Z шляхом введення дробів $\frac{m}{n}$, де m, n – цілі числа, тобто шляхом розгляду впорядкованих пар цілих чисел. Доведення теореми 2.3 зводиться до фактичної побудови поля $\bar{K}$. Цю побудову здійснюватимемо аналогічно, як і при побудові поля раціональних чисел, тобто шляхом розгляду множини всіх впорядкованих пар елементів з кільця K .

I. Отже, розглянемо множину $\tilde{K}$ всіх впорядкованих пар (a, x) , $(a, x \in K, x \neq 0)$ елементів із кільця K . Ці пари зручно записувати у вигляді $\frac{a}{x}$ і називати дробами. Введемо в цій множині відношення рівності таким способом: дроби $\frac{a}{x}$ і $\frac{b}{y}$ будемо називати рівними, $\frac{a}{x} = \frac{b}{y}$, якщо $ay = bx$. Так введемо відношення, яке є відношенням еквівалентності на множині $\tilde{K}$. Справді, відношення рівності задовольняє всім трьом умовам з означення відношення еквівалентності:

$$\text{а) } \forall \frac{a}{x} \in \tilde{K} : \frac{a}{x} = \frac{a}{x}, \text{ бо } ax = ax \text{ / рефлексивність/;}$$

$$\text{б) } \forall \frac{a}{x}, \frac{b}{y} \in \tilde{K} : \left(\frac{a}{x} = \frac{b}{y} \right) \Rightarrow \left(\frac{b}{y} = \frac{a}{x} \right), \text{ бо з рівності}$$

$$ay = bx \Rightarrow bx = ay \text{ / симетричність/;}$$

$$\text{в) } \frac{a}{x}, \frac{b}{y}, \frac{c}{z} \in \tilde{K} : \left(\frac{a}{x} = \frac{b}{y} \right) \wedge \left(\frac{b}{y} = \frac{c}{z} \right) \Rightarrow \left(\frac{a}{x} = \frac{c}{z} \right), \text{ бо перемноживши рівності}$$

$$ay = bx \text{ і } bz = cy. \quad (1)$$

Одержимо $(ay)(bz) = (bx)(cy)$, звідси скориставшись асоціативністю і комутативністю множення в кільці K та властивістю 11, § 1, будемо мати.

$$az = cx \quad (2)$$

(це при умові, що $b \neq 0$: якщо $b = c$, то в силу того, що в K немає дільників нуля, з рівності (1) випливатиме: $a = 0, c = 0$ і тоді рівність (2) очевидна).

Відомо, що всяке відношення еквівалентності на множині визначає розбиття цієї множини на класи. Тому введене нами відношення рівності дробів в множині K визначає розбиття цієї множини класи рівних між собою дробів. Кожен такий клас є сукупністю всіх рівних між собою дробів і тому він повністю означається будь-яким своїм елементом $\frac{a}{x}$, через

це будемо його позначати так: $\left\{ \frac{a}{x} \right\}$. Різні такі класи не містять рівних між собою дробів і об'єднання всіх таких класів співпадає із множиною $\tilde{K}$.

$$\text{Отже, } \bar{K} = \left\{ \left\{ \frac{a}{x} \right\} \mid a, x \in K, x \neq 0 \right\}.$$

II. Доведемо, що множина $\bar{K}$ утворює поле. Для цього треба ввести в множині $\bar{K}$ операції додавання і множення. Введемо їх так:

$$\forall \left\{ \frac{a}{x} \right\}, \left\{ \frac{b}{y} \right\} \in \bar{K} : \left\{ \frac{a}{x} \right\} + \left\{ \frac{b}{y} \right\} = \left\{ \frac{ay + bx}{xy} \right\}, \left\{ \frac{a}{x} \right\} * \left\{ \frac{b}{y} \right\} = \left\{ \frac{ab}{xy} \right\}.$$

Ці означення коректні, бо кільце K є областю цілісності і тому із нерівностей $xy \neq 0$ випливає, що $x \neq 0$. Покажемо, що так введені операції є однозначними, тобто, що сума і добуток класів $\left\{ \frac{a}{x} \right\}$ і $\left\{ \frac{b}{y} \right\}$ не залежить від вибору представників класів. Інакше кажучи, що коли

$$\frac{a_1}{x_1} = \frac{a}{x}, \frac{b_1}{y_1} = \frac{b}{y}, \quad (3)$$

то

$$\left\{ \frac{a_1}{x_1} \right\} + \left\{ \frac{b_1}{y_1} \right\} = \left\{ \frac{a}{x} \right\} + \left\{ \frac{b}{y} \right\}, \left\{ \frac{a_1}{x_1} \right\} * \left\{ \frac{b_1}{y_1} \right\} = \left\{ \frac{a}{x} \right\} * \left\{ \frac{b}{y} \right\}. \quad (4)$$

Рівність (3) означає, що

$$a_1x = ax_1, b_1y = by_1. \quad (5)$$

Щоб довести рівності (4), треба довести рівності:

$$\frac{a_1y_1 + b_1x_1}{x_1y_1} = \frac{ay + bx}{xy}, \frac{a_1b_1}{x_1y_1} = \frac{ab}{xy},$$

а для цього треба показати справедливість рівностей:

$$(a_1y_1 + b_1x_1)xy = (ay + bx)x_1y_1, (a_1b_1)(xy) = (ab)(x_1y_1),$$

які в силу дистрибутивності і асоціативності рівносильні рівностям:

$$a_1y_1xy + b_1x_1x = aux_1y_1 + bxx_1y_1, a_1b_1xy = abx_1y_1.$$

Якщо врахувати, що в кільці K множення комутативне, асоціативне і дистрибутивне, то перша з останніх рівностей одержується із вірних рівностей (5) домноженням першої з них на xy_1 , другої – на xx_1 і наступним додаванням одержаних рівностей, а друга – почленним перемноження рівностей (5). Цим справедливість рівностей (4) доведена.

Таким чином, які б не брали дробі із класів $\left\{ \frac{a}{x} \right\}$ і $\left\{ \frac{b}{y} \right\}$ сума і добуток цих класів залишаються незмінними.

Приступимо до перевірки виконання аксіом поля в множині $\bar{K}$. Справедливість асоціативності, комутативності, додавання і множення та дистрибутивність множення відносно додавання в множині $\bar{K}$ безпосередньо випливає із справедливості цих властивостей в кільці K . Перевіримо, наприклад, дистрибутивність множення відносно додавання:

$$\left\{\frac{a}{x}\right\}\left(\left\{\frac{b}{y}\right\}+\left\{\frac{c}{z}\right\}\right)=\left\{\frac{a}{x}\right\}\left\{\frac{bx+cy}{yz}\right\}=\left\{\frac{a(bx+cy)}{xyz}\right\}=\left\{\frac{abx+acy}{xyz}\right\},$$

$$\left\{\frac{a}{x}\right\}\left\{\frac{b}{y}\right\}+\left\{\frac{a}{x}\right\}\left\{\frac{c}{z}\right\}=\left\{\frac{ab}{xy}\right\}+\left\{\frac{ac}{xz}\right\}=\left\{\frac{abxz+acxy}{x^2yz}\right\}=\left\{\frac{abx+acy}{xyz}\right\},$$

звідки внаслідок рівності правих частин одержуємо:

$$\left\{\frac{a}{x}\right\}\left(\left\{\frac{b}{y}\right\}+\left\{\frac{c}{z}\right\}\right)=\left\{\frac{a}{x}\right\}\left\{\frac{b}{y}\right\}+\left\{\frac{a}{x}\right\}\left\{\frac{c}{z}\right\}.$$

Щоб вказати нульовий елемент в множині $\bar{K}$, зауважимо, що множина всіх дробів виду $\frac{0}{x}$ утворює клас рівних дробів, бо

$$\forall x, y \in K; \quad x, y \neq 0 : \frac{0}{x} = \frac{0}{y}$$

і з рівності $\left(\frac{a}{x} = \frac{0}{y}\right) \Rightarrow a = 0$.

$$\text{Крім того, } \left(\forall \left\{\frac{b}{y}\right\}\right) : \left\{\frac{b}{y}\right\} + \left\{\frac{0}{x}\right\} = \left\{\frac{bx}{yx}\right\} = \left\{\frac{b}{y}\right\}.$$

Отже, нулевим елементом в множині $\bar{K}$ є клас $\left\{\frac{0}{x}\right\}$. Протилежним

елементом класу $\left\{\frac{a}{x}\right\}$ є клас $\left\{\frac{-a}{x}\right\}$:

$$\left\{\frac{a}{x}\right\} + \left\{\frac{-a}{x}\right\} = \left\{\frac{ax + (-a)x}{x^2}\right\} = \left\{\frac{ax + (-ax)}{x^2}\right\} = \left\{\frac{0}{x^2}\right\} = \left\{\frac{0}{x}\right\}.$$

Роль одиниці в множині K відіграє клас $\left\{\frac{x}{x} \mid x \neq 0\right\}$, який складається із усіх дробів з однаковими ненулевими чисельниками і знаменниками. Справді,

$$\forall \left\{ \frac{b}{y} \right\} \in \bar{K} : \left\{ \frac{b}{y} \right\} \cdot \left\{ \frac{x}{x} \right\} = \left\{ \frac{bx}{yx} \right\} = \left\{ \frac{b}{y} \right\}.$$

Залишається тільки помітити, що множина $\left\{ \frac{x}{x} \right\}$ всіх дробів з рівними чисельниками і знаменниками справді утворює клас рівних дробів. Цей факт є наслідком того, що завжди $\frac{x}{x} = \frac{y}{y}$ і завжди з рівності $\frac{b}{y} = \frac{x}{x}$ випливає $bx = xy$, тобто, $b = y$. Якщо клас $\left\{ \frac{a}{x} \right\}$ є ненулевим, тобто, $a \neq 0$, то оберненим до цього класу є клас $\left\{ \frac{x}{a} \right\}$, що містить дріб $\frac{x}{a}$:

$$\left\{ \frac{a}{x} \right\} \cdot \left\{ \frac{x}{a} \right\} = \left\{ \frac{ax}{xa} \right\} = \left\{ \frac{x}{x} \right\}.$$

Таким чином, множина $\bar{K}$ задовольняє всім аксіомам з означення поля $\bar{K}'$ і тому вона є полем.

III. Покажемо нарешті, що кільце K ізоморфне підмножині поля $\bar{K}'$ в силу теореми 2.1 ця підмножина буде підкільцем. Вибір цієї підмножини показує нам ситуацію у випадку кільця Z цілих чисел ціле число a завжди дорівнює дробові $\frac{ax}{x}$, де x – довільне ненулеве ціле число. Якщо у випадку довільного кільця виявиться, що множини дробів $\frac{ax}{x}$, де a – фіксований елемент кільця K і x пробігає всю множину $K \setminus \{0\}$ є класами рівних дробів, то можна сподіватися, що поставивши у відповідність елементу $a \in K$ клас $\left\{ \frac{ax}{x} \right\}$, одержимо ізоморфне відображення кільця K на множину таких дробів.

Множина всіх дробів виду $\frac{ax}{x}$, де a – фіксований елемент кільця K і x пробігає $K \setminus \{0\}$ утворює клас рівних дробів, бо

$$\forall x, y \in K \setminus \{0\} : \frac{ax}{x} = \frac{ay}{y}$$

і з рівності $\frac{b}{y} = \frac{ax}{x}$ виходить, що $bx = ax$, тобто $b = a$.

Задамо відображення $f: K \rightarrow \bar{K}$ таким способом:

$$\forall a \in K: f(a) = \left\{ \frac{ax}{x} \right\}.$$

Відображення f є бієктивним відображенням кільця K на підмножину

$$\tilde{K}_0 = \left\{ \left\{ \frac{ax}{x} \right\} \mid a \in K \right\}: \forall a_1, a_2 \in K: (a_1 \neq a_2) \Rightarrow f(a_1) = \left\{ \frac{a_1x}{x} \right\} \neq f(a_2) = \left\{ \frac{a_2y}{y} \right\},$$

бо якби $\frac{a_1x}{x} = \frac{a_2y}{y}$, то $a_1xy = a_2yx$, звідси внаслідок того, що в K немає дільників нуля, на підставі властивості 11° §1 випливатиме $a_1 = a_2$, всупереч умові.

б) відповідно до означення відображення f

$$\forall \left\{ \frac{ax}{x} \right\}, \exists a \in K: f(a) = \left\{ \frac{ax}{x} \right\}.$$

Відображення f гомоморфне:

$$a_1, a_2 \in K: f(a_1 + a_2) = \left\{ \frac{(a_1 + a_2)x}{x} \right\} = \left\{ \frac{a_1x + a_2x}{x} \right\} = \left\{ \frac{a_1x}{x} \right\} + \left\{ \frac{a_2x}{x} \right\} = f(a_1) + f(a_2),$$

$$f(a_1, a_2) = \left\{ \frac{(a_1, a_2)x}{x} \right\} = \left\{ \frac{a_1x(a_2x)}{x} \right\} = \left\{ \frac{a_1x}{x} \right\} * \left\{ \frac{a_2x}{x} \right\} = f(a_1) * f(a_2).$$

Отже, відображення f є ізоморфним відображенням кільця K на підкільце $\tilde{K}_0$ кільця $\tilde{K}$ (множина $\tilde{K}_0$ є підкільцем кільця $\tilde{K}$ на підставі теореми 2.1 і того очевидного факту, що сума і добуток елементів із $\tilde{K}_0$ знову належать $\tilde{K}_0$). Цим доведено, що область цілісності K ізоморфно вкладається в поле $\bar{K}$.

В алгебрі побудована при доведенні теореми 2.3 поле $\bar{K}$ називають полем дробів або полем часток області цілісності K .

§2.5. ОЗНАЧЕННЯ ІДЕАЛУ КІЛЬЦЯ, ПРИКЛАДИ ІДЕАЛІВ

Серед усіх підмножин кільця K особливу роль відіграють ті, які містять усі різниці своїх елементів та усі добутки своїх елементів з довільними елементами кільця. Такі підмножини кільця називаються його ідеалами.

Означення 18. Підмножина I кільця K називається його ідеалом, якщо

- 1) $(\forall a, b \in I): a - b \in I;$
- 2) $(\forall a \in I)(\forall k \in K): ak, ka \in I.$

Теорема 2.4. Всякий ідеал I кільця K є підкільцем цього кільця.

Доведення. За означенням ідеалу

$$(\forall a \in I): a - a = 0 \in I,$$

тобто нуль кільця K належить ідеалу I .

Тоді $(\forall a \in I): (-a) = 0 - a \in I$ і, значить, $(\forall a, b \in I): a + b = a - (-b) \in I$, тобто, сума будь-яких двох елементів з I належить I . За другою умовою з означення ідеалу $(\forall a, b \in I): ab \in I$.

Отже,

- 1) $(\forall a, b \in I): a + b, ab \in I;$
- 2) $(\forall a \in I): (-a) \in I,$

а виконання цих умов достатнє для того, щоб підмножина кільця була підкільцем. Таким чином, I – підкільце кільця K .

Оскільки операція множення не в кожному кільці комутативна, то часто доводиться розглядати односторонні ідеали – лівосторонні, якщо

- 1) $(\forall a, b \in I): a - b \in I;$
- 2) $(\forall a \in I)(\forall k \in K): ka \in I$

та правосторонні, якщо

- 1) $(\forall a, b \in I): a - b \in I;$
- 2) $\forall a \in I(\forall k \in K): ak \in I.$

Через це ідеали в розумінні означення 18 називають двосторонніми.

Приклади:

1. Множина всіх цілих чисел, кратних натуральному числу n , є ідеалом кільця Z цілих чисел.

2. Сукупність усіх квадратних матриць n -го порядку, в яких останній стовпець складається з нулів, утворює лівосторонній ідеал в кільці M_n квадратних матриць n -го порядку над числовим полем P .

Виділимо деякі типи ідеалів комутативного кільця K з одиницею.

1^о Підмножина $O = \{0\}$ кільця K , яка складається тільки з одного нуля, є ідеалом, так званим нульовим ідеалом. Все кільце K теж є ідеалом самого себе і називається одиничним ідеалом.

Ці ідеали називаються тривіальними ідеалами кільця K .

2^о Якщо a – деякий елемент K , то множина $(a) = \{ak \mid k \in K\}$ є ідеалом кільця K , яким називається головним ідеалом кільця K , породженим елементом a .

Доведення очевидне.

3^о Нехай, $a_1, a_2, \dots, a_n$ деякі елементи кільця K . Тоді множина $I = \{x_1a_1 + x_2a_2 + \dots + x_na_n \mid x_1x_2\dots x_n \in K\}$ є ідеалом.

Справді, операція додавання в кільці комутативна, асоціативна, зв'язана з множенням, дистрибутивним законом та, крім того,

$$-(a+b) = -a-b \text{ і } a+b = a+(-b),$$

тому

$$\begin{aligned} 1) & (x_1a_1 + x_2a_2 + \dots + x_na_n) / x_1x_2\dots x_n - (x'_1a_1 + x'_2a_2 + \dots + x'_na_n) = x_1a_1 + \\ & + x_2a_2 + \dots + x_na_n / x_1x_2\dots x_n + (-x'_1a_1) + (-x'_2a_2) + \dots + (-x'_na_n) = [x_1a_1 + (-x'_1a_1)] + \\ & + [x_2a_2 + (-x'_2a_2)] + \dots + [x_na_n + (-x'_na_n)] = (x_1 - x'_1)a_1 + \dots + (x_n - x'_n)a_n \in I. \end{aligned}$$

$$2) \forall k \in K: k(x_1a_1 + x_2a_2 + \dots + x_na_n) = (kx_1)a_1 + \dots + (kx_n)a_n \in I.$$

Отже, I задовольняє обом умовам з означення ідеалу I , значить, є ідеалом.

Цей ідеал називається ідеалом, породженим елементами $a_1, a_2, \dots, a_n$

4) $I_1, I_2, \dots, I_n$ – деякі ідеали кільця K . Тоді множина

$I = \{a_1 + a_2 + \dots + a_n \mid a_k \in I_k, k = 1, 2, \dots, n\}$ утворює ідеал, який називається сумою ідеалів $I_1, I_2, \dots, I_n$.

Доведення аналогічне до 3).

5) Якщо I_1, I_2 – ідеали кільця K , то їх перетин – теж ідеал.

Дійсно, якщо $a_1, a_2 \in I_1 \cap I_2$, то $a_1, a_2 \in I_1 \mid a_1, a_2 \in I_2$. Оскільки I_1, I_2 – ідеали, то $a_1, a_2 \in I_1 \mid a_1, a_2 \in I_2$. Тому $a_1, a_2 \in I_1 \cap I_2$. Аналогічно перевіряється друга умова з означення ідеалу.

6) Нехай $f: K \rightarrow K'$ – гомоморфізм з кільця K в кільце K' . Тому його ядро $\text{Ker} f$ є ідеалом кільця K .

Справді, якщо $a, b \in \text{Ker} f$ то $f(a) = f(b) = 0$ і тому

$$f(a - b) = f(a) - f(b) = 0,$$

$$\forall k \in K: f(ka) = f(k) \cdot f(a) = f(k) \cdot 0 = 0,$$

тобто $a - b, ka \in \text{Ker} f$.

Кільце K , в якому не існує нетривіальних двосторонніх ідеалів називається простим.

Приклади:

1) Кільце M_n всіх матриць n -го порядку над полем є простим.

Щоб довести це, треба показати, що коли I – деякий ненульовий ідеал кільця $M_n = I$. Оскільки $I \subset M_n$, то залишається довести, що всяка матриця із M_n належить I . Внаслідок того, що всяку матрицю n -го порядку можна подати у вигляді суми n^2 матриць, в яких хіба що тільки один елемент не дорівнює 0, і всякий ідеал є підкільцем, тобто, разом із скінченною кількістю своїх елементів містить і їх суму, для доведення включення досить показати, що ідеалу I належать всі матриці із M_n , в яких тільки один елемент не дорівнює 0.

Отже, нехай A – деяка матриця n -го порядку, в якій всі елементи, крім a_1 , дорівнюють 0, а $G_H = a \neq 0$. Оскільки $I \neq \{0\}$, то в I існує матриця $B \neq 0$, в котрій деякий елемент $B_H \neq 0$. Розглянемо матрицю A_1 , в якій всі елементи, крім G''_{ft} , дорівнюють теж 0, а елементи a'_{1k} і a_{ft} підібрані так, що

$$G'_{jk} \cdot G''_{ft} = \frac{\infty}{\beta}$$

Легко бачити, що тоді $k(A = A_1B / A_2$ В силу другої умови з означення ідеалу $A_1B \in I$ і $(A_1B)A_2 \in I$. Тому матриця $A \in I$. Як вже відзначалося, з цього виходить, що $M_n \in I$.

2) Всяке поле P є простим кільцем.

Справді, нехай $I \neq \{0\}$ – довільний ідеал поля P і $a \neq 0$ – довільний його елемент. Тоді існує $a^{-1} \in P$. і згідно з другою властивістю з означення ідеалу:

Звідси на підставі цієї ж другої умови

$$(\forall a \in P): G \cdot I = a \in P$$

тобто $P \subset I$ і, значить, $P = I$.

Відсутність нетривіальних ідеалів – характерна властивість полів.

§2.6. КІЛЬЦЯ ГОЛОВНИХ ІДЕАЛІВ ТА ЕВКЛІДОВІ КІЛЬЦЯ

Означення 19. Область цілісності K з 1, кожен ідеал якої є головним називається кільцем головних ідеалів.

Приклад. Кільце Z цілих чисел є кільцем головних ідеалів. Дійсно, нехай I – довільний ідеал кільця Z . Якщо $I = \{0\}$ то $I = (0)$. Тому вважаємо, що $I \neq 0$. Тоді $\exists m \in I: m \neq 0$.

Внаслідок того, що I – підкільце, то $I^{-m} \in I$. Це означає, в кожному ідеалі є натуральне число. Нехай m_0 – найменше з усіх натуральних чисел ідеалу I . За теоремою про ділення з остачею

$$(\forall a \in I)(\exists q, r \in Z): a = m_0q + r, \quad 0 \leq r < m_0,$$

Згідно з другою умовою з означення ідеалу $m_0q \in I$, а згідно з першою $Z = a = m_0q \in I$. Це означає, що коли було б $I \neq 0$ то в I існувало б натуральне число r , менше за m_0 . Тому $r = 0$ і, отже, $a = m_0q$. Таким чином,

$$(\forall a \in I)(\exists q \in Z): a = m_0q,$$

тобто ідеал I – головний, $I = (m_0)$.

Означення 20. Область цілісності K з 1 називається евклідовим кільцем, якщо всякому її елементу $a \neq 0$ поставлено у відповідність натуральне число n_a так, що

$$(\forall a \in K), (\forall b \in K, b \neq 0) (\exists q, r \in K): a = bq + r,$$

причому $(r = 0) \vee (n_2 < n_0)$.

Приклад. Кільце Z цілих чисел є евклідовим кільцем.

Справді, за теоремою про ділення з остачею

$$(\forall a \in Z) (\forall b \in Z, b > 0) (\exists q, r \in Z): a = bq + r, 0 \leq r_1 < b \quad (1)$$

якщо $b < 0$ то $|b| > 0$ і значить,

$$\exists q, r \in Z: a = |b|q_1 + r_1, 0 \leq q_1 < |b|.$$

Останні співвідношення можна переписати так:

$$a = (-b)q_1 + r_1, 0 \leq q_1 < |b| \quad (2)$$

Із формул (1) і (2) виходить:

$$(\forall a \in Z) (\forall b \in Z, b \neq 0) (\exists q, r \in Z): G = bq + r, 0 \leq r < b.$$

Це означає, що коли кожному ненульовому цілому числу a поставити у відповідність його абсолютну величину, тобто покласти n_a , то кільце Z стає евклідовим кільцем.

Теорема 2.5. Всяке евклідове кільце є кільцем головних ідеалів.

Доведення. Треба довести, що всякий ідеал I є головним, якщо $I = \{0\}$, то I – головний ідеал, породжений нулем. Якщо $I \neq \{0\}$, то кожному його ненульовому елементові a поставлено у відповідність натуральне число n_a , тобто ідеал I співвіднесений з підмножиною $\lambda_i = \{n_a | a \in I\}$ множини натуральних чисел. В λ_i є найменше число n_{a_0} . Інакше кажучи, в I існує елемент $a_0 \neq 0$ такий, що

$$\forall a \in I, a \neq 0: n_{a_0} \leq n_a.$$

Очевидно, що $(a_0) \subset I$. Покажемо: що і навпаки $I \subset (a_0)$, звідси випливатиме потрібна рівність $I = (a_0)$.

За означенням евклідового кільця

$$(\forall a \in I)(\exists q, r \in K): a \neq 0 : a = I \subset a_0 q + q_1 (q = 0) \cup (n_r \leq n_{a_0}).$$

На підставі другої умови з означення ідеалу $a_0 q \in I$, а на підставі першої – елемент $r = a - a_0 q \in I$. Якби $r \neq 0$, то $n_r < n_{a_0}$, що суперечить вибору елемента a_0 . Тому $r = 0$ і, значить, $a = a_0 q$, тобто, $I \subset (a_0)$. **Теорема доведена.**

§2.7. ПОДІЛЬНІСТЬ В ОБЛАСТЯХ ЦІЛІСНОСТІ З ОДИНИЦЕЮ

На області цілісності з одиницею вдається розповсюдити багато відомих ефектів теорії подільності в кільці цілих чисел.

Нехай K – область цілісності з 1. Говорять, що елемент $a \in K$ ділиться на елемент $b \in K$, $b \neq 0$, якщо

$$\exists c \in K : a = bc; 0.$$

Елемент b називають дільником a і записують a/b . Якщо $ab = 1$ то елементи $a, b \in K$ називаються дільниками 1 кільця K . З рівності $ab = 1$ виходить, що a і b взаємно обернені. Отже, кожен дільник одиниці має обернений елемент. Навпаки, якщо для елемента $a \in K$ існує обернений елемент a^{-1} , та $aa^{-1} = 1$ і, значить, a – дільник одиниці. В множині цілих чисел дільниками 1 є числа 1 і -1: $(1 \times 1) = (-1) \times (-1) = 1$.

Зауважимо, що сукупність усіх дільників 1 утворює мультиплікативну групу. Цю групу дільників називають мультиплікативною групою кільця K .

Справді, якщо ε_1 і ε_2 деякі дільники 1, то $(\exists \varepsilon_1^{-1}, \varepsilon_2^{-1}) : \varepsilon_1 \varepsilon_1^{-1} = \varepsilon_2 \varepsilon_2^{-1} = 1$. Тоді $(\varepsilon_1 \varepsilon_2)(\varepsilon_1^{-1} \varepsilon_2^{-1}) = (\varepsilon_1 \varepsilon_1^{-1})(\varepsilon_2 \varepsilon_2^{-1}) = 1 * 1 = 1$ тобто, $\varepsilon_1 \varepsilon_2$ – дільник 1.

Виконання аксіом групи очевидне. Відзначимо, що всякий дільник ε одиниці є дільником довільного елемента $a \in K$, бо

$$a = a \cdot 1 = a(\varepsilon \varepsilon^{-1}) = \varepsilon(a \varepsilon^{-1}).$$

Елементи $a, b \in K$ називається асоційовними, якщо a є дільником b і b – дільником a , тобто, якщо

$$\exists c, d \in K : (a = bc) \cap (b = ad).$$

З цих рівностей виходить, що $a = a(dc)i$. Значить $dc = 1$, тобто d і c – дільники 1. Таким чином, асоційовні елементи відрізняються тільки дільниками 1.

Елементи $a \neq 0$ і з кільця K називається незвідним, якщо він не є дільником 1, і якщо із рівності $a = bc$ ($b, c \in K$) випливає, що b або c – дільники 1. Як бачимо, незвідний елемент, дільниками якого, попри дільників 1, є тільки елементи, асоційовні з ним. В кільці цілих чисел дільниками 1 є тільки 1, -1 , тому незвідні елементи – це числа, що діляться тільки на себе і на ± 1 , тобто, це прості числа і ті від’ємні, абсолютні величини яких прості.

Елемент $d \in K$ називається найбільшим спільним дільником елементів $a, b \in K$, $d = (a, b)$, якщо

$$1. a : d, b : d.$$

$$2. \forall d \in K : (d / a \cap d / b) \rightarrow (\varepsilon / d).$$

Теорема 2.6. Для всяких одночасно не рівних нулю елементів a, b із кільця K головних ідеалів існує їх найбільший спільний дільник $d \in K$, який належить ідеалу, породженому елементами a і b , тобто,

$$\exists x_0, y_0 \in K : d = ax_0 + by_0$$

Доведення. Розглянемо ідеал $I = \{ax + by \mid x, y \in K\}$ породжений елементами a і b . Оскільки кожен ідеал в K є головним, то існує елемент $d \in I$ такий, що $I = (d)$. Породжуючий елемент d цього ідеалу I є дільником всякого його елемента.

Відзначимо, що найбільший спільний дільник елементів $a, b \in K$ визначається неоднозначно: якщо $d = (a, b)$, то $\varepsilon d = (a, b)$, де ε – довільний дільник одиниці.

Теорема 2.7. Якщо p – незвідний елемент кільця головних ідеалів K і елементів a, b , $K \nmid p$, то p / ab , то p / a або p / b .

Доведення. Нехай p не є дільником a , і нехай $d = (a, p)$. Покажемо, що d – дільник 1. Справді, якщо d не був дільником 1, то внаслідок незвідності елемента p подільності $p : d$ ми мали б: $p = \varepsilon d$, де ε – деякий дільник 1.

Тоді $d = p\varepsilon^{-1}$ і, в силу подільності $a:d$, $a = p(\varepsilon^{-1}, c)$ ($c \in K$), що суперечить припущенню $a \nmid p$. Отже, d – дільник 1. $d = \varepsilon$.

Оскільки $\varepsilon = (a, p)$, то за теоремою 2.6

$$(\exists x_0, y_0 \in K): \varepsilon = ax_0 + py_0.$$

Помножимо цю рівність на b , матимемо

$$\varepsilon q = (ab)x_0 + p(y_0b).$$

Оскільки за умовою $ab \mid p$, то обидва доданки правої частини діляться на p і, значить, $\varepsilon b \mid p$, тобто $\exists q \in K: \varepsilon b = pq$ або інакше $b = p(\varepsilon^{-1}q)$, що означає $b \mid p$.

Таким чином, якщо $ab \mid p$ і один з співмножників не ділиться на p , то другий обов'язково ділиться на p .

Елементи $p_1, p_2, \dots, p_n$ такі, що

$$a = \varepsilon p_1 p_2 \dots p_n \quad (2)$$

причому в двох таких розкладах

$$a = \varepsilon p_1 p_2 \dots p_n \quad a = \varepsilon' q_1 q_2 \dots q_r$$

$r = 1$ та існують такі дільники одиниці $\varepsilon_1 \varepsilon_2 \dots \varepsilon_r$, що можливо після перестановки індексів, $p_i = \varepsilon_i q_i$ ($i = 1, 2, \dots, r$).

Лема 2.1. В кільці K головних ідеалів не існує нескінченного строго зростаючого ланцюжка ідеалів.

$$(a_1) \subset (a_2) \subset \dots \subset (a_n) \subset \dots \quad (3)$$

Доведення. Нехай ми маємо деяку строго зростаючий ланцюжок ідеалів (3) і $I = \bigcup_i (a_i)$ – об'єднання всіх ідеалів цього ланцюжка.

Пересвідчимося в тому, що множина I є ідеалом.

Виконання першої умови з означення ідеалу випливає з того, що коли $a, b \in I$, тобто

$$a, b \in \bigcup_i (a_i), \text{ то } (\exists n, m): (a \in (a_n)) \cap (b \in (a_m)),$$

Нехай для означеності $n \leq m$. Тоді $(a_n) \subset (a_m)$ і, значить, $a, b \in (a_m)$. Оскільки (a_m) – ідеал, то $a - b \in (a_m)$, внаслідок чого $a - b \in \bigcup_i (a_i) = I$. Якщо, крім того, $k \in I$, то $ak \in (a_n)$ тобто, виконується і друга умова з означення ідеалу.

Оскільки в кільці K кожен ідеал головний, то $(\exists c \in I): I = (c)$. Породжуючий елемент c ідеалу I належить $I = \bigcup_i (a_i)$ і, значить, в котромусь з ідеалів a_i , $c \in (a_1)$. Тоді $I = (c) \subset (a_1)$, але і I – об'єднання всіх ідеалів (a_i) , тому $(a_1) \subset I$. Із включень $I \subset (a_1)$ і $(a_1) \subset I$ виходить, що $I = (a_1)$, це і означає, що (a_1) – останній ідеал ланцюжка (3), чим лема доведена.

Лема 2.2. Головні ідеали (a) і (b) кільця K тоді і тільки тоді співпадають коли (a) і (b) асоційовані.

Доведення. Якщо $(a) = (b)$, то $a \in (b)$, $b \in (a)$, внаслідок чого $\exists k_1, k_2 \in Z: a = bk_1, b = ak_2$, що і означає асоційованість елементів a і b .

Навпаки, нехай елементи a і b асоційовані, тобто $a = b\varepsilon$, де ε – дільник 1. Тоді $\forall a_1 \in (a): (\exists k \in K): a = ak_1$.

Значить, $a_1 = b(\varepsilon k_1)$, внаслідок чого $a_1 \in (b)$. Звідси виходить, що $(a) \subset (b)$. Аналогічно $(b) \subset (a)$. Таким чином, $(a) = (b)$.

Будемо допускати, що в розкладі (2) індекс r приймати і значення 0. Тим самим домовимося вважати, що всякий дільник I на розкладі не незвідний елемент.

Теорема 2.8. (Основна теорема теорії кілець головних ідеалів). Всякий не нульовий елемент кільця K головних ідеалів допускає одночасний розклад на незвідні елементи.

Доведення.

I. Доведемо спочатку, що для кожного елемента із кільця K існує розклад на незвідні елементи, тобто, що кожен елемент із K можна подати у вигляді (2).

Нехай $a \neq 0$ – довільний елемент із K . Оскільки деякий дільник 1 є дільником і елемента a , то a завжди можна подати у вигляді

$$a = bc \quad (bc \in K). \quad (4)$$

Якщо із цього подання виходить, що b або c дільники I , то a є або дільником I або незвідним елементом і подання (4) треба розглядати як розклад елемента a на незвідні елементи.

Якщо у формулі (4) b і c – не дільники I , то до них можна застосувати ті ж міркування, які були застосовані до a . В результаті одержимо

$$b = b_1 b_2, c = c_1 c_2 \quad (b_1, b_2, c_1, c_2 \in K)$$

і, значить,

$$a = b_1 b_2 c_1 c_2.$$

Можливі два випадки: 1) кожен з множників b_1, b_2, c_1, c_2 є або, дільником I або незвідним елементом; 2) серед елементів b_1, b_2, c_1, c_2 принаймні один не є ні дільником I , ні незвідним елементом. В першому випадку для елемента a справедливий розклад (2), в другому – наші міркування треба застосувати до тих із елементів b_1, b_2, c_1, c_2 які не є ні дільниками I ні незвідними елементами.

Міркуючи таким способом далі, після певного числа кроків дістанемо

$$a = \varepsilon a_1 a_2 \dots a_n, \quad (5)$$

де ε – дільник I і $a_1, a_2, \dots, a_n$, – не дільники I запровадимо позначення $a_1' = a_2 \dots a_n, a_2' = a_3 \dots a_n, a_{n-1}' = a_n$.

$$\text{Тоді } a = (\varepsilon a_1) a_1' a_1' = a_2 a_2' a_2' = a_{n-1} a_{n-1}.$$

Внаслідок чого справедливе включення

$$(a) \subset (a_1') \subset (a_2') \subset \dots \subset (a_{n-1}'). \quad (6)$$

Які згідно з лемою 2.2 є строгими, бо породжуючі елементи цих ідеалів неасоційовані. Якщо в представленні (5) всі елементи $a_1, a_2, \dots, a_n$ – незвідні, то це означає. Що для a справедливий розклад /2/. Якщо ж декотрі із цих елементів не є незвідними, то процес міркування треба продовжити. Однак, цей процес може бути нескінченним, тому що тоді строго зростаючий ланцюг /6/ головних ідеалів був би теж нескінченним, що на підставі леми неможливо.

Отже, процес наших міркувань скінченний і після скінченного числа кроків одержимо для елемента a розклад /2/.

II. Доведемо тепер, що розклад кожного елемента $a \in K$ є однозначним.

Припустимо, що деякий елемент $a \in K$ має два розклади:

$$A = \xi p_1 p_2 \dots p_r, a = \xi' q_1 q_2 \dots q_j.$$

На незвідні множники. Тоді

$$\xi p_1 p_2 \dots p_r = \xi' q_1 q_2 \dots q_j.$$

Або інакше

$$(\xi')^{-1} \xi p_1 p_2 \dots p_r = q_1 q_2 \dots q_j. \quad (7)$$

Ліва частина цієї рівності ділиться на p_1 , тому і права $q_1 q_2 \dots q_r$ ділиться на p_1 . Оскільки p_1 незвідний елемент, то за теоремою 2.7, яку по індукції можна поширити на довільне скінченне число співмножників, котрийсь із елементів $q_1 q_2 \dots q_j$ ділиться на p_1 . Пронумерувати в разі потреби елементи $q_1 q_2 \dots q_j$ доб'ємося того, що q_1 і p_1 . Оскільки q_1 і p_1 – незвідні елементи, то існує дільник одиниці ξ_1 такий що, $q_1 = \xi_1 p_1$.

Підставивши одержаний вираз замість q_1 у формулу (7) і скоротивши на p_1 (на недільники нуля скорочувати можна), матимемо

$$\xi_1^{-1} (\xi')^{-1} \xi p_1 p_2 \dots p_r = q_1 q_2 \dots q_j.$$

ліва частина цієї рівності ділиться на p_2 . Тоді на p_2 ділиться і права. Провівши ті ж міркування, які були застосовані вище, матимемо

$$q_2 = \xi_2 p_2, \xi_2^{-1} \xi_1^{-1} (\xi')^{-1} \xi p_3 \dots p_r = q_3 \dots q_j.$$

якби було $r > 1$ то після r кроків мали б

$$\xi_2^{-1} \dots \xi_1^{-1} (\xi')^{-1} \xi = q_{r+1} \dots q_j,$$

або інакше $I = \xi' \xi' \xi_1 \dots \xi_r q_{r+1} \dots q_j$.

Ця рівність означає, що незвідні елементи $q_{r+1} \dots q_j$ є дільники I , а це суперечить їх незвідності. Отже $r > I$. лема логічно показує, що нерівність $I > r$ теж неможлива. Таким чином $I = r$ і справедливі одержані в процесі доведення рівності $q_1 = \xi_1 p_1, q_2 = \xi_2 p_2, \dots, q_r = \xi_r p_r$. **Теорема доведена.**

На закінчення даної теми відзначимо, що в області цілісності з I , яка не є кільцем головних ідеалів, розклад на незвідні елементи може бути неоднозначним.

Наведемо приклад. Легко перевірити, що сукупність $z(\sqrt{-3})$ комплексних чисел виду $a + b\sqrt{-3}$ і, де a і b – довільні цілі числа, є областю цілісності з 1. Покажемо, що кожен елемент $z \neq 0$ цього кільця має розклад на незвідні елементи, який може бути і неоднозначним.

З цією метою у відповідність кожному числу $z = a + b\sqrt{-3}$ і $z \in z(\sqrt{-3})$, поставимо ціле невід'ємне число $N(z) = a^2 + 3b^2$, яке назвемо нормою числа z . Елементарно показується, що

$$(\forall z, z_1, z_2 \in z(\sqrt{-3})): (z = z_1 z_2) \Rightarrow N(z) = (N(z_1) N(z_2)).$$

(Показати самостійно!). Зокрема, якщо $1 = z_1 z_2 (z_1, z_2 \in z(\sqrt{-3}))$, $N(1) = N(z_1)N(z_2)$. Оскільки $N(1) = N(1 + 0\sqrt{-3}) = 1$, $N(z_1) = N(z_2) = 1$. Якщо $z_1 = a_1 + b_{11}\sqrt{-3}$, то $a_1^2 + 3b_1^2 = 1$, звідки $a_1 = \pm 1$, $b_1 = 0$. Таким чином, дільниками $1 \in z(\sqrt{-3})$ є тільки числа 1 і -1 .

Можливість розкладу числа $z \in z(\sqrt{-3})$, $z \neq 0$ доведемо методом математичної індукції по нормі $N(z)$ і якщо $z \neq 0$, то $N(z) > 0$.

При $N(z) = 1$, як показано вище, $z = \pm 1$, а за домовленістю дільники 1 мають розклади на незвідні. Припустимо, що твердження вірне для всіх чисел з нормою меншою від m , тобто припустимо, що всі числа при z , для яких $N(z) < m$, мають розклади на незвідні числа із $z(\sqrt{-3})$. Нехай z – довільне число із $z(\sqrt{-3})$, норма якого $N(z) = m$. Число z завжди можна подати у вигляді

$$z = z_1 z_2 (z_1, z_2 \in z(\sqrt{-3})). \quad (8)$$

Якщо із цього подання випливає, що z_1 або z_2 – дільники 1, то за означенням z – незвідний елемент і він має тривіальний розклад на незвідні множники: $z = \varepsilon z$ ($\varepsilon = 1$). Якщо ні z_1 ні z_2 – не дільники 1, тобто $z_1, z_2 = \pm 1$, то $N(z_1), N(z_2) \neq 1$ із представлення $N(z) = N(z_1)N(z_2)$ випливає, що $N(z_1) < m$ і $N(z_2) < m$. Тоді за індуктивним припущенням z_1 і z_2 можна розкласти на незвідні множники. Підставивши ці розклади у формулу /8/, одержимо розклад і для елемента z .

Таким чином, кожен елемент із кільця $z(\sqrt{-3})$ має розклад на незвідні числа, але не для деякого числа із цього кільця цей розклад однозначний. Наприклад, число $4 \in z(\sqrt{-3})$ має такі розклади:

$$4 = 2 \cdot 2, 4 = (1 + \sqrt{3}i)(1 - \sqrt{3}i). \quad (9)$$

В цих розкладах числа 2, $1 \pm \sqrt{3}i$ і незвідні, бо їх норма дорівнює 2, а 2 не розкладається на нетривіальні множники. Тому і числа 2, $1 \pm \sqrt{3}i$ і не розкладаються на нетривіальні множники. Зрозуміло, що числа 2, $1 + \sqrt{3}i$, $2, 1 - \sqrt{3}i$ і неасоційовані, бо $2 \neq (\pm 1)(\pm \sqrt{3}i)$. Отже, розклади /9/ є різними розкладами числа 4.

§2.8. КОНГРУЕНЦІЇ ТА ФАКТОР КІЛЬЦЯ ЗА ІДЕАЛОМ

Крім алгебраїчних операцій в кільці K можуть бути введені і деякі інші відношення, зокрема, відношення еквівалентності. З алгебраїчної точки зору інтерес представляють тільки такі відношення еквівалентності, які певним способом узгодженні з операціями, означеними в кільці.

Означення 21. Говорять, що відношення еквівалентності $a \sim b$ в комутативному кільці K узгоджено з алгебраїчними операціями цього кільця, якщо:

$$(\forall a, b, c, d \in K): (a \sim b) \wedge (c \sim d) \Rightarrow (a + c \sim b + d) \wedge (ac \sim bd).$$

Прикладом відношення еквівалентності, узгодженого з операціями кільця, служить відношення конгруентності за модулем ідеалу.

Означення 22. Говорять, що елементи a, b комутативного кільця конгруентні між собою, за ідеалом $I \subset K$ і за модулем ідеалу I , якщо $a - b \in I$, і записується це так:

$$a \equiv b \pmod{I}.$$

Теорема 2.9. Відношення конгруентності за ідеалом I кільця K відношенням еквівалентності в K , узгодженим з операціями K .

Доведення. Оскільки кожен ідеал I кільця K є підкільцем, отже, і підгрупою групи цього кільця, то перевірка того, що відношення конгруентності за ідеалом I є відношення еквівалентності. Узгодженим з операцією додавання, приводиться точно так, як і в теорії груп. І тому зараз проводити її не будемо. Покажемо тільки, що коли

$$a \equiv b \pmod{I}, c \equiv d \pmod{I}, \tag{1}$$

то

$$ac \equiv bd \pmod{I} \tag{2}$$

з цією метою розглянемо різницю $ac - bd$

$$ac - bd = (ac - bc) + (bc - bd) = (a - b)c + b(c - d) \tag{3}$$

в силу конгруенції $/1/ a - b, c - d \in I$. тоді за другою умовою з означення ідеалу $(a - b)c, b(c - d) \in I$, внаслідок того, що ідеал є підкільцем $(a - b)c + b(c - d) \in I$, що рівносильна конгруенції (2). **Теорема доведена.**

Виявляється, що відношення конгруентності за ідеалом I вичерпуються усі відношення еквівалентності, узгодженні з операціями кільця. Точніше справедлива теорема 2.10.

Теорема 2.10. Для всякого відношення еквівалентності в кільця K , узгодженого з операціями цього кільця, існує ідеал I такий, що дане відношення еквівалентності є відношення конгруентності за ідеалом I .

Доведення цієї теореми проводити не будемо.

§2.9. ФАКТОР-КІЛЬЦЯ КОМУТАТИВНОГО КІЛЬЦЯ ЗА ІДЕАЛОМ I

Добре відомо, що всяке відношення еквівалентності на множені I породжує розбиття цієї множини на класи, класи еквівалентності. Та відношення конгруентності за модулем ідеалу I в кільці K породжує розбиття кільця K на класи. Ці класи називають суміжними класами або класами елементів. Конгруентних за ідеалом I .

Означення 23. Суміжним класом комутативного кільця K за ідеалом або класу елементів, конгруентних за ідеалом I кільця K називають всякий клас еквівалентності відношенням конгруентності за ідеалом I , тобто. Сукупність C_a усіх елементів кільця K , які конгруентні елементу $a \in K$, і значить конгруентні між собою за ідеалом I .

Як уже відзначалося, кожен ідеал I кільця K є підгрупою адитивної групи кільця K і, значить, відношення конгруентної в кільці K за ідеалом I є відношенням конгруентності в адитивній групі кільця K за підгрупою I , а кожен суміжний клас кільця K за ідеалом I є суміжним класом адитивної групи кільця K за підгрупою I . Тому суміжні класи кільця K за ідеалом I мають таку ж структуру, як і суміжні класи адитивної абелевої групи за підгрупою, тобто, справедлива така теорема.

Теорема 2.11. Всякий суміжний клас C_a комутативного кільця K за ідеалом I можна подати у вигляді $C_a = a + I$, де a – довільний елемент класу C_a . Навпаки, всяка множина $a + I$, де a – довільний елемент кільця K , утворює суміжний клас кільця K за ідеалом I .

Нагадаємо, що за означенням

$$a + I = \{a + I / x \in I\}.$$

Розглянемо сукупність K/I усіх суміжних класів комутативного кільця K за ідеалом I

$$K / I = \{a + I / a \in K\}.$$

Як відомо, у випадку адитивної абелевої групи ця сукупність утворює групу, так звану фактор-групу. У випадку кільця сукупність K/I є кільцем.

Теорема 2.12. Сукупність K/I усіх суміжних класів комутативного кільця K за ідеалом I є комутативним кільцем. Якщо кільце K містить I , то і кільце K/I містить одиницю.

Кільце K/I називають фактор-кільцем кільця K за ідеалом I .

Доведення. Сукупність K/I можна розглядати як сукупність суміжних класів адитивної групи кільця K за підгрупою I , а така сукупність, як відомо з теорії груп, утворює адитивну абелеву групу, фактор-групу групи K за підгрупою I , причому операція додавання задається формулою:

$$(\forall a + I, b + I \in K(I)) : (a + I) + (b + I) = (a + b) + I.$$

Тому для завершення доведення теореми треба тільки ввести у множині K/I операцію множення і перевірити, що вона є асоціативною, комутативною і пов'язана з додаванням дистрибутивним законом.

Операцію множення суміжних класів задамо так:

$$(\forall a + I, b + I \in K(I)) : (a + I)(b + I) = ab + I.$$

Покажемо, що так означене множення є однозначне, тобто, що за формулою у відповідність суміжним класам $a + I$ та $b + I$ ставиться єдиний суміжний клас $ab + I$. Неоднозначність може виникнути за рахунок того, що в поданні суміжного класу у виді $a + I$ елемент a є довільним елементом цього класу. Значить, якщо

$$a_1 \in a + I, b_1 \in b + I, \text{ то } a + I = a_1 + I, b + I = b_1 + I.$$

Тоді $(a_1 + I)(b_1 + I) = a_1 b_1 + I$ і щоб множення було однозначним, має бути справедлива рівність $ab + I = a_1 b_1 + I$.

Доведемо, що це насправді так.

Належності $a_1 \in a + I, b_1 \in b + I$, означають, що

$$(\exists x_1 x_2 \in I): a_1 = a + x_1, b_1 = b + x_2.$$

Тоді $a_1 b_1 = ab + (ax_1 + bx_2 + x_1 x_2) \in ab + I$ звідки виходить, що класи $ab + I$ і $a_1 b_1 + I$ мають спільний елемент $a_1 b_1$, і тому вони співпадають:

$$ab + I = a_1 b_1 + I.$$

Цим однозначність множення доведена.

Асоціативність множення класів випливає із асоціативності множення в K :

$$\begin{aligned} [(a+I)(b+I)](c+I) &= (ab+I)(c+I) = (ab)c+I = \\ &= a(bc)+I = (a+I)(bc+I) = (a+I)[(b+I)(c+I)]. \end{aligned}$$

Аналогічно доводиться комутативність множення класів. Так само аналогічно виводиться дистрибутивність:

$$\begin{aligned} (a+I)[(b+I)+(c+I)] &= (a+I)[(b+c)+I] = a(b+c)+I = \\ &= (ab+ac)+I = (ab+I)+(ac+I) = (a+I)(b+I)+(a+I)(c+I). \end{aligned}$$

Якщо в кільці K є одиниця, то, очевидно клас $1 + I$ – одиниця фактор-кільця K/I .

§2.10. ФАКТОР-КІЛЬЦЯ І ГОМОМОРФІЗМИ

Встановимо зв'язок між поняттям фактор-кільця і поняттям гомоморфізму кільця.

Нехай $f: K \rightarrow K'$ гомоморфізм кільця K в кільці K' . В §3 показано, що ядро $\text{Ker } f$ цього гомоморфізму є ідеалом кільця K . Тому можна говорити про фактор-кільце $K/\text{Ker } f$ кільця K за ядром гомоморфізму f . Як бачимо, кожен гомоморфізм визначає деяке фактор-кільце.

Виявляється, що і навпаки: якщо дано фактор-кільце K/I , поставивши у відповідність кожному елементу $a \in K$ суміжний клас $a + I$. Цей епіморфізм $x: K \rightarrow K/I$, ядром якого служить ідеал I . Цей епіморфізм називається канонічним гомоморфізмом. Гомоморфність так заданого відображення показується так:

$$\forall a, b \in K: x(a) = a + I, x(b) = b + I,$$

Тоді

$$x(a + b) = (a + b) + I = (a + I) + (b + I) = x(a) + x(b),$$

$$x(ab) = ab + I = (a + I)(b + I) = x(a)x(b).$$

Теорема 2.13. (про гомоморфізми) Для всякого епіморфізму $f: K \rightarrow K'$ існує єдиний ізоморфізм $\varphi: K/\text{Ker } f \rightarrow K'$ такий, що $f = \varphi \circ \chi$, де $\chi: K \rightarrow K/\text{Ker } f$ – канонічний гомоморфізм». Використовувати $\text{Ker } f$, а не $\text{Ker } \varphi$.

Якщо K – область цілісності з I і $\mathcal{I}(m)$ – головний ідеал, породжений елементом $m \in \mathcal{I}$, то всякі елементи $a, b \in \mathcal{I}$, які конгруентні за ідеалом $\mathcal{I}$, називають конгруентними за модулем m і записують, це так:

$$a \equiv b \pmod{m}$$

Суміжні класи кільця K – за ідеалом і $\mathcal{I}(m)$ називають в даному випадку суміжними класами за модулем m . Будь-який елемент суміжного класу називають часто лишком цього класу. Тому суміжні класи за модулем m часто називають класами лишків за модулем m .

Теорема 2.14. Елементи $a, b \in K$ конгруентні між собою за модулем $m \in K$ тоді і тільки тоді, коли

$$(\exists k \in K): a = b + mk.$$

Доведення. Якщо $a \equiv b \pmod{m}$, то $a - b \in (m)$ тобто $(\exists k \in K): a = b + mk$ навпаки, якщо $a = b + mk$, то $a - b = mk$, тобто, $a - b \in (m)$ і, значить, $a \equiv b \pmod{m}$. Відзначимо деякі властивості конгруенцій за модулем m . Основні властивості конгруенцій сформульовані в теоремі I. Із цієї теореми випливає, зокрема, що почленне додавання і множення конгруенцій за одним і тим же модулем не приводить до порушення конгруентності. Конгруентність не порушується ще й при таких перетвореннях:

1. Додавання до обох частин конгруенції одного і того ж елемента.
2. Перенесення з протилежним знаком будь-якого доданка з однієї частини конгруенції в другу.

3. Додавання до однієї частини конгруенції елемента, кратного модулю.

4. Множення обох частин конгруенції на будь-який елемент.

5. Ділення обох частин конгруенції на їх спільний дільник, що взаємно простий з модулем.

6. Множення обох частин конгруенції і модуля на довільний елемент.

7. Ділення обох частин конгруенції і модуля на їх довільний спільний дільник.

Доведення непорушності конгруентності при вказаних перетвореннях тривіальне і проводиться цілком аналогічно, як і для цілих чисел (див. наприклад, О. І. Бородін, Теорія чисел, §15).

Вкажемо ще одну просту і важливу властивість конгруенцій.

Якщо елементи $a, b \in K$ конгруентні за модулем $m_1, m_2, \dots, m_n \in K$, то вони конгруентні і за їх найменшим спільним кратним $[m_1, m_2, \dots, m_n]$.

Справді, із конгруенцій $a \equiv b \pmod{m_i}$ випливає $a - b : m_i$, тобто $a - b$ є спільним кратним чисел m_i і, значить, елемент $a - b$ ділиться $[m_1, m_2, \dots, m_n]$, звідки випливає потрібна конгруенція

$$a \equiv b \pmod{[m_1, m_2, \dots, m_n]}.$$

§2.11. КОНГРУЕНЦІЇ ТА КЛАСИ ЛИШКІВ ЗА МОДУЛЕМ m

В цьому параграфі застосуємо результати попереднього параграфу до кільця цілих чисел.

Насамперед зауважимо, що, як це показано в §2, кільце $\mathbb{Z}$ цілих чисел є кільцем головних ідеалів – всякий ненульовий ідеал в $\mathbb{Z}$ є сукупністю чисел, кратних деякому натуральному числу m , його можна записувати у вигляді $m\mathbb{Z}$. Тому конгруенції в цьому кільці є конгруенціями за модулем m . Нагадаємо, що за означенням числа $a, b \in \mathbb{Z}$ конгруентні за модулем m , якщо їх різниця $a - b$ ділиться націло на m . За теоремою 2.11 §5 числа $a, b \in \mathbb{Z}$ конгруентні за $\text{mod } m$ тоді і тільки тоді, коли існує $t \in \mathbb{Z}$

таке, що $a = b + mt$. Для цілих чисел справедливий ще один критерій конгруентності.

Теорема 2.15. Цілі числа a і b конгруентні за модулем m тоді і тільки тоді, коли вони мають однакові остачі при діленні на m .

Доведення. За теоремою про ділення з остачею

$$\exists q_1 r_1 \in \mathbb{Z} : a = mq_1 + r_1, 0 \leq r_1 < m,$$

$$\exists q_2 r_2 \in \mathbb{Z} : b = mq_2 + r_2, 0 \leq r_2 < m$$

Звідки $a - b = m(q_1 - q_2) + (r_1 - r_2)$. Оскільки перший доданок даної суми ділиться на m , то вся сума ділиться на m тоді і тільки тоді, коли на m ділиться другий доданок $r_1 - r_2$. Останнє, внаслідок того, $|r_1 - r_2| < m$ можливе тоді і тільки тоді, коли $r_1 - r_2 = 0$, тобто $r_1 = r_2$.

З теореми 2.10 §5 випливає, що сукупність чисел, конгруентних між собою за $\text{mod } m$, співпадає з деяким суміжним класом кільця $\mathbb{Z}$ за ідеалом $m\mathbb{Z}$. Через це сукупність чисел, конгруентних між собою за $\text{mod } m$, називається класом чисел, конгруентних за $\text{mod } m$, а будь-яке число із цього класу його представником або лишком. Тому клас чисел, конгруентних за модулем m ще називають класом лишків кільця цілих чисел за модулем m .

Як відомо, сукупність суміжних класів кільця K за ідеалом $\mathcal{I}$ утворює розбиття цього кільця, яке само є кільцем відносно операцій додавання та множення класів – фактор-кільцем $K/\mathcal{I}$. Тому сукупність класів лишків кільця цілих чисел за модулем m утворює фактор-кільце $\mathbb{Z}/m\mathbb{Z}$. З теореми I виходить, що фактор-кільце $\mathbb{Z}/m\mathbb{Z}$ є скінченим і містить m різних класів.

Справді, кожен клас лишків $\text{mod } m$ є сукупність всіх цілих чисел, що при діленні на m дають одну і ту ж остачу r . Оскільки всіх остач $\in m - 0, 1, 2, \dots, m-1$ – кожна з них міститься в одному і тільки в одному класі лишків та, навпаки, кожен клас містить одну з цих остач, то всіх різних класів лишків $\in m$.

Класи лишків за модулем m позначають часто через C_r , де r – остача чисел даного класу при діленні на m . Випишемо їх:

$$C_0 = 0 + m\mathbb{Z} = \{\dots, -2m, -m, 0, -m, 2m, \dots\},$$

$$C_1 = 1 + m\mathbb{Z} = \{\dots, -2m+1, -m+1, 1, m+1, 2m+1, \dots\}$$

$$C_r = r + m\mathbb{Z} = \{\dots, -2m+r, -m+r, r, m+r, 2m+r, \dots\}$$

$$C_{m-1} = (m-1) + m\mathbb{Z} = \{\dots, -2m+(m-1), -m+(m-1), m-1, 2m-1, \dots\}.$$

Якщо з кожного класу чисел за модулем m взяти по одному і тільки, по одному лишку, то одержана система чисел називається повною системою лишків модулем m . Найчастіше за повну систему лишків за модулем m вибирають найменші невід'ємні лишки $0, 1, 2, \dots, m$ або абсолютно найменші лишки, тобто лишки, які в своїх класах є найменшими за абсолютною величиною. За модулем 10, наприклад, повною системою найменших невід'ємних лишків є:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9,$$

а повною системою абсолютно найменших лишків є

$$0, 1, 2, 3, 4, 5, -4, -3, -2, -1.$$

Або

$$0, 1, 2, 3, 4, -5, -4, -3, -2, -1.$$

Крім повних систем лишків, в теорії чисел важливу роль відіграють так звані зведені системи лишків. Щоб підійти до цього поняття, зауважимо, що числа одного і того ж класу $C_r = \{r + mt\}, t \in \mathbb{Z}$ в силу відомого співвідношення

$$(m, mt + r) = (m, r).$$

Мають модулем один і той же найбільший спільний дільник. Зокрема, всі числа одного і того ж класу C_r є одночасно взаємно простими з m або взаємно не простими з m , тобто можна говорити про класи чисел, взаємно простих а модулем m . При цьому клас C_r є взаємно простим за модулем m тоді і тільки тоді, Коли $(r, m) = 1$. Це означає, що класів чисел, взаємно простих з модулем m , є стільки, скільки є чисел, менших від m і взаємно простих m , тобто, $\varphi(m)$. Якщо з кожного класу лишків, взаємно

простих за модулем m , взяти по одному і тільки по одному лишку, то одержана сукупність чисел називається зведеною системою лишків за модулем m . Щоб зведену систему, треба з повної системи ликів за модулем m вибрати числа, взаємно прості з m .

§2.12. КІЛЬЦЕ КЛАСІВ ЛИШКІВ ЗА МОДУЛЕМ m

Вище вже відзначалося, що сукупність усіх класів лишків m утворює кільце відносно операцій додавання і множення суміжних класів – фактор-кільце $\mathbb{Z}/m\mathbb{Z}$. Дослідимо, чи не є це кільце полем.

Лема 2.3. Сукупність m класів лишків $C_r = r + m\mathbb{Z}$, взаємно простих з модулем m , утворив у фактор-кільці $\mathbb{Z}/m\mathbb{Z}$ абелеву мультиплікативну групу порядку $\varphi(m)$.

Доведення. Відзначимо насамперед, що коли, $\mathcal{I} + m\mathbb{Z}, r + m\mathbb{Z} \in \mathfrak{M}$, то $(\mathcal{I}, m) = 1$ і $(r, m) = 1$, внаслідок чого $(\mathcal{I}r, m) = 1$. З цього виходить, що добуток довільних суміжних класів із $\mathfrak{M}(\mathcal{I} + m\mathbb{Z})(r + m\mathbb{Z}) = \mathcal{I}r + m\mathbb{Z}$ належить $\mathfrak{M}$, асоціативність і комутативність множення класів справедлива, бо $\mathbb{Z}/m\mathbb{Z}$ є комутативним кільцем. Внаслідок співвідношення $(1, m) = 1$.

Одиничний клас $C_1 = 1 + m\mathbb{Z}$ фактор-кільця $\mathbb{Z}/m\mathbb{Z}$ належить $\mathfrak{M}$. Для завершення доведення залишається показати, що кожен елемент $C_r \in \mathfrak{M}$ має обернений елемент, що теж належить $\mathfrak{M}$.

Нехай $C_r = r + m\mathbb{Z}$ – довільний клас із $\mathfrak{M}$. Тоді $(m, r) = 1$ і за теоремою 2.6 §4

$$(\exists \mathcal{I}, t \in \mathbb{Z}): 1 = r\mathcal{I} + mt$$

останньої рівності зокрема виходить що $(\mathcal{I}, m) = 1$, тобто клас $\mathcal{I} + m\mathbb{Z} \in \mathfrak{M}$. Крім того

$$(\mathcal{I} + m\mathbb{Z})(r + m\mathbb{Z}) = r\mathcal{I} + m\mathbb{Z} = (1 - mt) + m\mathbb{Z} = 1 + [m(-t) + m\mathbb{Z}].$$

Легко бачити, що $m(-t) + m\mathbb{Z} = m\mathbb{Z}$. Тому $(\mathcal{I} + m\mathbb{Z})(r + m\mathbb{Z}) = 1 + m\mathbb{Z}$, тобто клас $r + m\mathbb{Z} \in \mathfrak{M}$ є оберненим до класу $C_r = r + m\mathbb{Z}$.

Таким чином, $\mathfrak{M}$ – мультиплікативна абелева група. Оскільки за відзначеним в кінці п.1 класів лишків, взаємно простих з модулем $m \in \varphi(m)$, то порядок $\mathfrak{M}$ дорівнює $\varphi(m)$. **Лема доведена.**

Теорема 2.16. Якщо p – просте число, то кільце $\mathbb{Z}/p\mathbb{Z}$ класів лишків за модулем p є полем. Якщо m – складене число, то кільце $\mathbb{Z}/m\mathbb{Z}$ не є навіть областю цілісності.

Доведення.

1. Якщо p – просте число, то кожне з чисел $1, 2, \dots, p-1$ взаємно прості з p . Тому всі класи C_r лишків за модулем m , крім нульового класу $C_0 = m\mathbb{Z}$ належить абелевій мультиплікативній групі $\mathfrak{M}$, про яку йде мова в лемі. Це і означає, що в мультиплікативному кільці $\mathbb{Z}/p\mathbb{Z}$ з одиницею $1+m\mathbb{Z}$ всі елементи, крім нульового, мають обернені, тобто $\mathbb{Z}/p\mathbb{Z}$ є полем.

2. Нехай m – складене число. Оскільки m має нетривіальні натуральні дільники, що, звичайно, менші за нього, то

$$(\exists r \in \mathbb{Z}, 0 < r < m) : (m, r) = d \neq 1.$$

Покажемо, що клас $C_r = r + m\mathbb{Z}$ є дільником нуля. Оскільки $r < m$, то $r : m$ і, значить, клас $r + m\mathbb{Z} \neq m\mathbb{Z}$, тобто, не є нульовим класом кільця $\mathbb{Z}/m\mathbb{Z}$. Крім того, на підставі /I/.

$$(\exists k_1, k_2 \in \mathbb{Z}) : m = dk_1, r = dk_2, (k_1, k_2) = 1.$$

Внаслідок того, що $d \neq 1, k_1 < m$, значить, $k_1 : m$, тобто, клас $k_1 + m\mathbb{Z}$, є ненульовим. В той же час

$$(r + m\mathbb{Z})(k_1 + m\mathbb{Z}) = rk_1 + m\mathbb{Z} = (dk_1)k_2 + m\mathbb{Z} = mk_2 + m\mathbb{Z} = m\mathbb{Z}.$$

Отже, в кільці $\mathbb{Z}/m\mathbb{Z}$ існують дільники нуля, тобто, $\mathbb{Z}/m\mathbb{Z}$ не є областю цілісності і, тим більше, не є полем.

На закінчення цього параграфу використаємо доведену вище лему до доведення важливої теореми теорії чисел – теореми Ейлера.

Теорема 2.17. (Ейлера)

$$(\forall m \in \mathbb{N}) (\forall a \in \mathbb{Z}, (a, m) = 1) : a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Доведення. Оскільки $(a, m) = 1$ то клас $a + m\mathbb{Z}$ належить сукупності $\mathfrak{M}$ класів лишків, взаємно простих з модулем m . За лемою множина $\mathfrak{M}$ є мультиплікативною абелевою групою порядку $\varphi(m)$. Розглянемо в групі $\mathfrak{M}$ циклічну підгрупу $a + m\mathbb{Z}$, породжену класом $a + m\mathbb{Z}$. На підставі теореми Лагранжа порядок δ цієї підгрупи є дільником порядку $\varphi(m)$ групи $\mathfrak{M} : \varphi(m) = \delta k$.

Тому, що порядок циклічної підгрупи співпадає з порядком породжуючого її елемента,

$$(a + m\mathbb{Z})^\delta = 1 + m\mathbb{Z},$$

внаслідок чого

$$(a + m\mathbb{Z})^{\varphi(m)} = \left((a + m\mathbb{Z})^\delta \right)^k = 1 + m\mathbb{Z}$$

інакше кажучи,

$$a^{\varphi(m)} + m\mathbb{Z} = 1 + m\mathbb{Z}$$

Остання рівність показує, що $a^{\varphi(m)}$ і 1 належать до одного і того ж суміжного класу за модулем m і тому на підставі

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

Якщо $m = \rho$ – просте число, то $\varphi(\rho) = \rho - 1$ і теорему Ейлера можна формулювати так.

Теорема 2.18 (Ферма). Якщо ρ – будь-яке просте число і a – довільне ціле число, що не ділиться на ρ , то

$$a^{\rho-1} \equiv 1 \pmod{\rho}$$

Часто теорему Ферма подають в такій формі:

Якщо ρ – просте число, то

$$(\forall a \in \mathbb{Z}) : a^\rho \equiv a \pmod{\rho}.$$

Якщо $a \not\equiv \rho$, то справедливість останньої конгруенції очевидна. Якщо $a \equiv \rho$, то остання конгруенція одержується з попередньої домноженням на a , що конгруенції не порушує.

§2.13. ЗАСТОСУВАННЯ КОНГРУЕНЦІЙ ДО ВСТАНОВЛЕННЯ ОЗНАК ПОДІЛЬНОСТІ

Як відомо, в кільці Z цілих чисел визначені операції додавання, віднімання і множення, а дія ділення не завжди можлива. Тому виникає потреба визначити, при яких умовах цілі числа діляться одно на одне.

Подільність чисел – це певне відношення між числами, яке в Z_+ має такі властивості: *рефлексивність* ($a:a$), *транзитивність* ($[a:b \ b:c][a:c]$) і *антисиметричність* ($[a:b \ b:aa = b]$). Будь-яке відношення, яке має властивості рефлексивності, транзитивності і анти симетричності. Називається *відношенням не строгого порядку*. Отже, подільність чисел в Z_+ є відношенням не строгого порядку. Аналогічним відношенням частинної упорядкованості є, наприклад, відношення « $\geq$ » в кільці Z . Воно рефлексивне ($a \geq a$), транзитивне ($[a \geq b \wedge b \geq c] \Rightarrow [a \geq b]$), антисиметричне (якщо $a \geq b$ і $b \geq a$, то $b = a$).

Між відношеннями подільності $a \mid b$ в кільці Z можна встановити і таку аналогію. Відношення $a : b$ означає, що існує таке число c , при якому виконується рівність $a = bc$. Відношення $a \geq b$, або $a - b \geq 0$, означає, що існує таке число $c \geq 0$, при якому $a = b + c$. Рівності $a = bc$ і $a = b + c$, як бачимо, аналогічні.

Факт подільності двох чисел можна, звичайно, встановити за допомогою алгоритму ділення чисел з остачею. Проте для великих чисел це завдання досить складне. Тому бажано знайти зручні ознаки, за якими можна було б судити про подільність чисел, не виконуючи самого ділення. В цілому суть ознак подільності зводиться до того, що розгляд подільності деякого натурального числа a на натуральне число m змінюється розглядом подільності на число m іншого, меншого за a натурального числа b , яке можна знайти за деяким правилом, що визначається числовою функцією $f(a)$, тобто $b = f(a)$. При цьому числа a і $b = f(a)$ є, як кажуть. Рівноподільними на число m , тобто такі, які одночасно діляться або одночасно не діляться на число m . Часто вимагають, щоб вони були конгруентними за модулем m .

Одним із способів знаходження ознак подільності, оснований на конгруентності чисел, є так званий спосіб Паскаля¹. Нехай деяке натуральне число a при основі числення g має вигляд

$$a = p_n g^n + p_{n-1} g^{n-1} + \dots + p_1 g + p_0,$$

де коефіцієнти p_k є натуральні числа, які задовольняють нерівності $0 \leq p_k < g$. Позначимо через r_k остачу від ділення числа g^k на m , тобто $g^k \equiv r_k \pmod{m}$, і побудуємо число $b = f(a)$ за таким правилом:

$$b = f(a) = p_n r_n + p_{n-1} r_{n-1} + \dots + p_1 r_1 + p_0.$$

На основі властивості 9 п. 15.1 $a \equiv b \pmod{m}$. Оскільки $b < a$, то дістаємо таку ознаку Паскаля подільності чисел.

Якщо число $b = p_n r_n + p_{n-1} r_{n-1} + \dots + p_1 r_1 + p_0$ ділиться на число m , то ділиться на нього і число $a = p_n g^n + p_{n-1} g^{n-1} + \dots + p_1 g + p_0$.

Якщо ж b на число m не ділиться, то не ділиться на m і число a .

За допомогою цієї загальної ознаки можна встановити зручні конкретні ознаки подільності чисел, записаних у звичайній для нас десятковій системі числення. У цій системі $g = 10$ і число a має вигляд:

$$a = p_n 10^n + p_{n-1} 10^{n-1} + \dots + p_1 10 + p_0.$$

Коротко це можна записати так: $a = p_n p_{n-1} \dots p_1 p_0$.

а) Ознака подільності на 2 і на 5.

Оскільки $10^k : 2 \mid 10^k : 5$, то всі остачі r_k від ділення 10^k на числа 2 і 5 дорівнюють нулю. Тому за формулою (2) число $b = f(a) = p_0$. Отже, маємо таку ознаку:

Число a ділиться на 2 і на 5 тоді і тільки тоді, коли на них ділиться цифра одиниць числа a .

Приклад. Число $a = 8574 : 2$, бо $4 : 2$. Число 8127 не ділиться на 5, бо 7 не ділиться на 5.

б) Ознака подільності на 3 і на 9.

Оскільки всі остачі r_k від ділення 10^k на число 3 або 9 дорівнюють 1, то за (2) $b = f(a) = p_n + p_{n-1} + \dots + p_1 + p_0$

Отже, маємо таку ознаку:

Число a ділиться на 3 (або на 9) тоді і тільки тоді, коли сума цифр, які його зображують, ділиться на 3 (або відповідно на 9).

Приклад. Число $a=5742:3$, бо сума цифр $b=5+7+4+2=18:3$.

в) Ознака подільності на 11.

За модулем 11 маємо

$$10^{2k} \equiv 1 \pmod{11}, 10^{2k-1} \equiv -1 \pmod{11}.$$

Тому $r_{2k} = 1, r_{2k-1} = -1$, і, отже, за рівністю (2)

$$b = p_0 - p_1 + p_2 - p_3 + p_4 - p_5 + \dots = (p_0 + p_2 + p_4 + \dots) - (p_1 + p_3 + p_5 + \dots).$$

Враховуючи, що цифри p_{2k} з парними індексами в числі a стоять на непарних місцях, можна сформулювати таку ознаку:

Число a ділиться на 11 тоді і тільки тоді, коли різниця між сумою цифр, які стоять на непарних місцях, і сумою цифр, які стоять на парних місцях, ділиться на 11.

Приклад. Число $a=53746:11$, бо число

$$b = (6 + 7 + 5) - (4 + 3) = 18 - 7 = 11$$

ділиться на 11.

У системі числення з основою $g=10^2$ можна знайти зручні ознаки подільності на числа 4, 25, 50. Число a в цій системі можна записати так:

$$a = c_s 100^s + c_{s-1} 100^{s-1} + \dots + c_1 100 + c_0.$$

Порівнюючи це з (3), бачимо, що $c = p_1 10 + p_0 = \overline{p_1 p_0}$, тобто є двоцифровим числом, яке зображується двома останніми цифрами числа a в десятковій системі числення.

Враховуючи, що $a \equiv c \pmod{100}$ і числа 100^k діляться на числа 4, 25, 50, дістаємо такі ознаки подільності:

Число $a = \overline{p_n p_{n-1} \dots p_1 p_0}$ ділиться на 4 (або відповідно 25 чи 50) ділиться двоцифрове число $c_0 = \overline{p_1 p_0}$, утворене двома останніми цифрами числа a , записаного в десятковій системі числення.

Ознаки подільності є цінними, якщо вони прості, зручні для користування. Проте більшість ознак, які можна вивести з ознаки Паскаля, є

складними. Існує ряд зручних ознак подільності, які не впливають з загальної ознаки Паскаля, а знайдені іншими способами. Наприклад, одну з ознак подільності на 7 можна сформулювати так:

Число $a = 10a_1 + a_0$ ділиться на 7 тоді і тільки тоді, коли ділиться на 7 число $b = a_1 - 2a_0$.

Зазначимо, що на відміну від усіх попередніх ознак числа a і b тут рівноподільні на 7, а не конгруентні між собою за модулем $m=7$.

Приклад. $a = 285 = 28 \cdot 10 + 5, b = 28 - 2 \cdot 5 = 18$.

Оскільки b не ділиться на 7, то не ділиться на 7 і число 285. Зазначимо, що при діленні на 7 числа 285 дістаємо остачу 5, а при діленні на 7 числа 18 остача дорівнює 4 і тому $285 \not\equiv 18 \pmod{7}$.

Приклад. Встановити, чи ділиться на 7 число $a = 63364$.

Приклад можна розв'язати так. Перш за все $a = 63000 + 364$ і тому $63364 \equiv 364 \pmod{7}$. А $364 = 36 \cdot 10 + 4$. Тому $b = 36 - 2 \cdot 4 = 28$. Оскільки $28:7$ то й число $63364:7$.

Розглянемо питання про перетворення звичайного дробу в десятковий. Як відомо з арифметики звичайні дроби перетворюються або в скінченні, або не в скінченні періодичні десяткові дроби. При цьому звичайний дріб $\frac{a}{b}$ перетворюється в скінченний десятковий дріб тоді і тільки

тоді, коли канонічний розклад знаменника має вигляд $2^\alpha 5^\beta$. тобто не містить ніяких простих множників, крім 2 і 5. Для спрощення вважатимемо $\frac{a}{b}$ нескоротним правильним дробом. (Якщо він неправильний, то можна спочатку виділити цілу частину).

Звичайні нескоротні і правильні дроби виду $\frac{a}{2^\alpha \cdot 5^\beta}$ перетворюються в скінченні десяткові дроби з числом десяткових знаків, яке дорівнює найбільшому з чисел α або β . Справді, якщо

$\alpha = \beta$ то $\frac{a}{2^\alpha \cdot 5^\beta} = \frac{a}{2^\alpha \cdot 5^\alpha} = \frac{a}{10^\alpha}$ скінченний десятковий дріб. Якщо $\alpha < \beta$, то

$\frac{a}{2^\alpha \cdot 5^\beta} = \frac{a2^{\beta-\alpha}}{2^\beta \cdot 5^\beta} = \frac{a2^{\beta-\alpha}}{10^\beta}$ скінченний десятковий дріб. Якщо $\alpha > \beta$, то

$\frac{a}{2^\alpha \cdot 5^\beta} = \frac{a5^{\alpha-\beta}}{2^\alpha \cdot 5^\alpha} = \frac{a5^{\alpha-\beta}}{10^\alpha}$ скінченний десятковий дріб.

Легко зрозуміти, що нескоротний дріб виду $\frac{a}{c \cdot 2^\alpha \cdot 5^\beta}$, де c відмінне від 2 і 5, в скінченний десятковий дріб не перетворюється.

Справді, припускаючи супротивне, маємо

$$\frac{a}{c \cdot 2^\alpha \cdot 5^\beta} = \frac{d}{10^m},$$

Звідки $a \cdot 10^m = d \cdot c \cdot 2^\alpha \cdot 5^\beta$, де c – дільник числа $a \cdot 10^m$, що неможливо, бо c відмінне від 2 і 5 за умовою і $(a, c) = 1$. Ця суперечність доводить справедливість твердження.

Теорема 2.19. Якщо канонічний розклад знаменника b нескороченого дробу $\frac{a}{b}$ не містить у собі множників 2 і 5, то цей дріб перетворюється у чистий періодичний десятковий дріб; при цьому число цифр у періоді дорівнює показнику, до якого належить число 10, за модулем b .

Доведення. Для спрощення дріб $\frac{a}{b}$ вважатимемо правильним. Процес ділення числа a на число b при умові $a < b$ можна схематично зобразити так:

$$\begin{array}{r}
- \\
\cdot 10 \\
b \ q_1 \\
- r_1 10 \\
b \ q_2 \\
r_2 \\
\text{.....} \\
- r_{m-1} 10 \\
b \ q_m \\
\\
- r_m 10 \\
b \ q_{m+1} \\
r_{m+1} \\
\text{.....}
\end{array}$$

Цю схему в свою чергу можна подати у вигляді системи рівностей:

$$10a = bq_1 + r_1,$$

$$10r_1 = bq_2 + r_2$$

.....

$$10r_{m-1} = bq_m + r_m,$$

$$10r_m = bq_{m+1} + r_{m+1},$$

.....

де $r_1, r_2, \dots, r_m, r_{m+1}, \dots$ – остачі, а $q_1, q_2, \dots, q_m, q_{m+1}, \dots$ – частки проміжних обчислень. Будь-яка остача r_i , очевидно, задовольняє нерівність

$$0 < r_i < b,$$

а будь-які числа q_i задовольняють нерівність $0 \leq q_i < 10$, тобто є цифрами, з яких складається частка $0, q_1 q_2 \dots q_m q_{m+1} \dots$ в схемі (4).

Проаналізуємо властивості чисел r_i і q_i докладніше. Насамперед нагадаємо, що дріб $\frac{a}{b}$ є нескоротним і правильним. Це означає, що $(a, b) = 1$ і $a < b$. Таким чином, число a є один з найменших додатних лишків ЗСЛ за модулем b . Справді

$$[(a, b) = 1(10, b)][(10a, b) = 1].$$

Оскільки числа $10a$ і b взаємно прості, то з першої рівності (5) випливає, що $(r_1, b) = 1$. Справді за умови $(r_1, b) = d > 1$ впливало б, що вся права частина, а отже, і ліва частина ділилась би на d . Тому числа $10a$ і b не були б взаємно простими, що суперечить (7). За умов $0 < r_1 < b$ і $(r_1, b) = 1$ випливає, що остача r_1 є одним з найменших додатних лишків ЗСЛ за модулем b . Аналогічно можна показати, що й числа $r_2, \dots, r_m, r_{m+1}, \dots$ є найменшими додатними лишками ЗСЛ за модулем b . Але ЗСЛ за модулем b може мати не більше (b) найменших додатних лишків. Тому в системі рівностей (5) настане момент, коли одна з остач дорівнюватиме a . Нехай $r_m = a$. Тоді $m+1$ рівність (5) збіжиться з першою рівністю цієї системи. І тому Далі, ... рівність збіжиться з другою рівністю (5) і тому $q_2 = q_{m+2}, r_2 = r_{m+2}$. Таким чином, остачі r_i і частки q_i проміжних обчислень повторюватимуться. Тим самим частка в схемі (4) буде чистим періодичним десятковим дробом виду

$$0,(q_1q_2\dots q_m).$$

Для доведення теореми залишається показати, що перше повторення настане після δ кроків проміжних обчислень, де δ – показник, до якого належить 10 за модулем b . Справді, якщо δ – найменший показник, при якому здійснюється конгруенція

$$10^\delta \equiv 1 \pmod{b}$$

то при $r < b$ і $(r, b) = 1$ рівносильною їй є і конгруенція

$$10^\delta \cdot r \equiv r \pmod{b}$$

Остання конгруенція якраз і показує, що, приписавши до r нулів, що відповідає визначенню δ послідовних цифр частки, дістанемо при діленні $10^\delta \cdot r$ на b остачу b . При діленні a на b при $(a, b) = 1$ і $a < b$ аналогічно дістанемо через δ ділень остачу, яка дорівнює числу a . Отже, частка (8) має вигляд $0,(q_1q_2\dots q_m)$, що й треба було довести.

Зауваження. З конгруенції $10^\delta \equiv 1 \pmod{b}$ випливає, що $10^\delta - 1 \equiv 0 \pmod{b}$ або $99\dots 9 \equiv 0 \pmod{b}$.

Іншими словами, число $999\dots 9$, що складається з δ дев'яток – найменше з можливих чисел такої структури, яке ділиться на b . Це дає можливість досить легко знаходити число δ . Для цього треба послідовно ділити на b числа 9, 99, 999, 9999, ... і т. д., аж поки таке ділення не відбудеться. Кількість дев'яток у такому числі і дорівнює числу δ .

Теорема 2.20. Якщо канонічний розклад знаменника b нескоротного дробу $\frac{a}{b}$ має вигляд $b = c \cdot 2^\alpha \cdot 5^\beta$, де $(c, 10) = 1$, то цей дріб перетворюється у мішаний періодичний дріб; число цифр до періоду дорівнює γ , де γ – найбільше з чисел α і β ; число цифр періоду дорівнює δ , де δ – показник, якому належить число 10 за модулем c .

Доведення. Дріб

$$\frac{a}{b} = \frac{a}{c \cdot 2^\alpha \cdot 5^\beta}$$

помножимо на 10^γ , де $\gamma = \max\{\alpha, \beta\}$. Матимемо

$$\frac{10^\gamma \cdot a}{b} = \frac{a \cdot 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta}}{c} = \frac{a_1}{c}$$

і далі

$$[(a, c) = 1 \wedge (2, c) = 1 \wedge (5, c) = 1] \Rightarrow [(a \cdot 2^{\gamma-\alpha} \cdot 5^{\gamma-\beta}) = 1] \Rightarrow [(a_1, c) = 1]$$

За теоремою 2.19, дріб $\frac{a_1}{c}$ перетворюється в чистий періодичний дріб з числом цифр у періоді, яке дорівнює δ , де δ – показник, до якого належить 10 за модулем c . Щоб з нього дістати початковий дріб $\frac{a}{b}$, треба розділити його на 10, або інакше, перенести кому в знайденому періодичному дробі на γ знаків ліворуч; у результаті дістанемо мішаний періодичний дріб з числом γ цифр до періоду. **Теорему доведено.**

Приклади.

1. Знайти число цифр періоду десяткового періодичного дробу, в який перетворюється дріб $\frac{7}{39}$.

Ділимо на 39 послідовно числа 9, 99, 999, 9999, 99999. Нарешті з'ясовується, що тільки число 999999 націло ділиться на 39. Кількість дев'яток у цьому числі визначає довжину періоду: $\delta = 6$.

2. Знайти число цифр, яке міститься до періоду, і довжину періоду періодичного дробу, в який перетворюється дріб $\frac{13}{550}$.

Знаменник цього дробу в канонічному розкладі має вигляд $550 = 2 \cdot 5^2 \cdot 11$. Тому $\gamma = \max\{\alpha, \beta\} = 2$ є найбільшим з показників степеня цифр 2 і 5. Це означає, що періодичний десятковий дріб має дві цифри до періоду. Найменше з чисел, складених з дев'яток, яке ділиться на 11, є число 99. Воно складається з двох дев'яток. Це означає, що довжина ... періоду періодичного дробу дорівнює 2. І справді, як неважко перевірити, розглядуваний дріб перетворюється в такий періодичний дріб:

$$\frac{13}{550} = 0,02(36).$$

Розділ III

КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД ОДНОГО НЕВІДОМОГО

§3.1. ПОДІЛЬНІСТЬ МНОГОЧЛЕНІВ

В алгебрі многочленів вивчається знайоме ще із школи поняття многочлена від одного і кількох невідомих. В шкільному курсі алгебри і математичному аналізі під многочленом з одним невідомим розуміють вирази виду: $4x^7 - 3x^5 + 5x - 9$, $ax^2 + bx + c$, $ax + b$ і, більше загально, $a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. При цьому мається на увазі, що замість x можна підставити будь-яке дійсне число і виконувати зазначені дії, внаслідок чого кожному дійсному числу $x = x_0$ ставиться у відповідність дійсне число $a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$. Це означає, що досі, говорячи про многочлен, ми мали на увазі функцію $y = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$.

Однак таке «функціональне» тлумачення многочлена для потреб алгебри є незручним і не завжди можливим. Справа в тому, що в алгебрі доводиться розглядати многочлени з коефіцієнтами, взятими із довільного поля чи кільця. Серед полів і кілець є поля і кільця із скінченною кількістю елементів. Таким є, наприклад, поле $\mathbb{Z}/2\mathbb{Z}$ класів лишків за простим модулем 2. Це поле складається із двох елементів-класів C_0 і C_1 . Якщо ввести загальновживані позначення $C_0 = 0, C_1 = 1$, то таблицка додавання і множення в цьому полі виглядає так:

$$0 + 0 = 0 \quad 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0.$$

$$0 + 1 = 1 + 0 = 1 \quad 1 \cdot 1 = 1.$$

$$1 + 1 = 0.$$

Тому, наприклад, $(\forall x \in \mathbb{Z}/2\mathbb{Z}): x^3 + x^2 + x = x^3, x^2 + x = 0$.

Значить, коли на многочлени дивитися як на функції, то в полі $\mathbb{Z}/2\mathbb{Z}$ справедливі такі тотожні рівності многочленів:

$$x^2 + x = 0, x^3 + x^2 + x = x^3,$$

які суперечать загальноприйнятому розумінню тотожної рівності многочленів. З цього виходить, що в алгебрі, в усякому разі при розгляді многочленів, коефіцієнти яких взяті із нечислових полів і кілець, зручно відмовитись від розгляду многочленів як функцій і дати їм якесь зовсім інше означення.

Щоб зрозуміти, яким має бути алгебраїчне означення многочлена і сукупності многочленів, досить пригадати, що в сучасній алгебрі вивчаються алгебраїчні структури, більше того, сучасна алгебра – це теорія алгебраїчних структур. Коли говорять про алгебраїчну структуру, то мають на увазі множину, в якій задано одну чи декілька внутрішніх або зовнішніх алгебраїчних операцій, що задовольняють тим чи іншим умовам (аксіомам). В попередній частині курсу алгебри вивчалися такі алгебраїчні структури: півгрупи, групи, поля, лінійні простори і кільця. При вивченні лінійних операторів в лінійному просторі згадувалася ще одна алгебраїчна структура – лінійна алгебра. Нагадаємо означення дещо узагальнивши його.

Означення 1. Нехай K – комутативне кільце з 1. Алгеброю (лінійною алгеброю, гіперкомплексною системою) над K називається *векторний простір* (частіше кажуть, модуль) над K , в якому поряд з внутрішньою операцією $+$ запроваджена ще одна внутрішня операція $\times$, відносно яких $\mathfrak{A}$ утворює кільце, причому:

$$(\forall \alpha \in K)(\forall x, y \in \mathfrak{A}): \alpha(x, y) = (\alpha x) y = x(\alpha y) \quad (1)$$

Відомими прикладами алгебр над полем $\mathcal{P}$ є:

1. Множина M_n усіх матриць n -го порядку, складених із елементів поля $\mathcal{P}$.
2. Множина усіх лінійних операторів в n -вимірному лінійному просторі над $\mathcal{P}$.

Коли розглядати множину многочленів як функцій на довільному числовому полі $\mathcal{P}$, то звичайним способом в цій множині можна задати операції додавання і множення многочленів і множення чисел поля $\mathcal{P}$ на многочлени, причому ці операції задовольняють усім аксіомам кільця та лінійного простору і аксіомі (1), множення, крім того, комутативне. Це

означає, що множина многочленів, як функцій певного виду, утворює комутативну алгебру над полем $\mathcal{P}$. Особливістю цієї алгебри є те, що в ній існує многочлен $e(x) = x$ такий, що кожен многочлен є лінійною комбінацією скінченної кількості степенів цього многочлена.

Сукупність усіх степенів $x^0 = 1, x, x^2, \dots, x^n, \dots$ цього многочлена лінійно незалежна, тому що рівність

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n \equiv 0$$

справедлива тоді і лише тоді коли $\alpha_0 = \alpha_1 = \alpha_2 = \dots = \alpha_n = 0$.

Отже, сукупність многочленів $1, x, x^2, \dots, x^n, \dots$ утворює базу даної алгебри.

Зазначені алгебраїчні властивості многочленів як функцій на числовому полі бажано зберегти і в загальному випадку. Тим більше, як ми покажемо, ці властивості характеризують множину многочленів однозначно (з точністю до ізоморфізму). Тому доцільно ввести таке означення.

Означення 2. Нехай K – комутативне кільце з 1. Комутативна алгебра над кільцем K , в якій існує такий елемент x , що елементи $x^0 = 1, x, x^2, \dots, x^n, \dots$ утворюють базу цієї алгебри, називаються *кільцем многочленів зі змінним* (з невідомим) x над K і позначається $K[x]$. Елементи цієї алгебри називають многочленами від змінного x і позначаються $f(x), g(x), \varphi(x), \dots$

Ще раз нагадаємо, що елементи $1, x, x^2, \dots, x^n, \dots$ утворюють базу тоді і тільки тоді, коли:

а) $1, x, x^2, \dots, x^n, \dots$ лінійно незалежні, тобто лінійно незалежною є всяка їх скінченна підсистема;

б) всякий елемент $f(x)$ із $\mathcal{P}[x]$ є лінійною комбінацією скінченної сукупності елементів із $1, x, x^2, \dots, x^n, \dots$ тобто $f(x) = a_{k_1} x^{k_1} + a_{k_2} x^{k_2} + \dots + a_{k_n} x^{k_n}$

Елементи виду ax^n називаються *одночленами*. Якщо розглядати одночлен з нульовими коефіцієнтами, то всякий многочлен $f(x)$ може бути записаний у вигляді

$$f(x) = a_0x^0 + a_1x + a_2x^2 + \dots + a_nx^n = \sum_{k=1}^n a_kx^k \quad (2)$$

Елементи a_k в цьому записі називаються *коефіцієнтами* многочлена $f(x)$, а елемент x – цілком певний елемент даної алгебри, але за традицією його називають *змінним*, одночлени a_nx^n – членами многочлена $f(x)$.

В силу лінійної незалежності системи елементів $1, x, x^2, \dots$ подання всякого многочлена $f(x)$ у вигляді (2) є єдиним, якщо не брати до уваги членів з нульовими коефіцієнтами. Зокрема, нульовий елемент алгебри $K[x]$ і тільки він має в записі (2) всі коефіцієнти нулі. Цей елемент називається *нульовим многочленом*. Із єдності представлення (1) виходить, що многочлени $f(x)$ і $g(x)$ рівні тоді і лише тоді, коли вони складаються з одних і тих же ненульових членів, тобто, якщо в їх поданнях у вигляді (2) коефіцієнти при однакових степенях змінного x рівні.

Найбільше із чисел k , при якому в записі многочлена $f(x)$ у вигляді (2) $a_n \neq 0$ називається *степенем многочлена $f(x)$* , що позначається $\deg f(x)$ (*degree*). Як правило, вважатимемо, що в записі (2) $a_n \neq 0$ і, значить, степінь $f(x)$ дорівнює n . Коефіцієнт a_n називається, при цьому, *старшим коефіцієнтом* многочлена, а коефіцієнт a_0 при x^0 – *вільним членом*. Поняття степеня для нульового многочлена не вводиться, тобто, степінь нульового многочлена неозначений.

Із того, що в алгебрі $K[x]$ операції додавання і множення асоціативні і комутативні, множення дистрибутивне відносно додавання, легко випливає, що додавання і множення многочленів

$$f(x) = \sum_k a_k x^k, \quad g(x) = \sum_k b_k x^k$$

виконуються за звичайними правилами:

$$\begin{aligned} f(x) + g(x) &= \sum_k (a_k + b_k) x^k \\ f(x)g(x) &= \sum_k d_k x^k, \end{aligned} \quad (3)$$

де

$$d_k = \sum_{\substack{i,j=0 \\ i+j=k}}^k a_i b_j = \sum_{i=0}^k a_i b_{k-i},$$

причому, очевидно, $\deg(f + g) \leq \max(\deg f, \deg g)$

$$\deg(f \cdot g) \leq \deg f + \deg g.$$

Якщо K – область цілісності з 1, то в останній нерівності насправді має місце тільки знак $=$. Дійсно, якщо $\deg f = m$, $\deg g = n$, то $a_m \neq 0$, $b_n \neq 0$ і старшим коефіцієнтом добутку fg є елемент $d_{m+n} = a_m b_n$.

Оскільки K – область цілісності, то $d_{m+n} \neq 0$ і, значить, $\deg(f \cdot g) = m + n$. Зокрема, якщо $f(x) \neq 0$ і $g(x) \neq 0$, то і $f(x)g(x) \neq 0$. Таким чином, якщо K – область цілісності з 1, то алгебра $K[x]$ – теж область цілісності з одиницею, причому

$$\deg fg = \deg f + \deg g.$$

Роль одиниці в алгебрі $K[x]$ виконує многочлен x^0 .

§3.2. ІЗОМОРФНЕ ВКЛАДЕННЯ КІЛЬЦЯ K В АЛГЕБРУ $K[x]$

В нашій побудові кільце K фігурує як зовнішня множина, по відношенню до кільця $K[x]$. Насправді можна показати, що це кільце K ізоморфно складається в кільце $K[x]$. Для цього розглянемо в кільці $K[x]$ множину K_0 усіх многочленів нульового степеня ax^0 . Множина K_0 утворює підкільце кільця $K[x]$, бо

$$\begin{pmatrix} + \\ (ax^0) - (bx^0) \\ \cdot \end{pmatrix} = \begin{pmatrix} + \\ a - b \\ \cdot \end{pmatrix} x^0 \in K_0.$$

Задано відображення $f: K \rightarrow K_0$, поклавши:

$$(\forall a \in K): f(a) = ax^0.$$

Відображення f – ізоморфізм K на K_0 .

Оскільки ізоморфні множини з алгебраїчної точки зору можна не розрізняти, то можна провести ототожнення K з K_0 , ототожнивши відповідні при цьому елементи a та ax^0 , тобто поклавши:

$$\forall a \in K : ax^0 = a.$$

При такому ототожненні K стає підкільцем кільця $K[x]$, тобто не вважається зовнішньою множиною по відношенню до $K[x]$. Саме тому алгебраїчну структуру $K[x]$ переважно називають не алгеброю, а тільки кільцем, кільцем многочленів над кільцем K (цей факт відбито в означенні 2). Операція множення елементів із K на елементи із $K[x]$ вважають при цьому внутрішньою.

§3.3. ПРОБЛЕМА ІСНУВАННЯ ТА ЄДИНОСТІ КІЛЬЦЯ $K[x]$

Із самого означення математичного об'єкта ніколи не впливає, що насправді існує такий математичний об'єкт. В багатьох випадках існування означуваних об'єктів очевидне або безпосередньо впливає із попереднього розгляду. Наприклад, коли ми означуємо коло, як множину точок площини, рівновіддалених від даної точки, то спеціально ставити питання про існування кола не приходить. Однак, в більш складних випадках над існування означуваного об'єкта треба задуматися, тому що часто означення є тільки побажанням існування об'єкта із зазначеними властивостями.

Сама таким є означення 2 кільця $K[x]$. Проведені перед формулюванням означення 1.2 міркування про «функціональні» многочлени були нестрогими, мають часто евристичний характер і стосується тільки випадку, коли K – числове поле. Питання про існування $K[x]$ у випадку довільного комутативного кільця K з 1 залишається відкритим. Для його позитивного розв'язування досить навести приклад конкретної множини, яка б задовольняла усім умовам означення 2 (побудувати модель).

Спосіб побудови такого прикладу підказується однозначність запису всякого многочлена у вигляді (2), який означає, що всякий многочлен однозначно задається впорядкованою системою $(a_0, a_1, \dots, a_n)$ елементів кільця K . Виходить треба розглядати множину впорядкованих систем елементів із K . Операції в цій множині треба задавати відповідно до формул (3). Якщо після цього виявиться, що ця множина задовольняє умо-

вам означення 2, то проблема існування кільця $K[x]$ буде розв'язана позитивно. Після цього неважко довести, що всі можливі моделі кільця $K[x]$ ізоморфні між собою і, значить з точністю до ізоморфізму можна вважати, що над даним кільцем K існує лиш одне кільце $K[x]$.

Перейдемо до точних формулювань.

Теорема 3.1. Для всякого комутативного кільця K з 1 існує кільце многочленів $K[x]$, яке є з точністю до ізоморфізму єдиним. Останнє означає, що коли кільця K і S ізоморфні ($K \sim S$), то $K[x] \sim S[y]$, причому існує ізоморфізм $F: K[x] \rightarrow S[y]$, який зберігає ізоморфізм кілець K і S та задовольняє умову: $F(x) = y$.

Доведення: 1) Існування. Як відзначалося, треба розглядати множину впорядкованих систем елементів із K . Для зручності перетворимо кожну із цих систем в нескінченну послідовність, доповнивши її нулями, що відповідає можливості доповнення представлення (2) многочлена $f(x)$ доданками із нульовими коефіцієнтами.

Отже, нехай $\mathfrak{a}$ – множина всіх нескінченних послідовностей.

$$(a_n) = (a_0, a_1, \dots, a_n, \dots)$$

елементів кільця K , в якій всі елементи, починаючи з деякого номера, рівні 0. Задамо в множині $\mathfrak{a}$ алгебраїчні операції таким способом:

$$(a_k) + (b_k) = (a_k + b_k),$$

$$(a_k)(b_k) = (d_k), \quad (d_k = \sum_{i=0}^k a_i b_{k-i})$$

$$(\forall \alpha \in K)(\forall (a_k) \in \mathfrak{a}): \alpha(a_k) = (\alpha \cdot a_k).$$

Легко перевірити, що так задані операції задовольняють всім аксіомам комутативної алгебри. Покажемо, наприклад, справедливість дистрибутивності внутрішнього множення відносно додавання:

$$\begin{aligned} (a_k)((b_k) + (c_k)) &= (a_k)(b_k + c_k) = \left(\sum_{i=0}^k a_i (b_{k-i} + c_{k-i}) \right) = \left(\sum_{i=0}^k (a_i b_{k-i} + a_i c_{k-i}) \right) = \\ &= \left(\sum_{i=0}^k a_i b_{k-i} + \sum_{i=0}^k a_i c_{k-i} \right) = \left(\sum_{i=0}^k a_i b_{k-i} \right) + \left(\sum_{i=0}^k a_i c_{k-i} \right) = (a_k)(b_k) + (a_k)(c_k) \end{aligned}$$

(в цій викладці використано дистрибутивність множення відносно додавання в кільці K і означення алгебраїчних операцій в множині $\mathfrak{A}$). Отже, множина $\mathfrak{A}$ – алгебра над кільцем K .

Залишається показати, що в алгебрі $\mathfrak{A}$ є елемент x , степінь якого з цілими невід'ємними показниками утворюють базу $\mathfrak{A}$. Вибір елемента x підказується тим, що якби кільце $K[x]$ було побудоване, то многочлен $f(x) = x$ мав би коефіцієнти $(0, 1, 0, 0, \dots)$. Отже, покладемо:

$$x = (0, 1, 0, 0, \dots).$$

Тоді

$$x^2 = (0, 0, 1, 0, \dots),$$

$$x^3 = (0, 0, 0, 1, \dots),$$

$$x^n = (0, 0, 0, 0, \dots, 1, \dots).$$

Доповнивши множину цих степенів одиничним елементом алгебри $\mathfrak{A}$ $x^0 = (1, 0, 0, 0, \dots)$.

Ми помітимо, що всякий елемент $(a_0, a_1, a_2, \dots, a_n, 0, \dots) \in \mathfrak{A}$ лінійно виражається через степені

$$x^0, x, x^2, \dots, x^n, \dots : (a_0, a_1, a_2, \dots, a_n, 0, \dots) = a_0 x^0 + a_1 x + \dots + a_n x^n.$$

Система $x^0, x, x^2, \dots, x^n, \dots$ лінійно незалежна, бо для будь-якої її скінченної підсистеми $x^{k_1}, x^{k_2}, \dots, x^{k_n}$ рівність

$$\alpha_1 x^{k_1} + \alpha_2 x^{k_2} + \dots + \alpha_n x^{k_n} = 0 \quad (\alpha_1, \alpha_2, \dots, \alpha_n \in K)$$

рівносильна рівності

$$\begin{pmatrix} 0, \dots, \alpha_1, \dots, \alpha_2, \dots, \alpha_n, \dots \\ k_1+1 \quad k_2+1 \quad k_n+1 \end{pmatrix} = (0, \dots, 0, \dots, 0, \dots, 0, \dots),$$

Звідки $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$. Таким чином, система $1, x, x^2, \dots, x^n, \dots$ задовольняє обидві умови з означення бази лінійного простору і тому є базою алгебри $\mathfrak{A}$.

Отже, множина $\mathfrak{A}$ є кільцем многочленів над кільцем K .

2) Єдиність. Нехай $\varphi: K \rightarrow K_1$ – ізоморфізм кільця K в кільце K_1 . Треба показати існування такого ізоморфізму $F: K[x] \rightarrow K_1[y]$, що

$$(\forall a \in K): F(a) = \varphi(a) \text{ і } F(x) = y. \quad (4)$$

З цією метою задамо відображення $F: K[x] \rightarrow K_1[y]$

$$(\forall f(x) = \sum_k a_k x^k): F(f) = \sum_k \varphi(a_k) y^k.$$

Якщо взяти $f(x) = a: f(x) = x$, то одразу одержимо що відображення F задовольняє умови (4).

Бієктивність відображення F випливає з таких міркувань.

Якщо

$$f(x) = \sum_k a_k x^k \neq g(x) = \sum_k b_k x^k,$$

то в силу єдиності запису многочлена у вигляді (2) принаймні одному K $a_k \neq b_k$. Тоді, внаслідок ін'єктивності відображення φ , $\varphi(a_k) \neq \varphi(b_k)$ і, значить, $F(f) \neq F(g)$, тобто, F – ін'єктивне відображення. Якщо $f_1(y) = \sum_k a'_k y^k$ – довільний многочлен із $K_1[y]$, то із сур'єктивності відображення φ виходить $(\forall k)(\exists a_k \in K): a'_k = \varphi(a_k)$. Поклавши $f(x) = \sum_k a_k x^k$,

одержимо $F(f) = f_1$, звідки і випливає сур'єктивність відображення F .

Гомоморфність відображення F доводиться звичайним способом.

Якщо

$$f(x) = \sum_k a_k x^k \text{ і } g(x) = \sum_k b_k x^k,$$

то

$$\begin{aligned} F(f+g) &= F\left(\sum_k (a_k + b_k) x^k\right) = \sum_k \varphi(a_k + b_k) y^k = \\ &= \sum_k (\varphi(a_k) + \varphi(b_k)) y^k = \sum_k \varphi(a_k) y^k + \sum_k \varphi(b_k) y^k = F(f) + F(g), \end{aligned}$$

$$\begin{aligned}
F(f \cdot g) &= F\left(\sum_k \left(\sum_{i=0}^k a_i b_{k-i}\right) x^k\right) = \sum_k \varphi\left(\sum_{i=0}^k a_i b_{k-i}\right) y^k = \\
&= \sum_k \left(\sum_{i=0}^k \varphi(a_i) \varphi(b_{k-i})\right) y^k = \sum_k \varphi(a_k) y^k \sum_i \varphi(b_i) y^i = F(f) \cdot F(g).
\end{aligned}$$

§3.4. КІЛЬЦЕ $K[x]$ ЯК ПРОСТЕ ТРАНСЦЕНДЕНТНЕ РОЗШИРЕННЯ КІЛЬЦЯ K

Згідно із зробленою в п.3 домовленістю кільце K є підкільцем кільця $K[x]$ і, значить, $K[x]$ є розширенням K . Із цього виходить можливість побудови кільця $K[x]$ як деякого розширення кільця K . Треба тільки з'ясувати як треба будувати це розширення, щоб одержати кільце многочленів $K[x]$. З цією метою введемо два нових поняття.

Означення 3. Нехай кільце (поле) K є підкільцем (підполем) кільця (поля) K' називається **алгебраїчним над K** , якщо існують $n \in N$ і елементи $a_0, a_1, \dots, a_n \in K$ не всі одночасно рівні 0, такі що справедлива рівність

$$a_0 \alpha^0 + a_1 \alpha + a_2 \alpha^2 + \dots + a_n \alpha^n = 0. \quad (5)$$

Якщо при всякому $n \in N$ і елементах $a_0, a_1, \dots, a_n \in K$ рівність (5) справедлива тоді і тільки тоді, коли $a_0 = a_1 = \dots = a_n = 0$, то елемент α називається трансцендентним над K . Якщо $K = Q$ (поле раціональних чисел) і $K' = C$ (поле комплексних чисел), то говорять просто про алгебраїчні і трансцендентні числа.

Числа $\sqrt{2}$ та $\sqrt[5]{3^2}$ – алгебраїчні, бо вони задовольняють рівності:

$$-2 \cdot 1 + 0 \cdot \sqrt{2} + 1 \cdot (\sqrt{2})^2 = 0.$$

$$-9 \cdot 1 + 0 \cdot \sqrt[5]{3^2} + 0 \cdot (\sqrt[5]{3^2})^2 + 0 \cdot (\sqrt[5]{3^2})^3 + 0 \cdot (\sqrt[5]{3^2})^4 + 1 \cdot (\sqrt[5]{3^2})^5 = 0;$$

$$1 \cdot i^2 + 1 = 0$$

Можна довести, що числа π та i трансцендентні.

З означення безпосередньо випливає, що елемент $\alpha \in K'$ є алгебраїчним тоді і тільки тоді, коли множина його степенів $\alpha^0, \alpha, \alpha^2, \dots, \alpha^n, \dots$ лінійно залежна, і трансцендентним тоді і тільки тоді, коли ця множина лінійно незалежна.

Якщо x – деякий елемент кільця K' , то K' є кільцем, яке включає підкільце K і цей елемент x . Крім K' , включати в себе підкільце K і елемент x можуть і деякі його підкільця. Перетин всіх таких підкільць, як легко бачити, знову є підкільцем кільця K , причому мінімальним за включенням підкільцем, яке включає K і елемент x .

Означення 4. Нехай K – підкільце кільця K' і x – елемент K' . Мінімальне кільце, яке включає підкільце K і елемент x , називається **простим розширенням кільця K** , одержаним шляхом приєднання елемента x , і позначається $K[x]$. Якщо x – алгебраїчний елемент над K , то розширення $K[x]$ називається алгебраїчним, якщо x – трансцендентний елемент, то розширення $K[x]$ називається трансцендентним.

Зараз можемо вже дати відповідь на запитання, поставлену на початку даного пункту.

Теорема 3.2. Розширення K' кільця K є кільцем многочленів над кільцем K , тобто $K' = K[x]$, тоді і тільки тоді, коли воно є простим трансцендентним розширенням кільця K .

Доведення. Якщо K' – кільце многочленів, тобто $K' = K[x]$, то за п.з. $K < K[x]$ і, крім того, $x \in K[x]$ причому за означенням 2 система $1, x, x^2, \dots, x^n, \dots$ лінійно незалежна і, значить, x трансцендентний елемент над K . Якщо кільце $\tilde{K}$ – деяке розширення K , що містить x , то воно містить всі добутки, суми і різниці елементів кільця K та елемента x , значить, всі елементи виду $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ тобто, $\tilde{K} \supset K[x]$.

Т.ч. $K[x]$ – мінімальне розширення кільця K , що містить елемент x , трансцендентний над K , тобто, $K[x]$ – просто трансцендентне розширення K .

Нехай K – підкільце кільця $\tilde{K}$, $x \in \tilde{K}$ – трансцендентний елемент над K і K' – просте трансцендентне розширення K , одержане шляхом приєд-

нання елемента x . Легко бачити, що множина K_0 всіх елементів виду $a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ ($n \in N, a_0, a_1, \dots, a_n \in K$) утворює підкільце в $\tilde{K}$. З другого боку підкільце K' включаючи в себе елементи кільця K і елемент x , включає в себе всі елементи виду

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n \quad (n \in N, a_0, a_1, \dots, a_n \in K).$$

Тобто $K' \supset K_0$. Оскільки за умовою K' – мінімальне розширення кільця K , яке містить елемент x , то справедливе зворотнє включення $K' \subset K_0$. Отже, $K' = K$ тобто, всякий елемент кільця K' , можна подати у вигляді $a_0 + a_1x + \dots + a_nx^n$ ($n \in N, a_0, a_1, \dots, a_n \in K$).

Із цього не важко зробити висновок, що K' – алгебра над кільцем K , базою якої є система степенів $x^0, x, x^2, \dots, x^n, \dots$ т.ч., всяке просте трансцендентне розширення K' кільця K є кільцем многочленів.

Зауваження. Щоб побудувати кільце многочленів над кільцем K , треба взяти будь-який елемент x , трансцендентний на K , і розглядати всі елементи. $f(x) = a_0 + a_1x + \dots + a_nx^n$, де $n \in N, a_0, a_1, \dots, a_n \in K$ – ці елементи називаються многочленами, а їх сукупність утворює кільце многочленів $K[x]$.

Зауваження. Якщо взяти інший елемент $y \neq x$ трансцендентний над K , то одержимо $K[y]$. За теоремою 1 $K[x] \sim K[y]$ і тому їх можна не розрізняти. Т.ч., в записі (2) будь-якого многочлена x можна розглядати як символ, замість якого можна підставляти будь-який елемент, трансцендентний над K .

Формально і формулу (2) замість x можна підставляти будь-який елемент α із кільця K , або деякого його розширення S $f(\alpha) = a_0\alpha^0 + a_1\alpha + a_2\alpha^2 + \dots + a_n\alpha^n$ і виконувати всі зазначені в правій частині операції над елементами кільця K або S . В результаті одержимо елемент $f(\alpha)$ кільця K або S . Цей елемент називається значенням многочлена $f(x)$ при $x = \alpha$.

Т.ч., поряд з алгебраїчним трактуванням многочлена над K як елемента деякого простого трансцендентного розширення кільця K . Ми мо-

жемо розглядати многочлен над K як відображення кільця (або його розширення S) в кільце K (або S), тобто, розглядати його як функцію.

У зв'язку з двома трактуваннями многочлена (алгебраїчним і функціональним) приходить розрізняти 2 види рівності многочленів – алгебраїчну і функціональну.

Як зазначалося зразу після означення 2, 2 многочлени рівні тоді і тільки тоді, коли їх коефіцієнти при однакових степенях невідомого рівні. Це алгебраїчне розуміння рівності двох многочленів. Якщо ми розглянемо многочлени як функції, то рівність двох многочленів треба розуміти як рівність функцій, тобто, многочлени $f(x)$ і $g(x)$ над кільцем K рівні тоді і тільки тоді, коли

$$(\forall x \in K, S): f(x) = g(x)$$

Це функціональне розуміння рівності двох многочленів. Якщо многочлени

$$f(x), g(x) \in K[x] \text{ рівні } f(x) = g(x) \quad (6)$$

в алгебраїчному розумінні, то вони рівні і в функціональному розумінні: $(\forall \alpha \in S \supset K): f(\alpha) = g(\alpha)$; бо над α зліва і справа у формулі (6) виконуються одні і ті ж операції в однаковому порядку.

§3.5. МНОГОЧЛЕНИ НАД ПОЛЕМ

Досі ми розглядали кільце многочленів над областю цілісності K .

Тепер будемо вимагати, щоб область цілісності K була полем, тобто щоб в K для довільного $a_0 \neq 0$ існував обернений елемент a^{-1} , або щоб

$$\forall_{a,b \in K} \left[a \neq 0 \Rightarrow \exists_{a \in K} \left[c = a^{-1} \cdot b = \frac{b}{a} \right] \right].$$

Отже в подальшому будемо розглядати многочлени над полем P .

Однак було б помилково думати, що у випадку, коли кільце над яким розглядаються многочлени, є полем P , то й кільце многочленів $P[x]$ виявиться полем. Більш того для кожного многочлена ненульового степеня з $P[x]$ не існує оберненого елемента. Дійсно,

$$\forall f(x) \in P[x] : \deg f \geq 1, \text{ рівність } f(x) \cdot g(x)$$

неможлива ні при якому $g(x) \in P[x]$, адже $g(x)$ не може бути нуль-многочленом і тому

$$\deg f \cdot g = \deg f + \deg g \geq 1, \text{ звідки } f(x) \cdot g(x) \neq 1.$$

Однак для многочленів нульового степеня, які є елементами поля P , то для кожного з них обернений елемент в $P[x]$ існує і є також многочленом нульового степеня.

§3.6. КІЛЬЦЕ МНОГОЧЛЕНІВ ЯК ЕВКЛІДОВЕ КІЛЬЦЕ

Почнемо з означення.

Означення 5. Область цілісності K з одиницею називається евклідовим кільцем, якщо існує відображення φ множини відмінних від 0 елементів цієї області цілісності в множину цілих невід'ємних чисел N^0 , тобто це $\varphi: K \setminus \{0\} \rightarrow N^0$, яке задовольняє таку вимогу: для будь-яких елементів $a, b \in K, b \neq 0$ в K існують такі елементи q і r , що $a = bq + r$, при чому $r = 0$, або $\varphi(r) < \varphi(b)$.

Приклад. В кільці Z – відображення φ задане так:

$$\forall_{a \in Z, a \neq 0} [\varphi(a) = |a|].$$

Щоб довести, що кільце $P[x]$ многочленів над полем P є евклідовим, потрібно, згідно з означення евклідового кільця, показати, що:

1. $P[x]$ є область цілісності.
2. Існує відображення $\varphi: P[x] \setminus 0 \rightarrow N^0 = N \cup \{0\}$ таке, що має місце ділення з остачею, тобто

$$(\forall f, g \in P) (\exists s(x), r(x) \in P[x]) : (f(x) = g(x) \cdot s(x) + r(x))$$

причому або $r(x) = 0$ або $\varphi(r(x)) < \varphi(g(x))$

Той факт, що $P[x]$ – область цілісності було доведено раніше.

Відображення $\varphi: P[x] \setminus 0 \rightarrow N^0$ побудуємо так. Кожному многочлену відмінному від нуля поставимо у відповідність його степінь, тобто

$$\varphi(f(x)) = \deg f \in N^0.$$

Залишається довести здійсненність ділення з остачею в кільці $P[x]$.

Тобто, слід показати, що для довільних многочленів $f(x)$ і $g(x) \neq 0$ з кільця $P[x]$ існують многочлени $s(x)$ і $r(x)$ такі, що $f(x)$ можна подати у вигляді $f(x) = g(x) \cdot s(x) + r(x)$, де $r(x) = 0$ або $\deg r(x) < \deg g(x)$.

Теорема 3.3: Довільний многочлен $f(x)$ з кільця $P[x]$ ділиться з остачею на будь-який многочлен $g(x)$ з цього кільця, відмінний від нуль-многочлена; при цьому часта і остача також належить до $P[x]$ і визначаються однозначно.

Доведення: Існування (можливість). Нехай

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

а) $f(x) = 0$, то $s(x) = 0$, $r(x) = 0$.

б) Нехай тепер $n = \deg f < \deg g = m$, тоді $s(x) = 0$, $r(x) = f(x)$;

в) Нехай $n \geq m$.

Виконаємо доведення індукцією по n .

1. Нехай $n = 0$ тоді $m = 0$

$$f(x) = a_0, \quad g(x) = b_0 \neq 0 \quad s(x) = \frac{a_0}{b_0}, \quad r(x) = 0.$$

Очевидно, що $s(x) \in P[x]$, бо $\frac{a_0}{b_0} \in P$.

2. Припустимо, що теорема справедлива для всіх многочленів таких, що $\deg f < n$, і доведемо її для многочленів степеня n .

Розглянемо многочлен

$$P(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x), \quad a_n \neq 0 \quad b_m \neq 0.$$

Тому $\deg P < n$ і за припущенням індукції $P(x)$ можна поділити з остачею на $g(x)$:

$$P(x) = g(x) \cdot s_1(x) + r_1(x), \quad s_1(x), r_1(x) \in P[x],$$

$$r_1(x) = 0 \text{ або } \deg r_1 < \deg g.$$

$$\text{Отже } f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = g(x) \cdot s_1(x) + r_1(x).$$

$$\text{Звідки } f(x) = g(x) \cdot s(x) + r(x), \text{ де } r(x) = r_1(x), \quad s(x) = s_1(x) + \frac{a_n}{b_m} x^{n-m}.$$

Зрозуміло, що $s(x), r(x) \in P[x]$ і, що $r(x) = 0$, або $\deg r(x) = \deg r_1 < \deg g$.

Щоб закінчити доведення слід встановити єдиність частки $s(x)$ і остачі $r(x)$.

Припустимо, що $f(x) = g(x) \cdot s(x) + r(x)$, $\deg r < \deg g$.

$$f(x) = g(x) \cdot s_1(x) + r_1(x), \deg r_1 < \deg g.$$

Потрібно довести, що

$$g(x)(s(x) - s_1(x)) = r(x) - r_1(x).$$

За умовою $g(x) \neq 0$. Якщо припустити, що $r(x) \neq r_1(x)$ то і $s(x) \neq s_1(x)$, але тоді

$$\deg g(x) \cdot \deg(s(x) - s_1(x)) = \deg g + \deg(s - s_1) > \deg(r - r_1) \text{ суперечність}$$

Як наслідок, маємо.

Теорема 3.4. Кільце многочленів над полем P є евклідове кільце $P[x]$.

Зауваження 3.1. У кільці $K[x]$, де K – область цілісності, але не поле, ділення з остачею, взагалі кажучи нездійсненне.

Так в кільці $Z[x]$. $f(x) = x^2 + 1$, $g(x) = 3x - 1$ многочленів $s(x)$ та $r(x)$ не існує.

Приклад:

$$f(x) = x^4 - 2x^3 = x - 1, \quad g(x) = x^2 - 1,$$

$$f, g \in Q[x].$$

Знайти $s(x)$ і $r(x)$.

§3.7. СХЕМА ГОРНЕРА. РОЗКЛАД МНОГОЧЛЕНА $F(x)$ ЗА СТЕПЕНЯМИ $x - \alpha$

Однак попередній приклад можна було розв'язати, за методом невідзначених коефіцієнтів. Дійсно

$$x^4 - 2x^3 = x - 1 = (x^2 - 2)s(x) = r(x).$$

$$s(x) = A_2x^2 + A_1x + A_0, \quad r(x) = B_1x + B_0.$$

$$x^4 - 2x^3 + x - 1 = (x^2 - 2)(A_2x^2 + A_1x + A_0) + B_1x + B_0$$

$$\text{Звідси} \begin{cases} x^4 & A_2 = 1 & A_2 = 1 \\ x^3 & A_1 = -2 & A_1 = -2 \\ x^2 & -2A_2 + A_0 = 0 \Rightarrow & A_0 = 2 \\ x & -2A_1 + A_1 = 1 & B_1 = -3 \\ x^0 & -2A_0 + B_0 = 1 & B_0 = 3 \end{cases}$$

$$s(x) = x^2 - 2x = 2$$

$$r(x) = -3x + 3$$

Застосовуючи такий спосіб, для окремого але важливого випадку, коли $g(x) = x - \alpha$,

$$\begin{aligned} & a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \\ & = (x - \alpha)(A_{n-1} x^{n-1} + A_{n-2} x^{n-2} + \dots + A_1 x + A_0) + r \end{aligned}$$

$$\deg r = 0$$

$$\begin{array}{l} a_n = A_{n-1} \\ a_{n-1} = A_{n-2} - \alpha A_{n-1} \\ \text{Тоді} \dots\dots\dots \Rightarrow \\ a_1 = A_0 - \alpha A_1 \\ a_0 = r - \alpha A_0 \end{array} \left[\begin{array}{l} A_{n-1} = a_n \\ A_{n-2} = a_{n-1} + \alpha A_{n-1} \\ A_{n-3} = a_{n-2} + \alpha A_{n-2} \\ \dots\dots\dots \\ A_0 = a_1 + \alpha A_1 \end{array} \right. \quad r = a_0 + \alpha A_0$$

	a_n	a_{n-1}	a_{n-2}	a_{n-3}	...	a_1	a_0
α	a_n	$\underbrace{\alpha A_{n-1} + a_{n-1}}$	$\underbrace{\alpha A_{n-2} + a_{n-2}}$			$\underbrace{\alpha A_1 + a_1}$	$\underbrace{\alpha A_0 + a_0}$
	A_{n-1}	A_{n-2}	A_{n-3}			A_0	r

Зауваження. Ділення з остачею многочлена $f(x)$ на лінійний двочлен виду $x - \alpha$, здійснене і в кільці многочленів над будь-якою областю цілості K (що не є полем), $\alpha \in K$.

Приклад.

$$x^4 - 2x^2 + 2x - 1 \text{ на } x - 2$$

	1	0	-2	2	-1
2	1	$1 \cdot 2 + 0 = 2$	$2 \cdot 2 + (-2) = 2$	$2 \cdot 2 + 2 = 6$	$2 \cdot 6 + (-1) = 11$

$$s(x) = x^3 + 2x^2 + x + 4 \quad r(x) = 11.$$

Нехай $f(x)$ – многочлен n -го степеня над полем P , $\alpha \in P$.

$$f(x) = (x - \alpha) \cdot f_1(x) + c_0.$$

При $n > 1$ $f_1(x) = (x - \alpha) \cdot f_2(x) + c_1$.

$$f_2(x) = (x - \alpha) \cdot f_3(x) + c_2.$$

$$f_{n-1}(x) = (x - \alpha) \cdot f_n(x) + c_{n-1} \quad \deg f_n = 0 \quad f_n = c_n.$$

Виключаючи $f_{n-1}, f_{n-2}, \dots, f_2, f_1$, дістанемо

$$f(x) = c_n (x - \alpha)^n + c_{n-1} (x - \alpha)^{n-1} + \dots + c_1 (x - \alpha) + c_0.$$

Приклад: Знайти розклад многочлена

$$f(x) = x^5 - 3x^3 + x^2 - 2x + 1$$

За степенями $x - 1$

	1	0	-3	1	-2	1
1	1	1	-2	-1	-3	$\boxed{-2}$
1	1	2	0	-1	$\boxed{-4}$	
1	1	3	3	$\boxed{2}$		
1	1	4	$\boxed{7}$			
1	1	$\boxed{5}$				
1	$\boxed{1}$					

$$f(x) = (x-1)^5 = 5(x-1)^4 + 7(x-1)^3 + 2(x-1)^2 - 4(x-1) - 2.$$

§3.8. ПОДІЛЬНІСТЬ МНОГОЧЛЕНІВ. ІДЕАЛИ КІЛЬЦЯ $P[x]$

Означення 6. Кажуть що многочлен $f(x) \in P[x]$ ділиться на многочлен $g(x) \in P[x]$, $g(x) \neq 0$, якщо існує многочлен $s(x) \in P[x]$ такий що $f(x) = g(x) \cdot s(x)$ і пишуть $f(x) : g(x)$

Властивості подільності:

$$1. \quad f, g, h \in P[x] \quad [f(x) : g(x) \quad g(x) : h(x) \quad f(x) : h(x)].$$

$$2. \quad f, g, h \in P[x] \quad [f : h \quad g : h \quad (f \pm g) : h].$$

$$3. \quad f, h \in P \quad [f : h \quad g(x) \in P[x] \quad f(x)g(x) : h(x)].$$

$$4. \quad n, f_1(x), f_2(x), \dots, f_m(x) \in P[x] \quad f_1(x) : h \quad f_2(x) : h \quad \dots \quad f_m(x) : h$$

$$g_1(x), g_2(x), \dots, g_m(x) \in P[x] \quad [(f_1(x)g_1(x) + \dots + f_m(x)g_m(x)) : h(x)].$$

$$5. \quad f \in P[x], c \in P[x], c \neq 0 \quad [f(x) : c].$$

$$6. \quad f, g \in P[x], c \in P[x], c \neq 0 \quad [f(x) : g(x) \quad f(x) : cg(x)].$$

Означення 7. Два многочлени $f(x)$ і $g(x) \in P[x]$ називаються асоційованими, якщо вони відрізняються лише множником, який є відмінною від 0 константою:

$$f(x)=cg(x) \text{ або } g(x)=\frac{1}{c}f(x)=c'f(x).$$

Означення 8. Непорожня підмножина I многочленів $f(x) \in P[x]$ є ідеалом $P[x]$, якщо виконуються умови:

1. $f(x), \varphi(x) \in I \Rightarrow [f(x) - \varphi(x)] \in I$.
2. $f(x) \in I, g(x) \in P[x] \Rightarrow [f(x)g(x)] \in I$.

Серед ідеалів кільця особливу роль відіграють головні ідеали, кожний з яких породжений деяким елементом кільця.

У кільці з одиницею головний ідеал, породжений елементом f , складається з усіх елементів кільця, кратних f , і позначають $(f(x))$.

Якщо в області цілісності з одиницею усі ідеали – головні, то її називають кільцем головних ідеалів.

Покажемо, що $P[x]$ є кільцем головних ідеалів. Це твердження є наслідком теореми яка стверджує, що кожне евклідове кільце є кільцем головних ідеалів.

Проте доведемо цей факт, спираючись на теорему про ділення з остачею.

Теорема 3.5. Кільце $P[x]$ многочленів над довільним полем P є кільцем головних ідеалів.

Доведення. Як відомо головний, головний ідеал кільця $P[x]$ має вигляд $(f) = \{f(x)g(x)\}$, де $f(x)$ – фіксований, а $g(x)$ – довільний многочлен з $P[x]$ (оскільки $P[x]$ – кільце з одиницею).

Нам потрібно довести, що для довільного ідеалу I кільця $P[x]$ знайдеться многочлен $f(x)$ такий, що $I = (f(x))$.

Можливі 2 випадки:

1. $I = \{0\}$, тобто складається лише з нуль-многочлена, то твердження теореми вірне, бо тоді $I = (0)$ – головний ідеал, породжений нуль-многочленом.

2. Нехай $I \neq \{0\}$, тобто в I існують многочлени, відмінні від нуля. Позначимо через $f(x)$ якийсь многочлен найменшого степеня з I . Такий многочлен існує, бо степені многочленів – невід'ємні цілі числа, отже, в будь-якій сукупності многочленів є многочлени найменшого степеня. Оскільки $f(x) \in I$ і I – ідеал, то для довільного $g(x) \in P[x]$ маємо $f(x)g(x) \in I$ тобто $(f) \subset I$.

Залишається показати, що $(f) = I$, тобто будь-який многочлен $q(x)I$ можна подати у вигляді $q(x) = f(x) \cdot s(x)$, де $s(x) \in P[x]$.

Дійсно, поділимо $q(x)$ на $f(x)$ з остачею маємо $q(x) = f(x) \cdot s(x) + r(x)$, де $\deg r(x) < \deg f(x)$ або $r(x) = 0$.

Оскільки $q(x)I \in f(x)I$ то і $r(x) = q(x) - f(x) \cdot s(x)I$.

Тепер маємо, $r(x)I \in f(x)I$ і $\deg r(x) < \deg f(x)$, але за умовою (за вибором) $\deg f(x)$ – найменший в I , а це можливо лише коли $r(x) = 0$.

Тоді $q(x) = f(x) \cdot s(x)$.

§3.9. НАЙБІЛЬШИЙ СПІЛЬНИЙ ДІЛЬНИК. АЛГОРИТМ ЕВКЛІДА

Означення 9. Якщо многочлен $d(x)$ є дільником многочлена $f(x)$ і многочлена $g(x)$, то він називається спільним дільником многочленів $f(x)$ і $g(x)$.

Означення 10. Спільний дільник многочленів $f(x)$ і $g(x)$, який ділиться на кожний інший спільний дільник цих многочленів, називається найбільшим спільним дільником многочленів $f(x)$ і $g(x)$ і позначають (f, g) .

Звичайно будь-які два многочлени мають тривіальні спільні дільники, а саме дільники одиниці кільця $P[x]$; такими дільниками є усі відмінні від 0 константи.

Якщо $d(x)$ – найбільший спільний дільник, то й кожний многочлен $cd(x)$, де c – елемент поля P , відмінний від нуля, також є НСД цих многочленів, проте з точністю до сталого множника найбільший спільний дільник визначається однозначно.

Дійсно, якщо $d(x)$ і $d_1(x)$ – НСД тоді $\{d(x) : d_1(x) \mid d(x)\} \Rightarrow d_1(x) \mid d(x)$ і $d(x)$ – асоційовані.

Означення 11. Многочлени $f(x)$ і $g(x) \in P[x]$ називаються взаємно простими, якщо їхній спільний дільник є многочленом нульового степеня (відмінного від нуля константою) або $(f, g) = 1$.

Розглянемо спосіб знаходження НСД двох многочленів.

Нехай $f(x), g(x) \in P[x], g(x) \neq 0$.

Нехай $\deg f(x) \geq \deg g(x)$.

Виконаємо послідовне ділення з остачею

$$f(x) = g(x)s_1(x) + r_1(x) \quad \deg r_1(x) < \deg g(x)$$

$$g(x) = r_1(x)s_2(x) + r_2(x) \quad \deg r_2(x) < \deg r_1(x)$$

$$r_1(x) = r_2(x)s_3(x) + r_3(x)$$

.....

$$r_{n-2}(x) = r_{n-1}(x)s_n(x) + r_n(x).$$

$$r_{n-1}(x) = r_n(x)s_{n+1}(x).$$

Якщо $\deg r_n(x) = 0$, то $r_{n-1}(x) = 0$ бо будь-який многочлен ділиться на многочлен нульового степеня.

Отже $r_n(x)$ – спільний дільник.

Легко показати, що $r_n(x)$ – НСД. Отже.

Теорема 3.6. Остання відмінна від нуля остача алгоритму Евкліда є НСД многочленів і $f(x)g(x)$.

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

Знайти (f, g) .

Теорема 3.7. Для будь-яких двох многочленів $f(x)$ і $g(x) \in P[x]$ існує НСД $d(x)$, причому $d(x)$ можна подати у вигляді

$$d(x) = f(x)u(x) + g(x)v(x),$$

де $u(x), v(x)$ – деякі многочлени.

Приклад. Попередній.

Наслідок. Многочлени $f, g \in P[x]$ взаємно прості тоді і тільки тоді, коли існують многочлени $u(x), v(x) \in P[x]$ такі, що: $f(x)u(x) + g(x)v(x) = 1$.

Властивості (що випливають із наслідку).

$$1. \quad f, g, h \in P[x] \left[(f, g) = 1 \wedge (f, h) = 1 \Rightarrow (f, g, h) = 1 \right].$$

$$2. \quad f, g, h \in P[x] \left[fg : h \wedge (f, h) = 1 \Rightarrow g(x) : h(x) \right].$$

$$3. \text{ }_{f,g,h} P[x] \left[f \div g \wedge f \div h \wedge (g,h)=1 \Rightarrow f \div gh \right].$$

Доведення теореми. З алгоритму Евкліда

$$d(x) = r_{n-2} - r_{n-1} s_n$$

$$r_{n-1} = r_{n-3} - r_{n-2} s_{n-1}$$

$$r_{n-2} = r_{n-4} - r_{n-3} s_{n+2}$$

.

і т. д. Підставивши послідовно одержимо

$$d = fu + gv.$$

§3.10. НАЙМЕНШЕ СПІЛЬНЕ КРАТНЕ МНОГОЧЛЕНІВ

Означення 12. Спільне кратне многочленів $f(x)$ і $g(x) \in P[x]$ називається будь-який многочлен $s(x) \in P[x]$ такий, що $s(x) \div f(x) \wedge s(x) \div g(x)$. Найменшим спільним кратним многочленів $f(x)$, $g(x)$ називають спільне кратне $f(x)$ і $g(x)$, яке ділить будь-яке інше спільне кратне цих многочленів; і позначається $[f(x); g(x)]$.

Теорема 3.8. Для будь-яких відмінних від нуля многочленів $f(x)$ і $g(x)$ найменше спільне кратне існує і визначається однозначно з точністю до сталого множника.

Доведення. Розглянемо многочлен $q(x) = \frac{f(x)g(x)}{(f,g)}$, де (f,g) – НСД.

Отже $q(x)$ – спільне кратне $f(x)$ і $g(x)$, бо $q(x) = \frac{f(x)}{(f,g)} g(x) = \frac{g(x)}{(f,g)} f(x)$.

Нехай тепер $s(x)$ – будь-яке інше СК, тоді $s(x) \div f$ і $s(x) \div g$, а тому

$s(x) = s_1(x) \cdot f(x)$, причому $\frac{s_1(x)f(x)}{g(x)} = p(x) \in P[x]$. Нехай тепер

$$f(x) = (f, g) f_1(x)$$

$$g(x) = (f, g) g_1(x)$$

де $f_1(x), g_1(x) \in P[x], (g_1(x), f_1(x)) = 1$.

Тоді $p(x) = \frac{s_1(x) f_1(x) (f, g)}{g_1(x) (f, g)} = \frac{s_1(x) f_1(x)}{g_1(x)}$ але $(f_1(x), g_1(x)) = 1$, то

$s_1(x) : g_1(x)$. Тобто $\frac{s_1(x)}{g_1(x)} = t(x) P[x], s_1(x) = g_1(x) t(x)$, тобто $s(x) = s_1(x) \cdot$

$$f(x) = f(x) g_1(x) t(x) = \frac{f(x) g_1(x) (f, g)}{(f, g)} t(x) = \frac{f(x) g(x)}{(f, g)} t(x) = q(x) t(x),$$

тобто $s(x) : q(x)$ – тобто $q(x)$ – НСК.

§3.11. НЕЗВІДНІ МНОГОЧЛЕНИ

Означення 13. Многочлен $f(x) \in P[x]$ називається незвідним над полем P , якщо він не є константою і не має дільників, відмінних від константи і від многочленів виду $cf(x)$, де c – константа.

Означення 13.* Многочлен $f(x) \in P[x]$ – незвідний у полі P , якщо $\deg f \geq 1$ і якщо з рівності $f(x) = g(x)s(x), g(x), s(x) \in P[x]$ випливає $\deg g = 0 \vee \deg s = 0$.

Означення 14. Многочлен $f(x) \in P[x]$ називається звідним у полі P коли $\deg f \geq 1$ і коли існують такі многочлени $g(x), s(x) \in P[x]$, що $f(x) = g(x)s(x)$, при чому $\deg g \geq 1$ і $\deg s \geq 1$.

Зауваження. Звідність чи незвідність многочлена залежить від поля P , над яким він розглядається.

Наприклад:

1. Многочлен $x^2 + 1$ незвідний у полі Q і в полі R . Однак цей многочлен звідний у полі C . Доведемо, що цей многочлен незвідний у полі R .

Припустимо супротивне, тобто

$$x^2 + 1 = (ax + b)(cx + d), a, b, c, d \in R. a \neq 0, c \neq 0.$$

Нехай $x = -\frac{b}{a}$, тоді $\left(-\frac{b}{a}\right)^2 + 1 = 0 \Rightarrow a^2 + b^2 = 0$ – що неможливо бо $a \neq 0$.

2. Многочлен $x^2 - 2$ незвідний у полі Q , але він звідний у полі $\{a + b\sqrt{2}, a, b \in Q\}$.

$$x^2 - 2 = (ax + b)(cx + d) \quad x = -\frac{b}{a}.$$

Теорема 3.9. Многочлен першого степеня над довільним полем P незвідний у цьому полі.

Доведення. $f(x) \in P[x]$ $\deg f(x) = 1$ $f(x) = g(x) \cdot s(x)$, $\deg g(x) = 1$, то $\deg s(x) = 0$ або навпаки.

Властивості незвідних многочленів.

1. Якщо $P(x)$ – многочлен, незвідний у даному полі, то і многочлен $cp(x)$, де c – довільна відмінна від нуля константа, незвідний у цьому полі.

2. Якщо $p(x)$ – незвідний у даному полі многочлен, а $f(x)$ – довільний многочлен над цим полем, то $f(x)$ ділиться на $P(x)$, або ці многочлени взаємно прості.

3. Якщо незвідний в даному полі многочлен $P(x)$ ділиться на інший незвідний многочлен у цьому полі многочлен $q(x)$, то ці многочлени збігаються з точністю сталого многочлена.

4. Якщо добуток многочленів $f(x)$ і $g(x)$ ділиться на незвідний многочлен $P(x)$, то хоча б один з цих множників ділиться на $P(x)$.

Дійсно, якщо $f(x) : p(x)$, $(f, p) = 1$, а тоді $g(x) : P(x)$.

Теорема 3.10. Кожний многочлен з кільця, степеня, розкладається в добуток незвідних многочленів $f(x)P[x] \geq 1$.

Дійсно якщо многочлен $f(x) \in P[x]$ сам незвідний, то вказаний добуток складається з одного многочлена. Якщо ж він, звідний, то може бути представлений у вигляді добутку многочленів меншого степеня.

Якщо серед цих многочленів знову є звідні многочлени, то проводимо?

1. $n=1$. $f(x)$ – представлений у вигляді добутку що складається з одного многочлена.

2. Нехай теорема справедлива при $n=k$.

3. Розглянемо випадок $\deg f(x) = k+1$.

а) Якщо $f(x)$ незвідний то добуток складається з одного множника.

б) Якщо звідний то за означенням $f(x) = g(x)s(x)$, де $\deg g(x) \geq 1$ і $\deg s(x) \geq 1$, крім того $\deg g(x) \leq n$ або $\deg f(x) \leq n$, то за пунктом 2, вони розкладаються в добуток незвідних множників.

Теорема 3.11. Якщо многочлен з кільця двома способами розкладається в добуток незвідних множників: $f(x)P[x]$.

$$f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_t(x) \quad (*)$$

то $s = t$ і, при відповідній нумерації, має місце рівність:

$$q_i(x) = c_i p_i(x), \quad i = 1, 2, \dots, s, \quad (***)$$

де c_i – відмінні від 0 елементи поля P .

Доведення. Ця теорема вірна для многочленів першого степеня, так як вони не звідні. Так як $q_1(x)$ є дільником $f(x)$, то в силу властивості 4) і рівності (*), $q_1(x)$ буде дільником хоча б одного з многочленів $P_i(x)$, наприклад $p_1(x)$. Так як, многочлен $p_1(x)$ незвідний, а степінь $q_1(x)$ більше нуля, то існує такий елемент c_1 , що

$$q_1(x) = c_1 p_1(x) \quad (**)$$

Підставляючи вираз для $q_1(x)$ в (*) і скорочуючи на $p_1(x)$, маємо ($P[x]$ – обл. цілісності)

$$p_2(x)\cdots p_s(x) = c_1 q_2(x)\cdots q_t(x).$$

Так як степінь цього многочлена, рівного цим добуткам, менше степеня $f(x)$, то згідно припущення (за методом математичної індукції), $s-1 = t-1$, звідки $s = t$, і що існують елементи $c_2', c_3', \dots, c_s'$, що

$$c_2 p_2(x) = c_1 q_2(x),$$

звідки

$$q_2(x) = (c_1^{-1} c_2') p_2(x) \text{ і } c_i p_i(x) = q_i(x), i = 3, \dots, s.$$

Показавши $c_1^{-1} c_2' = c_2$ і враховуючи (**), одержимо рівність.

Наслідок. Довільний многочлен ненульового степеня над полем P можна подати у вигляді $f(x) = [p_1(x)]^{k_1} [p_2(x)]^{k_2} \dots [p_m(x)]^{k_m}$, де $p_1(x), \dots, p_m(x)$ – полярно різні (неасоціативні) многочлени, незвідні у полі P . Це зображення єдине з точністю до сталих множників і нумерації.

Означення 15. Якщо многочлен $p_i(x)$ входить у канонічний розкладу степені з показником k_i , кажуть, що $p_i(x)$ є множителем кратності k_i многочлена $f(x)$. Множники, кратність яких більша за одиницю, називаються кратними множниками многочлена.

Означення 16. Незвідний многочлен $p_i(x)$ є множителем k_i -ї кратності многочлена $f(x)$, якщо ділиться на $f(x)[p_i(x)]^{k_i}$, але не ділиться на $[p_i(x)]^{k_{i+1}}$.

Теорема 3.12. Якщо многочлен і розкладені на незвідні множники в довільному полі P , то найбільший спільний дільник дорівнює добутку всіх незвідних множників, які входять у розклад як, так і. Якщо таких спільних незвідних многочленів немає, то $f(x)g(x)(f,g) f(x)g(x)(f,g) = 1$.

§3.12. КОРИНІ МНОГОЧЛЕНА

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ многочлен над полем P , а Δ будь-яке розширення поля P (зокрема може бути $\Delta = P$).

Як відомо, $\forall \alpha \in \Delta$ можна обчислити значення многочлена $f(x)$ при $x = \alpha$.

Означення 17. Корінь многочлена $f(x)$ многочлена $f(x) \in P[x]$ називається елемент α будь-якого розширення Δ поля P такий, що $f(\alpha) = 0$.

Корінь многочлена $f(x)$ називають таким нулем многочлена $f(x)$.

Теорема 3.13. Елемент $\alpha \in P$ є коренем многочлена $f(x) \in P[x]$ тоді і тільки тоді, коли лінійний двочлен $x - \alpha$ є дільником многочлена $f(x)$.

Доведення: За т. Безу остача від ділення на $x - \alpha$ дорівнює $f(\alpha)$. Отже, $f(x) : (x - \alpha)$ тоді і тільки тоді, коли $f(\alpha) = 0$ – тобто α -корінь.

Означення 18. Елемент $\alpha \in P$ називається коренем многочлена $f(x) \in P[x]$, якщо $f(x)$ ділиться на $x - \alpha$.

Означення 19. Елемент $\alpha \in P$ називається k -кратним коренем (коренем k -ї кратності) многочлена $f(x) \in P[x]$, якщо $f(x)$ ділиться на $(x - \alpha)^k$, але не ділиться на $(x - \alpha)^{k+1}$.

Теорема 3.14 (Кронекера). Для будь-якого многочлена $f(x)$, незвідного над полем P , існує таке розширення цього поля $\bar{P}$, в якому міститься корінь $f(x)$.

Доведення. Нехай маємо многочлен $f(x)$ степеня $n \geq 2$, незвідний над полем P . Потрібно побудувати розширення поля P , яке містить корінь для $f(x)$.

Для цього розіб'ємо кільце многочленів $P[x]$ на класи, відносячи до одного класу множники, що дають при діленні на многочлен $f(x)$ одна-

кові остачі. Тобто, многочлени $\varphi(x)$ і $\psi(x)$ відносяться до одного класу, якщо їх різниця ділиться на $f(x)$.

Позначимо ці класи $A, B, C, \dots$ Означимо суму і добуток цих класів так.

Виберемо з класів A і B по представнику $\varphi_1(x) \in A, \psi_1(x) \in B$ і позначимо через $\tau_1(x) = \varphi_1(x) + \psi_1(x)$.

$$\theta_1(x) = \varphi_1(x) \cdot \psi_1(x).$$

Виберемо тепер в класах A і B інші многочлени $\varphi_2(x) \in A, \psi_2(x) \in B$.

Тоді

$$\tau_2(x) = \varphi_2(x) + \psi_2(x),$$

$$\theta_2(x) = \varphi_2(x) \cdot \psi_2(x).$$

Оскільки $\varphi_1(x), \varphi_2(x) \in A$ тому $\varphi_1(x) - \varphi_2(x) : f(x)$ аналогічно $\psi_1(x) - \psi_2(x) : f(x)$. Тому

$$\begin{aligned} \tau_1(x) - \tau_2(x) &= [\varphi_1(x) + \psi_1(x)] - [\varphi_2(x) + \psi_2(x)] = \\ &= [\varphi_1(x) - \varphi_2(x)] + [\psi_1(x) - \psi_2(x)] : f(x). \end{aligned}$$

Аналогічно $\theta_1(x) - \theta_2(x) : f(x)$.

Отже $\tau_1(x)$ і $\tau_2(x)$ належать класу $A + B$, а θ_1 і $\theta_2 \in A * B$.

Крім того ми показали, що операції не залежать від вибору представників класів.

Покажемо, що сукупність класів, на які розбито нами кільце $P[x]$, з введеними в них операцій додавання і множення перетворюється в поле.

Дійсно, справедливість законів асоціативності і комутативності для обох операцій і закону дистрибутивності випливає з справедливості цих законів в кільці $P[x]$, оскільки операції над класами зводиться до операції над многочленами, що належать цим класам.

Роль нуля виконує очевидно клас, складений з многочленів, що діляться націло на $f(x)$. Цей клас назовемо нульовим.

Протилежним для класу A , що складається з многочленів, які дають при діленні на $f(x)$ остачу $\varphi(x)$, буде служити клас, складений з многочленів, які дають при діленні на $f(x)$ остачу $-\varphi(x)$.

Звідси випливає, що в множині класів виконується однозначно операція віднімання.

Покажемо, що в множині класів виконується операція ділення. Для цього покажемо, що існує клас, який виконує роль одиниці, а також для всякого ненульового класу існує обернений клас.

Одиницею буде клас E , який складений з многочленів, які дають при діленні на $f(x)$ остачу 1.

Нехай клас A – ненульовий. Многочлен $\varphi(x) \in A$, і $\varphi(x)$ не ділиться націло на $f(x)$, а оскільки $f(x)$ – незвідний, то $(f(x), \varphi(x)) = 1$.

А тому $\exists u(x), v(x) \in P[x]: \varphi(x) * u(x) + f(x) * v(x) = 1$ звідси

$$\varphi(x) * u(x) = 1 - f(x) * v(x).$$

З останньої нерівності слідує, що добуток многочленів $\varphi(x) * u(x)$ при діленні на $f(x)$ дає остачу 1.

Нехай $\varphi(x) \in A$, $u(x) \in B$, тоді $A * B = E \rightarrow B = A^{-1}$. Тобто існує клас для всякого ненульового класу.

Тобто сукупність класів – ПОЛЕ.

Позначимо це поле через $\bar{P}$ і покажемо що воно є розширенням поля P .

Кожному елементу a поля P відповідає клас, складений з многочленів, які дають при діленні на $f(x)$ остачу a ; сам елемент a , як многочлен нульового степеня належить цьому класу.

Всі класи цього виду складають в полі $\bar{P}$ підполе, ізоморфне полю P .

Дійсно, взаємна однозначність відповідності очевидна; з другого боку в цих класах можна вибрати як представниками елементи поля P , а тому сума (добуток) елементів поля P відповідає сумі (добуток) відповідних класів. Отже ми маємо право не відрізняти елементи поля P і відповідні їм класи.

Позначимо, через X – клас, які при діленні на $f(x)$ дають остачу x .

Покажемо що він є коренем для многочлена $f(x)$.

Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

Позначимо через A_i клас, $a_i \in A_i$, і знайдемо, чому дорівнює елемент (*) $A_n X^n + A_{n-1} X^{n-1} + \dots + A_1 X + A_0 \in \bar{P}$.

Вважаючи представників класів A_i елементи a_i , $i = 0, 1, \dots, n$, а представники класу X – многочлени x і використовуючи означення додавання і множення класів, ми одержимо, що в класі (*) міститься сам многочлен $f(x)$. Але $f(x)$ націло ділиться сам на себе, тому клас (*) – нульовий.

Таким чином замінивши в (*) класи A_i відповідними їм елементами $a_i \in P$, ми одержимо, що в полі $\bar{P}$ має місце рівність.

$a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 = 0$, тобто клас X є коренем многочлена $f(x)$.

Теорема 3.15. Для будь-якого многочлена $f(x) \in P[x]$ степеня $\deg f \geq 1$ існує таке розширення L поля P , в якому $f(x)$ розкладається на лінійні множники.

Тобто існує розширення L поля P , в якому степінь усіх незвідних множників многочленом $f(x)$ дорівнює 1.

Доведення. Нехай $\deg f = n$. За теоремою Кронекера існує розширення K_1 поля P , в якому $f(x)$ має корінь α_1 і тому може бути поданий у вигляді $f(x) = (x - \alpha_1) f_1(x)$, де $f_1(x) \in K_1[x]$, $\deg f_1 = n - 1$. Застосовуючи тепер теорему Кронекера до поля K_1 і многочлена $f_1(x)$ дістанемо розширення поля K_2 поля K_1 , в якому існує корінь α_2 многочлена $f_1(x)$. Зрозуміло, що α_2 є коренем $f(x)$, а K_2 – є розширенням поля P , в якому справедливий розклад $f(x) = (x - \alpha_1)(x - \alpha_2) f_2(x)$, $f_2(x) \in K_2[x]$, $\deg f_2 = n - 2$.

Продовжуючи цей процес, дістанемо розширення $K_3, \dots, K_n$ поля P , корені $\alpha_3, \dots, \alpha_n$ і дільником $f_3(x) \dots f_n(x)$ многочлена $f(x)$, поки не дістанемо $\deg f_{n+1} = 0$, тобто $f_{n+1} = c \in K_n$. Поле K_n і є шуканим полем L , бо воно є розширенням поля P , в якому

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n).$$

Означення 20. Поле L , в якому многочлен $f(x)$ розкладається на лінійні множники, називають полем розкладу цього многочлена.

Наприклад.

$$f(x) = x^4 - 2 \in \mathbb{Q}[x].$$

Над полем $\mathbb{Q}$ многочлен $x^4 - 2$ є незвідним.

Над полем $\mathbb{Q}(\sqrt{2})$:

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}).$$

Над полем $\mathbb{R}$:

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x^2 + \sqrt{2}).$$

Над полем $\mathbb{C}$:

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Означення 21. Поле P називається алгебраїчно замкнутим, якщо воно є полем розкладу для будь-якого многочлена $f(x) \in P[x]$ ненульового степеня.

Наслідок. Многочлен $f(x) \in P[x]$ n -го степеня має полі розкладу n -коренів.

Наслідок. У полі розкладу многочлена $f(x) = a_n x^n + \dots + a_1 x + a_0$ має канонічний розклад виду

$$f(x) = a_n (x - \alpha_1)^{k_1} (x - \alpha_2)^{k_2} \dots (x - \alpha_m)^{k_m}$$

$$k_1 + k_2 + \dots + k_m = n,$$

де $\alpha_1, \alpha_2, \dots, \alpha_m$ – різні корені многочлена.

Теорема 3.16 (Вієта). Якщо $\alpha_1, \alpha_2, \dots, \alpha_m$ – корені многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in P[x],$$

то

$$\alpha_1, \alpha_2, \dots, \alpha_n = \frac{a_{n-1}}{a_n}$$

$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \dots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n}$$

.....

$$\sum_{C_n^k} \alpha_{j_1} \alpha_{j_2} \dots \alpha_{j_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

.....

$$\alpha_1 \alpha_2 \dots \alpha_{n-1} \alpha_n = (-1)^k \frac{a_0}{a_n}$$

$\sum_{C_n^k}$ – сума по всіх C_n^k комбінаціях з n індексів $1, 2, \dots$, по k .

Для доведення формул досить виконати множення у правій частині

$$a_n x^n + a_{n-1} x^{n-1} \dots + a_1 x + a_0 = a_n (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

звести подібні члени і прирівняти коефіцієнти при однакових степенях x в обох частинах.

Ці співвідношення називаються формулами Вієта.

§3.13. ПОХІДНА ВІД МНОГОЧЛЕНА. ВІДОКРЕМЛЕННЯ КРАТНИХ МНОЖНИКІВ

Означення 22. Похідною від многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} \dots + a_1 x + a_0$$

називається многочлен

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$$

Похідну від многочлена ненульового степеня, а також похідну від нуль-многочлена беруть рівною нулю.

Безпосередньо з означення випливає, що похідна від многочлена над полем P є знову многочлен над полем P .

Будемо вважати, що P є поле характеристики 0. При цій умові

$$\deg f'(x) = \deg f - 1.$$

У випадку поля скінченної характеристики $p \leq 1$ многочлен $g(x) = x^p$ має похідною нуль-многочлен.

Правила:

$$[f(x) + g(x)]' = f'(x) + g'(x),$$

$$[f(x)g(x)]' = f'(x)g(x) + f(x)g'(x),$$

$$[cf(x)]' = cf'(x), c = \text{const},$$

$$[f(x)^k]' = k[f(x)]^{k-1} f'(x), k \in N.$$

Раніше ми показали, що всякий многочлен над полем P можна єдиним способом надати у вигляді добутку многочленів нижчих степенів, незвідних у цьому полі:

$$f(x) = [p_1(x)]^{k_1} [p_2(x)]^{k_2} \dots [p_l(x)]^{k_l}. \quad (1)$$

Покажемо, що в деяких випадках можна розробити загальний метод розкладання многочлена на множники.

Виберемо у розкладі (1) ті незвідні множники $P_i(x)$, кратність яких k_i дорівнює одиниці, позначимо добуток цих множників через $\varphi_1(x)$:

$$\varphi_1(x) = p_{j_1}(x) p_{j_2}(x) \dots p_{j_r}(x).$$

Аналогічно, через $\varphi_3(x)$ позначимо добуток незвідних множників з розкладу (1), що мають кратність 3, і т.д.

Тоді розклад (1) можна записати у такому вигляді:

$$f(x) = \varphi_1(x) \varphi_2^2(x) \varphi_3^3(x) \dots \varphi_m^m(x),$$

або

$$f = \varphi_1, \varphi_2^2, \varphi_3^3, \dots, \varphi_m^m \quad (2)$$

(якщо множників кратності $k < m$ в розкладі (1) немає, вважають, що $\varphi_k = 1$).

Теорема 3.17. Якщо незвідний у даному полі P характеристики 0 многочлен $q(x)$ є множителем $k \geq 2$ для многочлена $f(x)$, то він є множ-

ником кратності $k - 1$ для похідної $f'(x)$. Якщо $q(x)$ є множником першої кратності многочлена $f(x)$, то він не входить у розклад похідної $f'(x)$ на незвідні множники.

Доведення.

$$f(x) = [q(x)]^k \varphi(x), (\varphi(x), q(x)) = 1.$$

$$\begin{aligned} f'(x) &= k[q(x)]^{k-1} q'(x) \varphi(x) + [q(x)]^k \varphi'(x) = \\ &= [q(x)]^{k-1} [kq'(x) \varphi(x) + q(x) \varphi'(x)]. \end{aligned}$$

Звідки видно, що $f'(x) : [q(x)]^{k-1}$. Для того щоб довести, що $q(x)$ є для $f'(x)$ множником $(k - 1)$ -ї кратності, треба ще показати, що многочлен $\Psi(x) = kq'(x) \varphi(x) + q(x) \varphi'(x)$ не ділиться на $q(x)$. Якби $\Psi(x)$ ділився на $q(x)$, то й $q'(x) \varphi(x) = \frac{1}{k} [\Psi(x) - q(x) \varphi'(x)]$ ділився б на $q(x)$.

Оскільки $(\varphi(x), q(x)) = 1$, тоді $q'(x) : q(x)$, а це не можливо, бо $\deg q'(x) = \deg q$. Якщо кратність k множника $q(x)$ дорівнює 1, то дістанемо

$$f'(x) = q'(x) \varphi(x) + q(x) \varphi'(x).$$

З наведених вище міркувань видно, що $f'(x)$ на $q(x)$ не ділиться, що й означає, що в цьому разі $q(x)$ не входить у розклад $f'(x)$.

Наслідок. Для того щоб многочлен $f(x)$ не мав кратних множників, необхідно і достатньо, щоб $f(x)$ був взаємно простим із своєю похідною $f'(x)$.

Отже, як ми одержали, кожний многочлен у даному полі можна подати у вигляді

$$f = \varphi_1, \varphi_2^2, \varphi_3^3, \dots, \varphi_m^m.$$

Оскільки $\varphi_1(x)$ є добутком незвідних множників многочлена $f(x)$, які мають кратність $k - 1$, то в $f'(x)$ жодний з цих множників входити не буде. Отже

$$f' = \varphi_2, \varphi_3^2, \dots, \varphi_m^{m-1} \Psi_1,$$

де $\Psi_1 \dot{=} \varphi_1, \varphi_2, \dots, \varphi_m$.

$$\text{Тоді } d_1 = (f, f') = \varphi_2, \varphi_3^2, \dots, \varphi_m^{m-1}$$

$$d_1' = \varphi_3, \varphi_4^2, \dots, \varphi_m^{m-2} \Psi_2,$$

де $\Psi_2 \dot{=} \varphi_i$ ($i = 2, \dots, m$).

$$d_2 = (d_1, d_1') = \varphi_3, \varphi_4^2, \dots, \varphi_m^{m-2}.$$

Аналогічно

$$d_3 = (d_2, d_2') = \varphi_4, \varphi_5^2, \dots, \varphi_m^{m-3},$$

.....

$$d_{m-2} = (d_{m-3}, d_{m-3}') = \varphi_{m-1}, \varphi_m^2,$$

$$d_{m-1} = (d_{m-2}, d_{m-2}') = \varphi_m,$$

$$d_m = (d_{m-1}, d_{m-1}') = 1.$$

Поділимо f на d_1 , дістанемо

$$q_1 = \frac{f}{d_1} = \varphi_1, \varphi_2, \dots, \varphi_m,$$

$$q_2 = \frac{d_1}{d_2} = \varphi_2, \varphi_3, \dots, \varphi_m,$$

$$q_3 = \frac{d_2}{d_3} = \varphi_3, \varphi_4, \dots, \varphi_m,$$

.....

$$q_{m-1} = \frac{d_{m-2}}{d_{m-1}} = \varphi_{m-1}, \varphi_m,$$

$$q_m = \frac{d_{m-1}}{d_m} = \varphi_m.$$

На кінець

$$\varphi_1 = \frac{a_1}{q_2}; \varphi_2 = \frac{a_2}{q_3}; \dots; \varphi_{m-1} = \frac{a_{m-1}}{q_m}; \varphi_m = q_m.$$

Висновок. У довільного многочлена над полем P можна відокремити кратні множники за допомогою скінченного числа раціональних дій над деякими многочленами.

Приклад. Відокремити кратні множники многочлена

$$f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4.$$

Теорема 3.18. Для того, щоб був коренем кратності k многочлена, необхідно і достатньо, щоб $\alpha f(x)$

$$f(\alpha) = f'(\alpha) = \dots f^{(k-1)}(\alpha) = 0; f^{(k)}(\alpha) \neq 0. \quad (*)$$

Доведення. Необхідність. Нехай α є коренем $f(x)$ кратності k . Це означає, що $x - \alpha$ є незвідним множником k -ї кратності многочлена $f(x)$.

Але тоді, попередньою теоремою, $(x - \alpha)$ є незвідним множником похідної $f'(x)$ кратності $k - 1$.

Аналогічно, α є коренем $(k - 2)$ -ї кратності многочлена $f''(x)$ і т.д. Нарешті $f^{(k-1)}(x)$ має $(x - \alpha)$ своїм множником кратності 1, а $f^{(k)}(x)$ цього множника не має зовсім, тобто за наслідком теореми Безу $f^{(k)}(\alpha) \neq 0$.

Достатність. Нехай виконується умова (*). Тоді α є коренем многочлена $f(x)$.

Позначимо кратність цього кореня через l і покажемо, що $l = k$. З доведеного вище випливає

$$f(\alpha) = f'(\alpha) = \dots = f^{(l-1)}(\alpha) = 0; f^{(l)}(\alpha) \neq 0. \quad (**)$$

Якби $l < k$, то з (*) $\Rightarrow f^{(l)}(\alpha) = 0$, що суперечить (**). Аналогічно відкидаємо припущення $l > k$. Отже $l = k$.

Приклад 4.2. $f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$, $x = 2$ кратність кореня $x = 2$ дорівнює двом.

Розділ IV

КІЛЬЦЕ МНОГОЧЛЕНІВ ВІД КІЛЬКОХ ЗМІННИХ

§4.1. ПОБУДОВА КІЛЬЦЯ МНОГОЧЛЕНІВ

Нехай R^1 – область цілісності з одиницею, а $R[x_1]$ – сукупність многочленів від однієї змінної x над R^1 .

Як відомо $K[x_1]$ – область цілісності з одиницею.

Отже ми можемо побудувати кільце многочленів над $K[x_1]$ від однієї змінної x_2 , тобто сукупність.

Усіх многочленів виду:

$$a_n(x_1)x_2^n + a_{n-1}(x_1)x_2^{n-1} + \dots + a_0(x_1), \quad (1)$$

де

$$a_0(x_1) = a_{m_0,0}x_1^{m_0} + a_{m_0-1,0}x_1^{m_0-1} + \dots + a_{10}x_1 + a_{00}, \quad (2)$$

.....

$$a_0(x_1) = a_{m_n,n}x_1^{m_n} + \dots + a_{1,n}x_1 + a_{0n}.$$

Згідно доведеної теореми кільце $K[x_1][x_2]$ є область цілісності.

Підставляючи в (2) в (1) дістанемо вираз

$$\sum_{j=0}^n \sum_{i=0}^{m_j} a_{ij} x_1^i x_2^j, \quad a_{ij} \in K.$$

Тобто якусь скінченну сукупність членів виду $a_{\mu\nu} x_1^\mu x_2^\nu$, де $a_{\mu\nu} \in K$, а μ і ν – якісь невід'ємні цілі числа.

Навпаки, будь-яку скінченну суму виду

$$\sum_{\mu,\nu} a_{\mu\nu} x_1^\mu x_2^\nu \quad (3)$$

можна розглядати як елемент кільця $K[x_1][x_2]$. Будемо позначати його $K[x_1, x_2]$

Наприклад:

$$\phi(xy) = 3x^2y - 5xy^3 + x^7 - 1 + x^2y^3 + 2y - 7xy^2.$$

Як многочлен над $Q[x]$

$$\phi(xy) = 7xy^2 + (x^2 - 5x)y^3 + (3x^2 + 2)y + (x^7 - 1).$$

Означення 1. Кільцем многочлена $K[x_1, x_2, \dots, x_{n-1}, x_n]$ від n змінних $x_1, x_2, \dots, x_{n-1}, x_n$ над областю цілісності K називається кільце многочленів від змінної x_n над кільцем $K[x_1, x_2, \dots, x_{n-1}]$.

$$\text{Тобто } K[x_1, x_2, \dots, x_{n-1}, x_n] = (K[x_1, x_2, \dots, x_{n-1}])[x_n].$$

Теорема 4.1. Кільце многочленів $K[x_1, x_2, \dots, x_n]$ над областю цілісності K є областю цілісності.

Теорема 4.2. Кожний елемент $\phi \in K[x_1, x_2, \dots, x_n]$ можна подати у вигляді

$$\phi = \sum_{i=1}^n A_i x_1^{k_{1i}} x_2^{k_{2i}} \dots x_n^{k_{ni}}, \quad A_i \in K, K_{ij} \in \mathbb{Z}_+, \quad (4)$$

$$i = 1, 2, \dots, n, j = 1, 2, \dots, n.$$

Навпаки, будь-який вираз виду (4) є елементи кільця $K[x_1, x_2, \dots, x_n]$.

Означення 2. Кожний елемент кільця $K[x_1, x_2, \dots, x_n]$ називають многочленом від n змінних $x_1, x_2, \dots, x_n$ над K і позначають $\int[x_1, x_2, \dots, x_n]$.

§4.2. РІЗНІ ФОРМИ ЗОБРАЖЕННЯ МНОГОЧЛЕНІВ

При записі многочлена $f(x_1, x_2, \dots, x_n)$ у формі (4) ми завжди вважаємо, що серед членів многочлена немає подібних. Тому форму многочлена будемо називати його канонічною або нормальною.

Теорема 4.3. Будь-який многочлен $f(x_1, x_2, \dots, x_n) \in R(x_1, \dots, x_n)$ можна подати в канонічній формі лише єдиним способом (з точністю до порядку членів) [11, с. 274].

Означення 3. Степенем члена $Ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ многочлена називається сума $k_1 + k_2 + \dots + k_n$.

Число k_i ($i = 1, 2, \dots, n$) називають степенем даного члена відносно x_i . Найбільший із степенів членів називається степенем многочлена, а член з найбільшим степенем називається старшим членом многочлена.

Означення 4. Якщо всі одночлени (члени) многочлена мають той самий повний степінь l , то многочлен називається однорідним многочленом (формою) степеня l .

Очевидно, що будь-який многочлен можна подати як суму скінченного числа однорідних многочленів різни степенів.

§4.3. ЛЕКСИКОГРАФІЧНЕ ВПОРЯДКУВАННЯ ЧЛЕНІВ МНОГОЧЛЕНА

Враховуючи зручність однозначного впорядкування членів при вивченні многочленів бажано ввести якусь іншу характеристику членів многочлена так, щоб для членів, які не є подібними. Ця характеристика завжди була неоднаковою.

Розглянемо будь-які два члени многочлена

$$T_1 = Ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}. \quad (1)$$

$$T_2 = Bx_1^{l_1}x_2^{l_2}\dots x_n^{l_n}. \quad (2)$$

Якщо ці члени не подібні, то не всі відповідні степені k_1 і l_1 рівні між собою, тобто існує принаймні одне таке натуральне число p ($1 \leq p \leq n$), що $k_i = l_i$ ($i = 1, 2, \dots, p-1$), але $k_p \neq l_p$.

Якщо $k_p > l_p$, то член (1) називається вищим, ніж член (2).

Якщо $k_p < l_p$, то член (1) називається нижчим, ніж член (2); це рівнозначно тому, що (2) – вищий ніж член (1).

Лема 4.1. Вищий член добутку двох многочленів дорівнює добутку вищих членів цих многочленів.

Доведення. Нехай

$$f(x_1, \dots, x_n) = Ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n} + Bx_1^{l_1} x_2^{l_2} \dots x_n^{l_n} + \dots + Dx_1^{m_1} x_2^{m_2} \dots x_n^{m_n},$$

$$g(x_1, x_2, \dots, x_n) = \alpha x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} + Mx_1^{\beta_1} x_2^{\beta_2} \dots x_n^{\beta_n} + \dots + Kx_1^{\gamma_1} x_2^{\gamma_2} \dots x_n^{\gamma_n}.$$

Зауваження. Примноженні многочлена $f(x_1, \dots, x_n)$, на будь-який член виду $S = Cx_1^{\omega_1} x_2^{\omega_2} \dots x_n^{\omega_n}$ лексикографічне розміщення членів многочлена очевидно не порушується.

Утворимо добуток $f \cdot g$ помноживши спочатку f на перший член многочлена g , потім на другий член і т. д.

Отже кожна група членів буде розміщено лексикографічно.

Тому вищий член усього добутку слід шукати лише серед вищих членів цих окремих груп, тобто серед членів

$$L Ax_1^{\alpha_1+k_1} x_2^{\alpha_2+k_2} \dots x_n^{\alpha_n+k_n}; M Ax_1^{\beta_1+k_1} x_2^{\beta_2+k_2} \dots x_n^{\beta_n+k_n}; \dots; K Ax_1^{\gamma_1+k_1} x_2^{\gamma_2+k_2} \dots x_n^{\gamma_n+k_n}.$$

Але ці члени записані тут у такому порядку, в якому їх дістанемо при множенні многочлена g , розміщеного лексикографічно, на члени $Ax_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$.

Тому вищий серед них буде той, який утворено при множенні вищого члена g , тобто члени $L Ax_1^{\alpha_1+k_1} x_2^{\alpha_2+k_2} \dots x_n^{\alpha_n+k_n}$, що і треба було довести.

§4.4. СИМЕТРИЧНІ МНОГОЧЛЕНИ. ОЗНАЧЕННЯ І ЕЛЕМЕНТАРНІ ВЛАСТИВОСТІ

Означення 5. Многочлен $f(x_1, x_2, \dots, x_n)$ називається симетричним відносно змінних $x_1, x_2, \dots, x_n$, якщо внаслідок довільної перестановки змінних $x_1, x_2, \dots, x_n$ утворюється многочлен, який дорівнює даному.

$$x_1^2 + x_2^2, x_1x_2^2 + x_1^2x_2.$$

Означення 6. Симетричні многочлени

$$\sigma_1 = x_1 + x_2 + \dots + x_n,$$

$$\sigma_2 = x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n,$$

...

$$\sigma_n = x_1x_2 \dots x_n$$

будемо називати основними симетричними функціями.

Властивості.

1. Сума, різниця, добуток симетричних многочленів над деяким полем P є знову симетричними многочленами над цим полем.
2. Якщо симетричний многочлен містить деякий член

$$x_1^{e_1}, x_2^{e_2}, \dots, x_n^{e_n}$$

то він містить і член, утворений з нього внаслідок довільної перестановки показників.

Лема 4.2. Якщо $A x_1^{e_1}, x_2^{e_2}, x_3^{e_3}, \dots, x_n^{e_n}$ вищий член симетричного многочлена, то $e_1 \geq e_2 \geq \dots \geq e_n$.

Доведення. Нехай

$$A x_1^{e_1}, x_2^{e_2}, x_3^{e_3}, \dots, x_n^{e_n} \tag{1}$$

вищий член симетричного многочлена. Симетричний многочлен f містить і такі доданки

$$A x_2^{e_2}, x_1^{e_1}, x_3^{e_3}, \dots, x_n^{e_n}, \tag{2}$$

$$A x_1^{e_1}, x_3^{e_3}, x_2^{e_2}, \dots, x_n^{e_n} \quad (3)$$

вище (2) то $e_1 \geq e_2$.

вище (3) то $e_2 \geq e_3$.

Лему доведено.

Лема 4.3. Нехай

$$A x_1^{e_1}, x_2^{e_2}, \dots, x_n^{e_n} \quad (1)$$

вищий член деякого симетричного многочлена. Тоді вищий член добутку основних симетричних многочленів $A \sigma_1^{e_1-e_2} \sigma_2^{e_2-e_3} \dots \sigma_{n-1}^{e_{n-1}-e_n} \sigma_n^{e_n}$ співпадають.

Доведення. Дійсно, як відомо вищий член добутку симетричних многочленів добутку вищих членів цих многочленів.

$$A x_1^{e_1-e_2} (x_1 x_2)^{e_2-e_3} (x_1 x_1 x_1)^{e_3-e_3} \dots (x_1 x_2 \dots x_{n-1})^{e_{n-1}-e_n} (x_1 x_2 \dots x_n)^{e_n},$$

$$A x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}.$$

§4.5. ОСНОВНА ТЕОРЕМА ТЕОРІЇ СИМЕТРИЧНИХ МНОГОЧЛЕНІВ

Теорема 4.5. Всякий симетричний многочлен від n змінних над полем P можна подати у вигляді $f(x_1 x_2 \dots x_n)$ многочлена від елементарних симетричних многочленів $\sigma_1 \sigma_2 \dots \sigma_n$ причому коефіцієнти цього многочлена належать тому самому полю P .

Зауваження 2.1. Усіх членів певного степеня l може бути лише скінчене число, яке дорівнює числу способів, якими l можна подати як суму n невід'ємних цілих упорядкованих доданків.

Наприклад. При $l = 5$

$$5 = 0 + 5, 5 = 1 + 4, 5 = 2 + 3, 5 = 3 + 2, 5 = 4 + 1, 5 = 5 + 0.$$

Зауваження 2.2. Теорему досить довести для однорідних симетричних многочленів, оскільки кожний симетричний многочлен можна подати як суму однорідних симетричних многочленів.

Доведення. Нехай вищий член однорідного симетричного многочлена $f(x_1x_2\dots x_n)$ має степінь N і дорівнює

$$A x_1^{e_1} x_2^{e_2} \dots x_n^{e_n}. \quad (1)$$

Побудуємо симетричний многочлен

$$g(x_1x_2\dots x_n) = A \sigma_1^{e_1-e_2} \sigma_2^{e_2-e_3} \dots \sigma_{n-1}^{e_{n-1}-e_n} \sigma_n^{e_n}.$$

Згідно леми 2, вищий член цього многочлена дорівнює (1).

Крім того, він однорідний, бо такими є многочлени $\sigma_1\sigma_2\dots\sigma_n$.

Степінь многочлена g степеню многочлена f , бо в них однакові вищі члени.

Розглянемо

$$f_1(x_1x_2\dots x_n) = f(x_1x_2\dots x_n) - g(x_1x_2\dots x_n).$$

Многочлен $f_1(x_1x_2\dots x_n)$ – також однорідний симетричний многочлен степеня N .

Але f_1 вже не містить усіх членів цього степеня. Дійсно він не містить члена (1), який у цій різниці знищується. Крім цього, в цій різниці знищуються всі різні члени, одержані перестановками показників.

Тобто f_1 містить лише члени нижчі за (1).

Нехай вищий член многочлена f_1 має вигляд

$$B x_1^{m_1} x_2^{m_2} \dots x_n^{m_n}. \quad (2)$$

Позначимо через

$$g_1(x_1x_2\dots x_n) = B \sigma_1^{m_1-m_2} \sigma_2^{m_2-m_3} \dots \sigma_{n-1}^{m_{n-1}-m_n} \sigma_n^{m_n}$$

і утворимо різницю

$$f_2(x_1x_2\dots x_n) = f_1(x_1x_2\dots x_n) - g_1(x_1x_2\dots x_n),$$

f_2 – симетричний многочлен і однорідний степеня N , який не містить членів (1) та (2), а тільки нижчі.

Оскільки різних членів степеня N може бути лише скінчене число, то на якомусь кроці ми одержимо, що різниця

$$f_k(x_1x_2\dots x_n) - g_k(x_1x_2\dots x_n) = 0.$$

Не може містити жодного члена степеня N .

Тоді

$$f_1 = f - g,$$

$$f_2 = f_1 - g_1,$$

...

$$f_{k-1} = f_k - g_k,$$

$$0 = f_k - g_k,$$

$$\sum_{i=1}^k f_i = f + \sum_{i=1}^k f_i - g_1 - g_2 - \dots - g_k,$$

$$f = g_1 + g_2 + \dots + g_k.$$

Тобто $f(x_1 \dots x_n) = \varphi(\sigma_1 \sigma_2 \dots \sigma_n)$.

Коефіцієнти многочлена φ знайдено з коефіцієнтів даного многочлена за допомогою операції додавання і, а тому належать полю P .

Теорема 4.6. Зображення симетричного многочлена у вигляді многочлена від основних симетричних функцій єдине [11].

Теорема 4.7. Якщо $g(x)$ – многочлен від однієї змінної над полем P з коренями $\alpha_1, \alpha_2, \dots, \alpha_n$ (які можуть не належати полю P), то довільний симетричний многочлен $f(x_1 x_2 \dots x_n)$ над полем P при $x_1 = \alpha_1, x_2 = \alpha_2, \dots, x_n = \alpha_n$ набуває значення, яке є елементом поля P .

Доведення. Дійсно згідно теореми 4.5

$$f(x_1 x_2 \dots x_n) = g(\sigma_1 \sigma_2 \dots \sigma_n),$$

$$\sigma_1 = x_1 + x_2 + \dots + x_n,$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n,$$

...

$$\sigma_n = x_1 x_2 + \dots + x_n.$$

Нехай $g(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$, $\alpha_1, \alpha_2, \dots, \alpha_n$ його корені, тоді за теоремою Вієта

$$\left\{ \begin{array}{l} \sigma_1(\alpha_1 \dots \alpha_n) = \alpha_1 + \alpha_2 + \dots + \alpha_n = -\frac{a_{n-1}}{a_n} \\ \sigma_2 = \alpha_1 \alpha_2 + \dots + \alpha_{n-1} \alpha_n = \frac{a_{n-2}}{a_n} \\ \dots \\ \sigma_n = \alpha_1 \alpha_2 \dots \alpha_n = (-1)^n \frac{a_0}{a_n} \end{array} \right.$$

$$f(\alpha_1 \alpha_2 \dots \alpha_n) = g\left(-\frac{a_{n-1}}{a_n}, \frac{a_{n-2}}{a_n}, \dots, (-1)^n \frac{a_0}{a_n}\right) \in P.$$

Приклад. Обчислити значення симетричного многочлена $f(x_1 x_2 x_3) = x_1 + x_2 + x_3^4$ якщо x_1, x_2, x_3 корені многочлена $y = x^3 + x^2 - 2x - 5$.

§4.6. ОСНОВНА ТЕОРЕМА ТЕОРІЇ МНОГОЧЛЕНІВ

Лема 4.4. Якщо при $x = x_0$ многочлен $f(x)$ степеня $n \geq 1$, не обертається в нуль, $f(x_0) \neq 0$ і тому $|f(x_0)| > 0$, то можна знайти такий приріст h , ($h \in C$), що $|f(x_0 + h)| < |f(x_0)|$.

Доведення. Нехай $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ нехай $f(x_0) \neq 0$. Розкладемо f по степеням $x - x_0$:

$$f(x) = c_0 + c_1(x - x_0) + \dots + c_n(x - x_0)^n, \quad (1)$$

де $c_i \in C$, $c_0 = f(x_0) \neq 0$, $c_n \neq 0$.

Покладемо $z = x - x_0$

$$g(z) = c_0 + c_1 z + \dots + c_n z^n. \quad (2)$$

Нехай C_m - не нульовий коефіцієнт многочлена g з найменшим додатнім індексом ($0 \leq m \leq n$); тоді

$$f(x_0 + z) = g(z) = c_0 + c_m z^m + c_{m+1} z^{m+1} + \dots + c_n z^n. \quad (3)$$

Позначимо t

$$h(z) = \{c_{m+1} z + \dots + c_n z^{n-m-1}, m < n\} \quad (4)$$

$$0, m = n.$$

Тоді (3) можна записати так

$$g(z) = c_0 + c_m z^m + z^{m+1} h(z). \quad (5)$$

В силу (1) $\frac{c_0}{c_m} \neq 0$. Позначимо через d який-небудь з коренів m -го степеня з числа $(-\frac{c_0}{c_m})$

$$d^m = -\frac{c_0}{c_m}. \quad (6)$$

Покладемо в (5)

$$z = \lambda d, \text{ де } 0 < \lambda < 1, \lambda \in R. \quad (7)$$

Тоді з (5) в силу (6) маємо

$$g(\lambda d) = c_0 - c_0 \lambda^m + \lambda^{m+1} d^{m+1} h(\lambda d),$$

$$g(\lambda d) = c_0 \left[1 - \lambda^m + \lambda^{m+1} d^{m+1} \frac{1}{c_0} h(\lambda d) \right]. \quad (8)$$

З (4), домноживши на d^{m+1} , маємо $d^{m+1} h(\lambda d) = c_{m+1} d^{m+1} + \dots + c_n d^n \lambda^{n-m-1}$

$$(m < n); \text{ і } \left| \frac{d^{m+1} h(\lambda d)}{c_0} \right| \leq \frac{|c_{m+1} d^{m+1}| + \dots + |c_n d^n|}{|c_0|} \quad (m < n). \text{ Покладемо тепер}$$

$$B = \frac{|c_{m+1} d^{m+1}| + \dots + |c_n d^n|}{|c_0|}, \quad m < n \quad (9)$$

$$0, m = n.$$

Причому, при $m < n$, $B > 0$ оскільки $c_n \neq 0, Id \neq 0$.

$$\text{З (8) і (9)} \Rightarrow |g(\lambda d)| = |c| |1 - \lambda^m + \lambda^{m+1} B| = |c_0| \left[1 - \lambda^m (1 - \lambda B) \right].$$

Нехай $0 < \lambda < 1$, $\lambda B < 1$, тоді $g(\lambda d) < c_0$.

Але $c_0 = f(x_0)$ і в силу (3) $g(\lambda d) = f(x_0 + \lambda d)$.

Тоді $|f(x_0 + \lambda d)| < |f(x_0)|$, якщо $\{0 < \lambda < \min \left\{ 1; \frac{1}{B} \right\}, m < n, 0 < \lambda < 1,$

$m = n, h = \lambda d$. **Доведено!**

Теорема 4.8 (Гаусса). Довільний многочлен степеня $n \geq 1$ над полем комплексних чисел має принаймні один корінь, в загальному випадку – комплексний.

Доведення. Нехай f довільний многочлен степеня $n \geq 1$. Якщо $f(0) = 0$, то нуль є коренем многочлена f . Припустимо що $f(0) \neq 0$, і покладемо, що $|f(0)| = M$

Нехай r таке додатне число, що

$$(\forall x \in C) |x| \leq r \cdot |f(x)| \geq M.$$

Таке r існує в силу теореми про зростання модуля многочлена.

Нехай $K = \{x \in C : |x| \leq r\}$.

В силу попередньої теореми функція $|f(x)|$ досягає в K свого найменшого значення, тобто існує таке число $a \in K$, що (2) $|f(a)| \leq |f(x)|$ для всякого $x \in K : |x| \leq r_0$

В частості

$$|f(a)| \leq |f(x)| = M.$$

З (1) і (3) одержимо

$$(\forall x \in C) (|x| \leq r_0 \cdot |f(a)| \leq |f(x)|).$$

З (2) і (4) $\Rightarrow$

$$(\forall x \in C) (|f(a)| \leq |f(x)|).$$

Якщо $f(a) \neq 0$, то існує $c \in C$ таке, що $|f(c)| < |f(a)|$.

Однак нерівність протирічить (5), а тому

Випадок $f(a) \neq 0$ – неможливий.

Отже $f(a) = 0$, тобто a корінь многочлена f .

§4.7. НАСЛІДКИ З ОСНОВНОЇ ТЕОРЕМИ ТЕОРІЇ МНОГОЧЛЕНІВ

Теорема 4.9. Кожний многочлен, степінь якого вищий за одиницю, звідний у полі комплексних чисел.

Доведення. Нехай $f(x) \in C[x]$, і $\deg f(x) \geq 2$. За основною теоремою теорії многочленів існує хоча б один корінь x_0 цього многочлена.

За теоремою Безу (наслідок), $f(x)$ ділиться на $x - x_0$, тобто

$$f(x) = (x - x_0) f_1,$$

де $\deg f_1 \geq 1$, тобто $f_1(x)$ – многочлен ненульового степеня.

Наслідок. Для того щоб многочлен був незвідним у полі комплексних чисел, необхідно і досить, щоб його степінь дорівнював одиниці.

Теорема 4.10. Кожний многочлен n -го степеня над полем комплексних чисел єдиним способом розкладається на лінійні множники в цьому полі

$$f(x) = a_n (x - x_1)(x - x_2)(x - x_3) \dots (x - x_n),$$

де $x_1, x_2, x_3, \dots, x_n$ – корені, а a_n – старший коефіцієнт многочлена $f(x)$.

Доведення. Як було доведено раніше, кожен многочлен над полем C можна розкласти у добуток незвідних многочленів у цьому полі, причому ці многочлени визначаються однозначно з точністю до сталого множника:

$$f(x) = f_1(x) f_2(x) \dots f_m(x).$$

Але в полі комплексних чисел кожен незвідний многочлен має перший степінь. Отже, число множників $m = n$ і кожен з них є лінійним двочленом. Далі, оскільки $f_k(x)$ визначається з точністю до сталого множника, то будемо вважати, що в кожному з них старший коефіцієнт $= 1$, тобто $f_k(x) = x + \alpha_k$. Тоді $f(x) = A(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$.

Але, прирівнюючи старші коефіцієнти маємо $A = a_n$. Далі $-\alpha_1, -\alpha_2, \dots, -\alpha_n$ – корені многочлена, бо $f_k(-\alpha_k) = 0$. Позначимо їх через $x_1, x_2, \dots, x_n$. Отже,

$$f(x) = a_n(x - x_1)(x - x_2)(x - x_3) \dots (x - x_n).$$

Оскільки під числом коренів многочлена в даному полі розуміють число лінійних множників, то переконуємось у справедливості такого твердження.

Теорема 4.11. Многочлен n -го степеня над C має рівно n коренів з урахуванням їх кратностей.

Крім того, всі корені многочлена $f(x)$ над полем C належать C , тобто поле розкладу будь-якого многочлена $f(x)$ з комплексними коефіцієнтами є поле C комплексних чисел.

Висновок: поле C комплексних чисел є алгебраїчно замкнутим.

Теорема 4.12. Якщо комплексне число є коренем многочлена з дійсними коефіцієнтами x_0

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

то спряжене комплексне число $\overline{x_0}$ також є коренем цього многочлена.

Доведення. Обчислимо значення $f(x_0)$. Відокремивши дійсну та уявну частини, маємо:

$$f(x_0) = a_n x_0^n + a_{n-1} x_0^{n-1} + \dots + a_1 x_0 + a_0 = A + Bi.$$

Обчислимо тепер $f(\overline{x_0})$. Через те, що всі $a_k \in R$, то $\overline{a_k} = a_k$ і тому

$$f(\overline{x_0}) = a_n \overline{x_0}^n + a_{n-1} \overline{x_0}^{n-1} + \dots + a_1 \overline{x_0} + a_0 = \overline{a_n x_0^n + \dots + a_1 x_0 + a_0} = \overline{f(x_0)} = A - Bi.$$

Але x_0 – корінь, отже $A + Bi = 0 \Rightarrow A = 0, B = 0$, отже $A - Bi = 0 \Rightarrow f(\overline{x_0}) = 0$.

Теорема 4.13. Якщо комплексне число x_0 є коренем k -ої кратності ($k > 1$) многочлена з дійсними коефіцієнтами $f(x)$, то спряжене комплексне число $\overline{x_0}$ є коренем многочлена $f(x)$ тієї ж кратності k .

Доведення. Оскільки x_0 – корінь кратності k , то

$$f(x_0) = f'(x_0) = \dots = f^{(k-1)}(x_0) = 0, f^{(k)}(x_0) \neq 0.$$

Тоді згідно теореми 4.9

$$f(\overline{x_0}) = f'(\overline{x_0}) = \dots = f^{(k-1)}(\overline{x_0}) = 0.$$

З другого боку, $f^{(k)}(\overline{x_0}) \neq 0$, бо в противному разі за теоремою 4.9, число x_0 також було б коренем $f^{(k)}(x_0)$.

$$\text{Отже, } f(\overline{x_0}) = f'(\overline{x_0}) = \dots = f^{(k-1)}(\overline{x_0}) = 0, f^{(k)}(\overline{x_0}) \neq 0.$$

Теорема 4.14. Кожний многочлен над полем R , степінь якого перевищує 2, є звідним у цьому полі.

Доведення. Нехай $\deg f(x) > 2$. Нехай x_0 – корінь цього многочлена.

а) $x_0 \in R$, тоді за теоремою Безу

$$f(x) = (x - x_0)f_1(x), f_1(x) \in R[x]$$

і є многочленом ненульового степеня, отже, $f(x)$ – звідний у полі R .

б) якщо x_0 – комплексне число, то за теоремою 4.12 $\overline{x_0}$ – також корінь. Тому

$$f(x) = (x - x_0)(x - \overline{x_0})f_1(x).$$

Розглянемо $\varphi(x) = (x - x_0)(x - \overline{x_0}) = x^2 - (x_0 + \overline{x_0})x + x_0\overline{x_0}$, але $x_0 + \overline{x_0} \in R$, $x_0\overline{x_0} \in R$.

Отже, $f(x) \in R[x] : \varphi(x) \in R[x]$, а тому їх частка f_1 також є многочленом над R .

Теорема 4.15. Кожний многочлен над полем дійсних чисел допускає єдиний розклад на незвідні множники в цьому полі виду: $f(x)$

$$f(x) = a_n(x - x_1)^{k_1}(x - x_2)^{k_2} \dots (x - x_l)^{k_l} (x^2 + p_{l+1}x + q_{l+1})^{k_{l+1}} \dots (x^2 + p_mx + q_m)^{k_m}$$

[11, с. 321]

Зауваження. Будь-яке алгебраїчне рівняння з раціональними коефіцієнтами множенням на спільний знаменник усіх коефіцієнтів можна звести до рівняння з цілими коефіцієнтами.

Наприклад:

$$1/3x^2 + 1/2x^2 + x - 2/3 = 0, x \in Q,$$

$$2x^3 + 3x^2 + 6x - 4 = 0.$$

Означення 7. Многочлен $P(x)$ з цілими коефіцієнтами називається примітивним, якщо його коефіцієнти не мають спільних дільників, відмінних від ± 1 .

Лема 4.5. Добуток двох примітивних многочленів є примітивним многочленом.

Доведення. Нехай $f(x), g(x)$ – примітивні многочлени,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a,$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b.$$

Припустимо, що многочлен $g(x) = f(x)g(x)$ не є примітивним. Нехай p один із дільників на які діляться коефіцієнти $g(x)$. Всі коефіцієнти a_i ($i = 0, 1, \dots, n$) не можуть ділитися на p , бо $f(x)$ – примітивна.

Нехай k – найменший з індексів a_i , що не діляться на p .

Аналогічно, нехай l – найменший з індексів b_i , що не ділиться на p .

Розглянемо коефіцієнт $C_{k+l} = \sum a_i b_j$.

В цій сумі лише один з доданків $a_k b_l$ не ділиться на p , а отже C_{k+l} не ділиться на p , що суперечить припущенню.

Розглянемо тепер питання про звідність многочлена з цілими коефіцієнтами у полі раціональних чисел.

Теорема 4.16. Для того щоб многочлен $f(x)$ з цілими коефіцієнтами був звідним у полі Q раціональних чисел, необхідно і достатньо, щоб він був звідним у кільці Z цілих чисел, тобто щоб існували многочлени $f_1(x)$ і $f_2(x)$ ненульового степеня з цілими коефіцієнтами такі, що

$$f(x) = f_1(x) \cdot f_2(x).$$

Доведення. Необхідність. Нехай $f(x) \in Z[x]$, звідний у полі раціональних чисел, тобто $f(x) = g_1(x) \cdot g_2(x)$, $\deg g_1(x) \neq 0$, $\deg g_2(x) \neq 0$, де $g_1(x), g_2(x)$ – многочлени з раціональними коефіцієнтами.

Ми повинні довести, що існують многочлени ненульового степеня $f_1(x), f_2(x)$ з цілими коефіцієнтами добуток яких дорівнює $f(x)$.

Нехай після зведення коефіцієнтів до спільного знаменника і винесення цього знаменника за дужки многочлен $g_1(x)$ має вигляд: $g_1(x) = \alpha/\beta S_1(x)$, де $S_1(x)$ – многочлен з цілими коефіцієнтами, β – спільний знаменник коефіцієнтів, а α – НСД коефіцієнтів многочлена $g_1(x)$ після зведення до спільного знаменника.

Зрозуміло, що $S_1(x)$ – примітивний многочлен. Можна вважати, що $(\alpha, \beta) = 1$.

Аналогічно $g_2(x) = \gamma/\delta S_2(x)$, де $S_2(x)$ – примітивний многочлен, а $(\gamma, \delta) = 1$.

Отже, $f(x) = \alpha\gamma/\beta\delta S_1(x) S_2(x)$.

Достатність. Доведемо, що $\alpha\gamma/\beta\delta$ – ціле число. Дійсно, припустимо що $\alpha\gamma/\beta\delta = p/q$, $(p, q) = 1$.

Добуток $S_1(x) \cdot S_2(x) = S(x)$ за лемою примітивний многочлен. Нехай c_k – якийсь коефіцієнт $S(x)$. Добуток $c_k \cdot p/q$ має бути цілим числом для будь-якого k , бо $f(x) = p/q \cdot S(x)$ має цілі коефіцієнти. Але $(p, q) = 1$, тому $c_k: q$ для будь-якого k . Отже, $S(x)$ – не примітивний многочлен. Отже, $\alpha\gamma/\beta\delta = t \in \mathbb{Z}$. Поклавши $f_1(x) = t S_1(x)$, $f_2(x) = t S_2(x)$, одержимо $f(x) = f_1(x) \cdot f_2(x)$, $f_1(x), f_2(x) \in \mathbb{Z}[x]$.

Теорема 4.17. Якщо в многочлені з цілими коефіцієнтами $f(x) = a_n x^n + \dots + a_1 x + a_0$ коефіцієнти $a_0, a_1, \dots, a_{n-1}$ діляться на просте число p , причому a_0 не ділиться на p^2 , а старший коефіцієнт a_n не ділиться на p , то многочлен $f(x)$ незвідний у полі раціональних чисел.

Доведення. Згідно з теоремою 4.16 досить показати, що $f(x)$ при цих умовах не може бути добутком двох многочленів ненульового степеня з цілими коефіцієнтами. Припустимо супротивне

$$f(x) = (b_r x^r + b_{r-1} x^{r-1} + \dots + b_1 x + b_0)(c_s x^s + c_{s-1} x^{s-1} + \dots + c_1 x + c_0) \quad (r + s = n).$$

Нехай $r \geq s$

$$a_0 = b_0 c_0 \Rightarrow a_0 \not\vdots p^2, b_0 \vdots p, c_0 \not\vdots p$$

$$a_1 = b_1 c_0 + b_0 c_1$$

.....

$$a_r = b_r c_0 + b_{r-1} c_1 + \dots + b_{r-s} c_s$$

.....

$$a_n = b_r c_s \Rightarrow a_n \div p,$$

що неможливо.

Основне значення теореми 2 в тому, що з неї випливає існування многочленів довільного степеня з цілими коефіцієнтами незвідних у полі раціональних чисел.

Теорема 4.18. У кільці многочленів над полем раціональних чисел є многочлени довільного степеня, незвідні у полі Q .

Теорема 4.19. Якщо многочлен $f(x)$ з раціональними коефіцієнтами, степінь якого більший за одиницю, має хоча б один раціональний корінь r , то $f(x)$ звідний у полі раціональних чисел.

Доведення:

$$r\text{-корінь} \Rightarrow f(x) = (x - r)f_1(x), \deg f_1(x) \geq 1.$$

Обернене твердження не вірне.

Теорема 4.20. Якщо многочлен третього степеня із раціональними коефіцієнтами не має раціональних коренів, то він незвідний у полі раціональних чисел.

Доведення: Припустимо супротивне.

Нехай $f(x) = f_1(x) \times f_2(x)$, f_1, f_2 – многочлени ненульового степеня із $Q[x]$. Оскільки $\deg f_1 + \deg f_2 = 3$, то степінь одного з них = 1, а другий – степінь = 2.

Нехай $\deg f_1(x) = 1$, тобто $f_1(x) = ax + b$, тоді $x = -b/a$ – раціональний корінь, а це суперечить умові.

§4.8. РАЦІОНАЛЬНІ КОРЕНІ МНОГОЧЛЕНІВ З РАЦІОНАЛЬНИМИ КОЕФІЦІЄНТАМИ

Можна вважати, що рівняння над полем Q завжди можна вважати рівнянням з цілими коефіцієнтами.

Теорема 4.21. Щоб число $\frac{q}{p}$, де q, p взаємно прості числа, було коренем рівняння $a_n x^n + \dots + a_1 x + a_0 = 0$ з цілими коефіцієнтами, необхідно, щоб p було дільником вільного члена a_0 , а q – дільником старшого коефіцієнта a_n цього рівняння.

Наслідок. Якщо старший коефіцієнт рівняння з цілими коефіцієнтами $=1$, то всі раціональні корені цього рівняння є цілими числами і дільником вільного члена.

Теорема 4.22. Для того, щоб p/q , де $(p, q) = 1$, було раціональних коренем многочлена з цілим коефіцієнтами $f(x) = a_n x^n + \dots + a_1 x + a_0$, необхідно, щоб при довільному цілому k число $f(k)$ ділиться на $p - q^k$ ($p - q^k \neq 0$).

Доведення. Поділимо $f(x)$ на $x - k$

$$f(x) = (x - k)(b_{n-1}x^{n-1} + \dots + b_1x + b_0) + \alpha(k),$$

$$b_{n-1}, \dots, b_1, b_0 \in Z.$$

Підставимо $x = \frac{p}{q}$ і врахуємо що $f(\frac{p}{q}) = 0$, маємо

$$-f(k) = (\frac{p}{q} - k) (b_{n-1}(\frac{p}{q})^{n-1} + \dots + b_1 \frac{p}{q} + b_0)$$

звідси

$$-q^n f(k) = (p - q^k) (b_{n-1}p^{n-1} + \dots + b_1 p q^{n-2} + b_0 q^{n-1}) \Rightarrow q^n f(k) : p - q^k.$$

Покажемо що q і $p - kq$ взаємно прості, припустимо супротивне $(q, p - kq) = \alpha$, $\alpha \neq 1 \Rightarrow (q, p) = \alpha$ що суперечить умові. Отже $(q, p - q^k) = 1$. Таким чином $f(k) : p - q^k$.

Наслідок. Якщо старший коефіцієнт a_n даного многочлена $f(x)$ з цілими коефіцієнтами $= 1$, то його раціональними коренями можуть бути лише такі цілі числа p для яких $f(k)$ ділиться на $p - k$ при всякому цілому k , при якому $p - k \neq 0$.

Дійсно, згідно Наслідку Т.6 при $a_n = 1$ маємо $q = 1$ звідки і випливає наше твердження.

Розділ V

АЛГЕБРАЇЧНІ РОЗШИРЕННЯ ЧИСЛОВИХ ПОЛІВ

§5.1. АЛГЕБРАЇЧНІ ЧИСЛА І СКІНЧЕННІ РОЗШИРЕННЯ ПОЛІВ

Означення 1. Число називається алгебраїчним, якщо воно є коренем деякого многочлена з раціональними коефіцієнтами.

Означення 2. Число α називається алгебраїчним відносно числового поля Δ , якщо воно є коренем деякого многочлена над полем Δ .

Число, яке не є алгебраїчним відносно поля Δ , називається трансцендентним відносно Δ .

Нехай α – корінь многочлена степеня n над полем Δ :

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0. \quad (1)$$

Будемо вважати, що многочлен $f(x)$ незвідний у полі Δ , бо в протилежному випадку можна було б розглянути той незвідний множник многочлена, який має α своїм коренем.

Якщо $g(x)$ – будь-який многочлен над полем Δ , коренем якого є α , то внаслідок незвідності $f(x)$ многочлен $g(x) = f(x)$, а тому має α степінь не нижче за n .

Якщо ж $g(x)$ – незвідний, то він збігається з $f(x)$ з точністю до сталого множника.

Отже, зведений многочлен $f(x)$ – єдиний незвідний многочлен над полем Δ , який має α своїм коренем, а його степінь n найнижчий серед степенів усіх многочленів з коренем α .

Означення 3. Зведений многочлен $f(x)$, незвідний у полі Δ , який має своїм коренем, називається мінімальним многочленом числа α , а його степінь n – степенем алгебраїчного числа відносно поля Δ .

Якщо α – число першого степеня відносно Δ , то $\alpha \in \Delta$. При $n > 1$ з незвідності $f(x)$ випливає, що $\alpha \in \Delta$.

Дійсно, якщо б $\alpha \in \Delta$, то подільність многочлена $f(x)$ на двочлен $x - \alpha$ означала б, що $f(x)$ звідний у полі Δ .

§5.2. ПРОСТЕ АЛГЕБРАЇЧНЕ РОЗШИРЕННЯ ПОЛЯ

Нехай Δ – деяке числове поле і α – число, яке не належить цьому полю.

Розглянемо мінімальне поле $P\{\Delta, \alpha\}$, яке містить і поле Δ і число α . Очевидно, $P\{\Delta, \alpha\}$, є розширенням поля Δ , яке містить число α .

Нехай α належить деякому надполю поля Δ . Мінімальне поле, що містить Δ і α , позначають $\Delta(\alpha)$; якщо $\alpha \notin \Delta$, це нетривіальне просте розширення.

Аналогічно можна розглянути розширення $\Delta(\alpha_1, \alpha_2, \dots, \alpha_n)$, утворене приєднанням кількох чисел $\alpha_1, \alpha_2, \dots, \alpha_n$, до поля Δ , тобто мінімальне поле $P\{\Delta, \alpha_1, \alpha_2, \dots, \alpha_n\}$.

Розширення, утворені приєднанням одного числа, часто називають простими.

Наприклад, поле $P\{a + b\sqrt{2}, a, b \in Q\}$ є простим алгебраїчним розширенням поля раціональних чисел, яке містить число $\sqrt{2}$.

Означення 4. Поле $\Delta(\alpha)$, утворене приєднанням до поля Δ числа α , алгебраїчного відносного поля Δ , називається простим алгебраїчним розширенням поля Δ .

Теорема 5.1. Поле $\Delta(\alpha)$, утворене з поля Δ приєднанням кореня α , незвідного у полі Δ многочлена n -го степеня

$$f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0, \quad (1)$$

складається з усіх чисел виду

$$\xi = c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1}, \quad (2)$$

де $c_0, c_1, \dots, c_{n-1}$ – довільні числа з поля Δ .

Доведення.

1. Покажемо, що числа виду (2) утворюють поле. Сума і різниця числа виду (2) – є числа того ж виду (очевидно). Розглянемо добуток і частку.

Нехай $\xi_1 \xi_2 = g_1(a)g_2(a) = g_a$, де $g(x)$ – многочлен. степінь якого може перевищувати $n - 1$.

Поділимо $g(x)$ на $f(x)$:

$$g(x) = f(x)\varphi(x) + \tau(x), \deg \tau(x) \leq n-1. \quad (3)$$

Підставляючи α в (3), і враховуючи, що $f(\alpha) = 0$, одержимо $g(\alpha) = \tau(\alpha)$, тобто $\xi_1 \xi_2 = \tau(\alpha)$, $\deg(\tau(x)) \leq n-1$, тобто число $\xi_1 \xi_2$ – виду (2).

Розглянемо частку. Досить показати, що для будь-якого числа $\xi = g(\alpha) \neq 0$ виду (2), число $\frac{1}{\xi}$ також буде числом виду (2). $f(x)$ – незвідний у полі Δ многочлен, $g(x)$ – або взаємно простий з $f(x)$, або ділиться на $f(x)$. Але $g(x)$ не може ділитися на $f(x)$, бо $\deg(g(x)) < \deg(f(x))$, а тому $(f(x), g(x)) = 1$. Тоді, як ми знаємо, існують, причому єдині, многочлени $\varphi(x)$ і $u(x)$, що має місце рівність $f(x)u(x) + g(x)\varphi(x) = 1$.

Показавши, $x = \alpha$, і враховуючи, що $f(\alpha) = 0$, одержимо $g(\alpha)\varphi(\alpha) = 1$, $\xi\varphi(\alpha) = 1$, $\frac{1}{\xi} = \varphi(\alpha)$.

Якщо многочлен $\varphi(x)$ має степінь менший за n , то твердження доведено.

Якщо $\deg(\varphi(x)) \geq n$, то $\varphi(x)$ та $f(x)$ з остачею, тобто $\varphi(x) = f(x)s(x) + \tau(x)$, звідси $\varphi(\alpha) = \tau(\alpha)$, де $\deg(\tau(x)) \leq n-1$. Тобто $\frac{1}{\xi}$ є числом виду (2). Отже числа виду (2) утворюють поле.

2. Позначимо його через Δ_1 .

Покажемо, що $\Delta_1 = \Delta(\alpha)$.

Оскільки $a \in \Delta$ і $\Delta < \Delta_1$, то $\Delta(a) \leq \Delta_1$

Навпаки, будь-яке поле, що включає a і поле Δ , повинно включати і всі числа виду (2), які утворюються з чисел поля Δ і числа a за допомогою дій множення і додавання. Тобто

$$\Delta(a) \geq \Delta_1$$

Тобто $\Delta_1 = \Delta(a)$

Наслідок. Якщо a – корінь многочлена другого степеня над полем Δ $f(x) = x^2 + px + \tau$, причому $a \notin \Delta$, то просте алгебраїчне розширення $\Delta(a)$ поля Δ , утворене приєднанням числа a , складається з усіх чисел виду $a + b\alpha$, де a, b – довільні числа з поля Δ .

Приклад

1. $Q(\sqrt{2})$.

2. $Q(\sqrt[3]{2})$.

3. $C = R(i)$.

Означення 5. Якщо α є коренем незвідного квадратного многочлена над Δ , то $\Delta(\alpha)$ є квадратичним розширенням поля Δ .

§5.3. АЛГЕБРАЇЧНІ РОЗШИРЕННЯ ПОЛЯ

Лема 5.1. Якщо Δ_2 – розширення поля Δ степеня m , а Δ_1 – довільне розширення Δ , що міститься в Δ_2 : $\Delta \subseteq \Delta_1 \subseteq \Delta_2$, то Δ_1 – також скінченне розширення Δ , причому його степінь $(\Delta_1 : \Delta)$ є дільником числа m .

Теорема 5.2. Складне алгебраїчне розширення $\Delta(\alpha_1)(\alpha_2)$ є скінченним розширенням поля Δ . Степінь цього розширення дорівнює добутку степеня розширення $\Delta(\alpha_1)$ відносно поля Δ на степінь розширення $\Delta(\alpha_1)(\alpha_2)$ відносно поля $\Delta(\alpha_1)$.

Доведення. Позначимо $\Delta_1 = \Delta(\alpha_1)$, $\Delta_2 = \Delta_1(\alpha_2)$. Тоді $\Delta \subseteq \Delta_1 \subseteq \Delta_2$. Обидва послідовні прості розширення є скінченними. Нехай $(\Delta_2 : \Delta_1) = n$. За формулою башти маємо

$$[\Delta_2 : \Delta] = [\Delta_2 : \Delta_1][\Delta_1 : \Delta] = mn.$$

Наслідок. Складне алгебраїчне розширення $\Delta(\alpha_1)(\alpha_2)\dots(\alpha_n)$ є скінченним розширенням поля Δ степінь цього розширення дорівнює добутку степенів усіх послідовних простих розширень.

Наслідок. Якщо $\Delta \subseteq \Delta_1 \subseteq \Delta_2 \subseteq \dots \subseteq \Delta_k$ є ланцюжок квадратичних розширень, то Δ_k є скінченним розширенням поля Δ степеня 2^k .

Теорема 5.3. Будь-яке скінченне розширення поля є його алгебраїчним розширенням.

Нехай Δ_1 – скінченне розширення n -го степеня поля Δ . Отже, Будь-які $n + 1$ елементів у полі Δ_1 є лінійно залежними відносно Δ . Тому якщо взяти в Δ_1 довільний елемент α і за його допомогою скласти $n + 1$ елементів $1, \alpha, \alpha^2, \dots, \alpha^n$, то ця система лінійно залежна відносно Δ , тобто існують такі $\lambda_i \in \Delta$, що $\lambda_0 + \lambda_1 \alpha + \dots + \lambda_n \alpha^n = 0$.

Отже, α – корінь многочлена $f(x) = \lambda_n x^n + \dots + \lambda_1 x + \lambda_0$ коефіцієнтами з поля Δ .

Теорема 5.4. Розширення $\Delta(\alpha_1, \alpha_2, \dots, \alpha_k)$, утворює з Δ приєднанням алгебраїчних відносно Δ чисел $\alpha_1, \alpha_2, \dots, \alpha_k$, збігається з складним алгебраїчним розширенням $\Delta(\alpha_1)(\alpha_2)\dots(\alpha_k)$

Доведення. Якщо побудувати послідовність $\Delta \subseteq \Delta_1 \subseteq \Delta_2 \subseteq \dots \subseteq \Delta_{k-1} \subseteq \Delta_k$, де $\Delta_1 = \Delta(\alpha_1)$, $\Delta_2 = \Delta(\alpha_2)$, ..., $\Delta_i = \Delta_{i-1}(\alpha_i)$, ..., $\Delta_k = \Delta_{k-1}(\alpha_k)$, то всі ці розширення є простими алгебраїчними розширеннями.

Справді, кожне α_i за умовою є алгебраїчним числом відносно поля Δ , а отже є алгебраїчним відносно розширення Δ_{i-1} цього поля. Тому $\Delta_i = \Delta_{i-1}(\alpha_i)$ є простим алгебраїчним розширенням. Розглянемо поле $\Delta_k = \Delta(\alpha_1)(\alpha_2)\dots(\alpha_k)$. Згідно теореми про будову простого алгебраїчного розширення, всі елементи цього поля є якісь многочлени над полем Δ від елементів $\alpha_1, \alpha_2, \dots, \alpha_k$.

Тим самим це поле має бути підполем поля $\Delta(\alpha_1, \alpha_2, \dots, \alpha_k)$, тобто $\Delta_k \subseteq \Delta(\alpha_1, \alpha_2, \dots, \alpha_k)$.

З другого боку, поле $\Delta(a_1, a_2, \dots, a_k)$ мінімальне з тих, що містять $\Delta, a_1, \dots, a_k$ і тому, $\Delta_k \supseteq \Delta(a_1, a_2, \dots, a_k)$.

Отже $\Delta(a_1, \dots, a_k) = \Delta(a_1)(a_2) \dots (a_k)$.

Теорема 5.5. Будь-яке скінченне розширення поля Δ є складним алгебраїчним розширенням [11].

Теорема 5.6. Будь-яке складне алгебраїчне розширення $\Omega = \Delta(a_1)(a_2) \dots (a_k)$ поля Δ є простим розширенням цього поля, тобто існує таке число ω , алгебраїчне відносно Δ , де $\Omega = \Delta(\omega)$.

Доведення. Застосуємо метод математичної індукції і розглянемо випадок $k = 2$. У цьому випадку $\Omega = \Delta(a_1)(a_2)$. Треба знайти ω , алгебраїчне відносно Δ , що $\Omega = \Delta(\omega)$.

Оскільки α_1 і α_2 алгебраїчні відносно Δ , то можна розглядати їх мінімальні многочлени $f(x)$ і $g(x)$ над полем Δ .

Нехай $\xi_1, \xi_2, \dots, \xi_n$ – корені $f(x)$, $\eta_1, \eta_2, \dots, \eta_m$ – корені $g(x)$

Очевидно, що всі числа $\xi_1, \dots, \xi_n$, попарно різні, бо в іншому випадку многочлен $f(x)$ був би звідним.

Нехай $\xi_1 = 2$, а $\eta_1 = \alpha_2$. Утворене число $\omega = \alpha_1 + c\alpha_2$, де c – деяке число з поля Δ , яке ми виберемо так, щоб для будь-якого $i = 1, 2, \dots, n$ і $j = 2, 3, \dots, m$,

$$\omega \neq \xi_i + \eta_j.$$

Такий вибір завжди можна зробити, бо числове поле Δ має безліч елементів а чисел

$$\alpha_1 + c\alpha_2 = \xi_i + c\eta_j \Leftrightarrow c = \frac{\alpha_1 - \xi_i}{\eta_j - \alpha_2},$$

де $i = 1, 2, \dots, n$; $j = 2, 3, \dots, m$ скінченна кількість.

Доведемо, що так означене число ω – шукане.

По перше, $\omega \in \Omega$ і тому алгебраїчне відносно Δ . Крім того $\Delta(\omega) = \Omega$. Покажемо, що $\Delta(\omega)$ містить кожне число з Ω , тобто $\Omega \subseteq \Delta(\omega)$.

Розглянемо многочлен $f_1(x) = f(\omega - cx)$.

Його коефіцієнти належать полю $\Delta(\omega)$, бо коефіцієнт многочлена $f(x)$ і c належить Δ ; $\omega \in \Delta(\omega)$. Серед коренів $f_1(x)$ число α_2 , бо $f_1(\alpha_2) = f(\omega - c\alpha_2) = f(\alpha_1) = 0$.

Отже, $f_1(x)$ та $g(x)$ мають спільний дільник корінь α_2 . Але ці многочлени не мають жодного іншого спільного кореня, бо

$$f(\eta_j) = 0 \ (j = 2, \dots, m) \Leftrightarrow f(\omega - c\eta_j) = 0 \ (j = 2, \dots, m) \Leftrightarrow$$

$$\omega - c\eta_j = \xi_i \ (i = 1, \dots, n; j = 2, \dots, m),$$

що суперечить умові

$$\omega \neq \xi_i + c\eta_j \ (i = 1, \dots, n; j = 2, \dots, m).$$

Отже НСД многочленів $f(x)$ та $g(x)$: $(f(x); g(x)) = x - \alpha_2$.

Оскільки $f(x)$ та $g(x)$ многочлени над полем $\Delta(\omega)$, яка є розширенням поля Δ , то і $x - \alpha_2$ – многочлен поля $\Delta(\omega)$, тобто $\alpha_2 \in \Delta(\omega)$.

Отже $\alpha_1 = \omega - c\alpha_2 \in \Delta(\omega)$.

Але тоді мінімальне поле $\Delta(\alpha_1, \alpha_2)$, яке містить поле Δ і числа α_1, α_2 можуть бути підполем $\Delta(\omega)$.

За теоремою 5.3

$$\Delta(\alpha_1, \alpha_2) = \Delta(\alpha_1), (\alpha_2) = \Omega.$$

Отже, $\Omega \leq \Delta(\omega)$, тобто при $k = 2$, $\Omega = \Delta(\omega)$.

Припустимо тепер, що теорема справедлива при $k = l \geq 2$ і доведемо справедливість її при $k = l + 1$.

Нехай $\Omega = \Delta(\alpha_1)(\alpha_2) \dots (\alpha_l)(\alpha_{l+1})$, де α_i ($i = 1, 2, \dots, l + 1$) – алгебраїчні відносно Δ числа. Розглянемо поле $\Omega_1 = \Delta(\alpha_1)(\alpha_2) \dots (\alpha_l)$. За припущенням індукції $\Omega = \Delta(\omega_1)$, де ω_1 – якесь алгебраїчне відносно Δ число.

Але тоді $\Omega = \Delta(\omega_1)(\alpha_{l+1})$ і, за твердженням теореми, Ω є просте алгебраїчне розширення поля Δ .

§5.4. ПОНЯТТЯ РОЗВ'ЯЗНОСТІ РІВНЯННЯ В КВАДРАТНИХ РАДИКАЛАХ

Означення 6. Кажуть, що рівняння

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0, (a_n \neq 0) \quad (1)$$

можна розв'язати в квадратних радикалах, якщо кожен з його n -коренів можна подати через коефіцієнти a_i ($i = 0, \dots, n$) за допомогою скінченного числа дій додавання, віднімання, множення, ділення та добування квадратного кореня.

Іншими словами, якщо його корені можна виразити через корені ланцюжка двочленних квадратних рівнянь:

$$x^2 - \alpha_0 = 0, \alpha_0 \in Q = \Delta_0;$$

$$x^2 - \alpha_1 = 0, \alpha_1 \in F_1 = F_0(\sqrt{\alpha_0});$$

$$x^2 - \alpha_2 = 0, \alpha_2 \in F_2 = F_0(\sqrt{\alpha_1});$$

.....

$$x^2 - \alpha_{k-1} = 0, \alpha_{k-1} \in F_{k-1} = F_{k-2}(\sqrt{\alpha_{k-2}}).$$

Таким чином, всі корені рівняння (1) раціонально виражаються через числа $\sqrt{\alpha_0}, \sqrt{\alpha_1}, \dots, \sqrt{\alpha_{k-1}}$ і належать полю $\Delta_k = \Delta_{k-1}(\sqrt{\alpha_{k-1}})$.

Отже, рівняння (1) розв'язане у квадратних радикалах, якщо існує зростаючий ланцюжок числових полів

$$\Delta_0 \subset \Delta_1 \subset \dots \subset \Delta_{k-1} \subset \Delta_k$$

такий, що кожне поле Δ_i ланцюжка є квадратним розширенням попереднього поля Δ_{i-1} і поле Δ_k містить всі корені рівняння (1).

§5.5. УМОВИ РОЗВ'ЯЗНОСТІ РІВНЯННЯ ТРЕТЬОГО СТЕПЕНЯ В КВАДРАТНИХ РАДИКАЛАХ

Теорема 5.7. Рівняння третього степеня $x^3 + ax^2 + bx + c = 0$ з раціональними коефіцієнтами розв'язне у квадратних радикалах тоді і тільки тоді, коли воно має хоча б один раціональний корінь.

Доведення. Нехай $f = x^3 + ax^2 + bx + c$ має хоча б один раціональний корінь, наприклад d , тоді $f(x) = (x - d)(x^2 + tx + n)$, $t, n \in Q$.

Тому рівняння розв'язне у квадратних радикалах.

Припустимо, що рівняння (1) розв'язне у квадратних радикалах не має раціональних коренів. Тоді існує ланцюжок квадратних розширень $Q = \Delta_0 \subset \Delta_1 \subset \dots \subset \Delta_{k-1} \subset \Delta_k$ таких, що хоча б один з квадратних коренів x_1, x_2, x_3 рівняння (1) міститься в $\Delta_k \setminus \Delta_{k-1}$, наприклад $x_1 \in \Delta_k \setminus \Delta_{k-1}$ і жоден з коренів не містився в Δ_{k-1} , тобто $\{x_1, x_2, x_3\} \cap \Delta_{k-1} = \emptyset$ (*)

Поле Δ_k є квадратним розширенням поля Δ_{k-1} , тобто існує елемент $\alpha \in \Delta_k \setminus \Delta_{k-1}$, такий, що $\Delta_k = \Delta_{k-1}(\alpha)$, $\alpha \notin \Delta_{k-1}$, $\alpha^2 \in \Delta_{k-1}$.

Тоді, враховуючи теорему про будову простого алгебраїчного розширення, елемент x_1 має вигляд $x_1 = p + q\alpha$, $p, q \in \Delta_{k-1}$, $q \neq 0$.

Покажемо, що $p - q\alpha$ також є коренем нашого рівняння $f = 0$.

Дійсно:

$$f(p + q\alpha) = (p + q\alpha)^3 + a(p + q\alpha)^2 + b(p + q\alpha) + c,$$

$$(p + q\alpha)^3 + a(p + q\alpha)^2 + b(p + q\alpha) + c = A + B\alpha,$$

$$A = f(p) + 3pq^2\alpha^2 + aq^2, \alpha^2 \in \Delta_{k-1},$$

$$B = 3p^2q + q^3\alpha^2 + 2apq + bq \in \Delta_{k-1}.$$

Оскільки $A, B \in \Delta_{k-1}$, але $\alpha \notin \Delta_{k-1}$, з $A + B\alpha = 0$ випливає $A = B = 0$. Для $x_1 = p + q\alpha$ і $x_2 = p - q\alpha$ маємо $x_1 - x_2 = 2q\alpha \neq 0$.

Провівши аналогічні перетворення, одержимо $f(p - q\alpha) = A - B\alpha = 0$.

Отже, $p - q\alpha$ – також корінь многочлена f . Нехай це буде $x = p - q\alpha$.

Тоді $x_1 - x_2 = 2p\alpha \neq 0$, отже $x_1 \neq x_2$. Крім того $x_1 + x_2 = 2p \in \Delta_{k-1}$.

За Теоремою Вієта $x_1 + x_2 + x_3 = -a$.

Тому $x_3 = -a - 2p \in \Delta_{k-1}$, що суперечить припущенню (*).

Наслідок. Рівняння (1) з раціональними коефіцієнтами розв'язне у квадратних радикалах тоді і тільки тоді, коли многочлен $x^3 + ax^2 + bx + c$. Звідний в кільці $Q[x]$.

§5.6. ПРИКЛАДИ ЗАДАЧ, НЕРОЗВ'ЯЗНИХ В КВАДРАТНИХ РАДИКАЛАХ

Теорема 5.8. Для того, щоб число ξ ($\xi \in R, C$) було побудоване циркулем і лінійкою, виходячи з поля $\Delta \subset R$, необхідно і достатньо, щоб ξ виражалось у квадратних радикалах через числа поля Δ .

а) Задача про подвоєння куба.

Побудувати куб (ребро куба), об'єм якого вдвоє більший за об'єм даного куба.

a – ребро даного куба

x – ребро V_2 , то $V_2 = 2V_1 \Rightarrow x^3 = 2a^3$.

При $a = 1 \Rightarrow x^3 - 2 = 0$.

$\sqrt[3]{2} \notin Q$ – $x^3 - 2$ – незвідний у Q .

б) Трисекція кута. Поділити довільний кут на три рівні частини.

Нехай $x = \cos \frac{\varphi}{3}$, $a = \cos \varphi$.

$$\cos \varphi + i \sin \varphi = \left(\cos \frac{\varphi}{3} + i \sin \frac{\varphi}{3} \right)^3 =$$

$$= \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3} \sin^2 \frac{\varphi}{3} + i \left(\cos^2 \frac{\varphi}{3} \sin \frac{\varphi}{3} - \sin^3 \frac{\varphi}{3} \right).$$

Тоді

$$\cos \varphi = \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3} \sin^2 \frac{\varphi}{3} = \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3} (1 - \cos^2 \frac{\varphi}{3}).$$

$$4 \cos^3 \frac{\varphi}{3} - 3 \cos \frac{\varphi}{3} - \cos \varphi = 0.$$

Отже, $4x^3 - 3x - a = 0$.

При $\varphi = \pi/2$, $a = 0$, рівняння розв'язане в квадратних радикалах.

Якщо $\varphi = \pi/3$, то $a = \cos \pi/3 = 1/2$. Одержимо:

$$4x^3 - 3x - \frac{1}{2} = 0.$$

$$8x^3 - 6x - 1 = 0.$$

Поклавши $y = 2x$, маємо $y^3 - 3y - 1 = 0$ – рівняння нерозв'язне у квадратних радикалах.

в) Квадратура круга.

Побудувати квадрат рівновеликий даному кругу.

$$R = 1, S_{кр} = \Pi. \text{ Тоді } x^2 - \Pi = 0.$$

Π -трансцендентне, тобто не алгебраїчне. Трансцендентність числа π встановив у 1882 р. німецький математик Ліндеман.

г) Поділ кола. Побудова правильного многокутника.

$n = 7, 9, 11, 13$ $n = 7$. Побудувати правильний семикутник, вписаний в одиничне коло.

$$z^7 - 1 = 0, (z - 1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = 0.$$

Покажемо, що рівняння нерозв'язне в квадратних радикалах.

$$z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0: z^3.$$

$$z^3 + z^2 + z + 1 + 1/z + 1/z^2 + 1/z^3 = 0.$$

$$t = z + 1/z, t^2 = z^2 + 2 + 1/z^2, t^3 = z^3 + 3z + 3 * 1/z + 1/z^3.$$

$$(z^3 + 3(z + 1/z) + 1/z^3) + (z^2 + 1/z^2 + z) - 2(z + 1/z) - 1 = 0, t^3 + t^2 - 2t - 1 = 0.$$

Немає раціональних коренів, отже нерозв'язне в квадратних радикалах.

Розділ VI

ЕЛЕМЕНТИ СУЧАСНОЇ АЛГЕБРИ

Попередні розділи посібника були присвячені класичним алгебраїчним структурам: групам, кільцям, ідеалам, кільцям многочленів та алгебраїчним розширенням полів. У сучасній математиці ці поняття не залишаються суто теоретичними. Вони лежать в основі алгоритмів, що застосовуються в комп'ютерній алгебрі, криптографії, інформаційній безпеці, теорії кодування, цифровому підписі та технологіях розподілених реєстрів. Саме тому природним продовженням курсу є розгляд тих напрямів, у яких класична алгебра переходить у сферу алгоритмів і практичних застосувань.

У цьому розділі увагу зосереджено на трьох взаємопов'язаних сюжетах. По-перше, розглянуто ймовірнісні тести простоти, що дають змогу швидко відрізнити прості числа від складених, навіть коли йдеться про дуже великі числа. По-друге, показано, як прості числа, скінченні кільця лишків та циклічні групи використовуються в криптографічних протоколах, насамперед у системі RSA. По-третє, окреслено роль алгебраїчних ідей у цифровому підписі та блокчейн-системах. Такий добір матеріалу узгоджується з попередніми розділами посібника: поняття групи, кільця та поля тут не повторюються ізольовано, а виступають як робочі інструменти для побудови реальних алгоритмів [12].

На відміну від класичних теоретичних побудов, у сучасній алгебрі важливо не лише довести існування певного об'єкта, а й уміти обчислити його, перевірити його властивості та оцінити складність алгоритму. Через це зростає роль поняття ефективності: хороший алгоритм повинен працювати швидко навіть для чисел, які мають сотні або тисячі двійкових розрядів. Саме в цьому контексті прості числа, малі теореми теорії чисел, розклади елементів у групах і структура скінченних полів стають змістовною частиною сучасної алгебри, а не лише прикладами до абстрактних означень.

§6.1. ОБЧИСЛЮВАЛЬНА АЛГЕБРА І МІСЦЕ ПРОСТИХ ЧИСЕЛ

Термін «обчислювальна алгебра» вживають для позначення сукупності методів, у яких алгебраїчні структури вивчають не тільки з погляду їх загальних властивостей, а й з позицій побудови явних алгоритмів. Якщо в класичному курсі достатньо знати, що певна підгрупа існує або що заданий ідеал є головним, то в алгоритмічній постановці постає питання: як швидко знайти породжувальний елемент, як ефективно обчислити найбільший спільний дільник, як перевірити оборотність елемента в кільці лишків, як встановити простоту числа або як виконати операції в скінченній групі так, щоб вони були придатні для реального комп'ютерного застосування [14].

Особливе місце в цій галузі займають прості числа. В елементарній теорії чисел вони розглядаються як «цеглинки» арифметики завдяки теоремі про єдиність розкладу натурального числа на прості множники. У сучасній алгебрі та інформатиці прості числа відіграють ще ширшу роль. По-перше, саме з ними пов'язана побудова полів класів лишків за простим модулем, де кожен ненульовий клас має мультиплікативний обернений. По-друге, багато криптографічних протоколів спираються на властивості груп, порядок яких визначається через великі прості числа або числа, пов'язані з ними. По-третє, алгоритми генерації ключів у системах з відкритим ключем вимагають уміння швидко знаходити великі прості числа та перевіряти простоту кандидатів [15].

У практичних задачах прості числа мають дуже великі розміри. Якщо для навчальних прикладів достатньо чисел порядку кількох сотень або тисяч, то в реальних криптографічних системах використовують числа, довжина яких становить сотні або навіть тисячі бітів. Це означає, що пряма перевірка всіх можливих дільників є неможливою. Тому основна проблема формулюється так: як установити, що велике натуральне число є простим, не виконуючи повного розкладу на множники? Відповідь на це питання і приводить до побудови ймовірнісних тестів простоти, що поєднують ідеї теорії чисел, груп і алгоритмічного аналізу [14].

Перші швидкі тести простоти спираються на властивості мультиплікативної групи ненульових класів лишків за простим модулем. Якщо p –

просте число, то множина ненульових класів лишків за модулем p утворює скінченну групу відносно множення. Її порядок дорівнює $p - 1$. З теореми Лагранжа випливає, що для кожного елемента a , взаємно простого з p , виконується рівність $a^{p-1} \equiv 1 \pmod{p}$. Ця проста, але глибока ідея дозволяє перейти від абстрактної теорії груп до алгоритму перевірки простоти.

У межах обчислювальної алгебри важливо також оцінювати вартість операцій. Додавання та множення великих чисел, знаходження остач, піднесення до степеня за модулем, побудова оберненого елемента за розширеним алгоритмом Евкліда – усе це повинно бути організоване так, щоб кількість кроків зростала не занадто швидко разом із довжиною вхідних даних. Тому сучасна алгебра в алгоритмічному аспекті тісно пов'язана з поняттям складності алгоритму. Один і той самий теоретично правильний метод може виявитися практично непридатним, якщо його складність занадто велика.

Таким чином, сучасний погляд на прості числа поєднує три рівні. Перший рівень – теоретичний, де прості числа є базовими об'єктами арифметики. Другий рівень – структурний, де прості модулі забезпечують появу полів і зручних групових конструкцій. Третій рівень – алгоритмічний, де постає потреба ефективно обчислювати, перевіряти та генерувати прості числа для прикладних цілей. Саме на перетині цих трьох рівнів і формується той зміст, який доцільно називати елементами сучасної алгебри.

§6.2. МАЛА ТЕОРЕМА ФЕРМА І ЙМОВІРІСНА ПЕРЕВІРКА ПРОСТОТИ

Одним із перших результатів, що безпосередньо веде до алгоритмів перевірки простоти, є мала теорема Ферма. Вона стверджує: якщо p – просте число і число a не ділиться на p , то $a^{p-1} \equiv 1 \pmod{p}$. Інша поширена форма цього твердження має вигляд $a^p \equiv a \pmod{p}$ для довільного цілого a . З погляду алгебри мала теорема Ферма є наслідком властивостей скінченної мультиплікативної групи класів лишків за простим модулем. З погляду алгоритмів це критерій, який необхідно виконувати всім простим числам [12; 13].

Звідси виникає природна ідея: взяти довільне натуральне число $n > 1$, обрати число a , взаємно просте з n , і перевірити, чи виконується $a^{n-1} \equiv 1 \pmod{n}$. Якщо вона не виконується, то n точно складене. Якщо ж вона виконується, то число n може бути простим. Такий підхід приводить до тесту Ферма. Він є надзвичайно простим в реалізації, бо піднесення до степеня за модулем можна виконувати швидко методом бінарного піднесення до степеня. У результаті навіть для дуже великих n перевірка однієї основи a виконується за прийнятний час [16].

Бінарне піднесення до степеня саме по собі є добрим прикладом алгоритмічного мислення в алгебрі. Якщо потрібно обчислити $a^m \pmod{n}$, не слід виконувати $m - 1$ послідовних множень. Натомість показник m подають у двійковому вигляді, а потім комбінують квадрати a, a^2, a^4, a^8 і т.д. Це дає змогу скоротити кількість множень до порядку $\log m$. Для великих чисел така різниця є принциповою: без цього методу тести простоти були б занадто повільними.

Однак слід наголосити на принциповій обставині. Мала теорема Ферма дає лише необхідну ознаку простоти, але не достатню. Це означає, що всяке просте число пройде перевірку, тоді як деякі складені числа можуть її також пройти. Саме тому тест Ферма є ймовірнісним: він дозволяє швидко відсіювати багато складених чисел, але не гарантує абсолютної правильності висновку для кожного окремого n . Для навчальних цілей цей факт є дуже важливим, оскільки показує межі застосовності навіть красивих теоретичних тверджень.

Розглянемо простий приклад. Для $n = 15$ і $a = 2$ маємо $2^{14} \pmod{15} = 4$, отже мала теорема Ферма не виконується, і число 15 одразу розпізнається як складене. Але вже для інших складених чисел ситуація може бути іншою. Наприклад, число $341 = 11 \cdot 31$ задовольняє співвідношення $2^{340} \equiv 1 \pmod{341}$, хоча воно складене. Такі приклади демонструють, що сам по собі тест Ферма не може слугувати остаточним критерієм простоти.

Попри це, ідея тесту Ферма має велике методичне значення. Вона наочно показує, як абстрактна теорія груп перетворюється на алгоритм. Крім того, у реальних програмах вона часто використовується як дуже швидка попередня перевірка перед застосуванням сильніших тестів. Сама ж концепція «випробовувати число за різними основами a » вияви-

лася надзвичайно плідною і привела до більш надійних ймовірнісних методів [15; 16].

Під час пояснення цього тесту корисно звертати увагу студентів на різницю між двома логічними схемами. З однієї сторони, твердження «якщо p просте, то виконується формула Ферма» є істинним. З іншої сторони, обернене твердження «якщо виконується формула Ферма, то число просте» є хибним. Саме ця логічна асиметрія змушує сучасну алгебру комбінувати суворі доведення з імовірнісними процедурами.

§6.3. СВІДКИ ФЕРМА, ЛЖЕЦІ ФЕРМА І ЧИСЛА КАРМАЙКЛА

Для точного опису поведінки тесту Ферма вводять спеціальну термінологію. Нехай n – непарне натуральне число, більше від 2, і a – ціле число, для якого $1 < a < n$ та $\gcd(a, n) = 1$. Якщо виконується $a^{n-1} \not\equiv 1 \pmod{n}$, то число a називають свідком складеності числа n у тесті Ферма, або свідком Ферма. Наявність хоча б одного такого свідка означає, що n складене. Якщо ж для складеного n виконується конгруенція $a^{n-1} \equiv 1 \pmod{n}$, то число a називають лжецем Ферма для n . Отже, свідок Ферма викриває складене число, а лжець Ферма, навпаки, маскує його під просте.

Розподіл свідків і лжеців для конкретного складеного числа є важливою характеристикою тесту. Для багатьох складених чисел лжеців порівняно небагато, тому випадковий вибір основи a з великою ймовірністю призведе до викриття складеності. Це і пояснює практичну корисність тесту Ферма. Якщо перевірити число n за кількома випадково обраними основами, то шанси помилково прийняти складене число за просте часто стають дуже малими. Проте існують складені числа, для яких ситуація значно гірша.

Особливу роль відіграють числа Кармайкла. Складене число n називають числом Кармайкла, якщо для кожного a , взаємно простого з n , виконується $a^{n-1} \equiv 1 \pmod{n}$. Іншими словами, всі допустимі основи є для нього лжецями Ферма. Отже, тест Ферма взагалі не здатний відрізнити таке число від простого. Найвідоміший приклад – $561 = 3 \cdot 11 \cdot 17$. Для цього числа конгруенція Ферма виконується для всіх a , що взаємно прості з 561 [13; 14].

Існування чисел Кармайкла показує, що в криптографії не можна покладатися на надто слабкі перевірки. Якщо генератор простих чисел використовував би лише тест Ферма, то в окремих випадках він міг би прийняти складене число за просте. Це призвело б до неправильної побудови ключів і, як наслідок, до потенційного руйнування всієї криптографічної схеми. Тому сучасні стандарти використовують більш сильні критерії, а слабкі тести залишають хіба що як попередній фільтр.

Наявність чисел Кармайкла має важливий теоретичний висновок: жоден алгоритм, заснований лише на одній конгруенції $a^{n-1} \equiv 1 \pmod{n}$, не може бути достатньо надійним. Потрібно використовувати сильніші групові властивості. Це і стало мотивом для створення вдосконалених тестів, зокрема тесту Міллера–Рабіна. У ньому аналізується не тільки остаточна рівність, а й послідовність квадратів, що виникає при розкладі числа $n-1$ у вигляді $2^s d$, де d непарне. Завдяки цьому багато «лжеців» Ферма перестають бути лжецями у сильнішому тесті [17].

З педагогічного погляду поняття свідка і лжеця є вдалим прикладом того, як сучасна алгебра поєднує строгі математичні структури з мовою ймовірностей. Алгоритм не дає відповіді в категоричній формі «завжди так», але забезпечує контрольовану похибку. Це суттєво відрізняє сучасні обчислювальні методи від багатьох класичних теоретичних доведень, де істинність встановлюється абсолютно. Проте в реальних цифрових системах саме така контрольована похибка, доведено мала, є цілком прийнятною.

У навчальній роботі корисно самостійно знаходити свідків Ферма для невеликих складених чисел. Така практика формує відчуття структури множини лишків за модулем n і дозволяє краще зрозуміти, чому одна й та сама формула може поводитися по-різному для різних модулів. Це також підготовлює до сприйняття сильніших тестів, де поведінка елементів у групі аналізується значно глибше.

§6.4. ТЕСТ МІЛЛЕРА-РАБІНА

Одним із найпоширеніших сучасних ймовірнісних тестів простоти є тест Міллера-Рабіна. Його ідея ґрунтується на такому спостереженні. Нехай n – непарне просте число. Тоді $n - 1$ можна записати у вигляді $2^s d$, де d – непарне. Якщо для деякої основи a , взаємно простої з n , виконати обчислення $a^d, a^{2d}, a^{4d}, \dots, a^{2^{s-1}d}$ за модулем n , то у випадку простого n ця послідовність має дуже спеціальну поведінку: або вже $a^d \equiv 1 \pmod{n}$, або на деякому кроці отримуємо -1 за модулем n , після чого наступний квадрат дає 1 [15; 17].

Якщо ж число n складене і для деякої основи a описана структура порушується, то така основа називається сильним свідком складеності числа n . Тоді n одразу визнається складеним. Якщо ж число проходить перевірку для вибраної основи a , то кажуть, що n є сильним ймовірно простим щодо основи a . На відміну від тесту Ферма, де складене число могло мати дуже багато лжеців, у тесті Міллера-Рабіна можна довести сильну оцінку: для кожного непарного складеного n кількість сильних лжеців не перевищує чверті всіх можливих основ. Отже, одна випадкова перевірка дає ймовірність помилки не більше $1/4$, а кілька незалежних перевірок зменшують її експоненціально [18].

Практичний алгоритм має такий вигляд. Спочатку перевіряють тривіальні випадки: парність числа, малі дільники, значення $n = 2$ або $n = 3$. Далі розкладають $n - 1$ як $2^s d$. Після цього випадково вибирають основу a з діапазону $2, 3, \dots, n - 2$ та обчислюють $x = a^d \pmod{n}$. Якщо $x = 1$ або $x = n - 1$, то поточна перевірка вважається успішною. Інакше починають послідовно підносити x до квадрата за модулем n . Якщо на якомусь кроці з'явиться $n - 1$, перевірка також вважається успішною; якщо ж до цього не дійшло і послідовність завершилася, то n оголошують складеним [14; 15].

Розглянемо короткий навчальний приклад. Нехай $n = 221$. Маємо $221 = 13 \cdot 17$, тобто число складене, але припустімо, що це невідомо. Тоді $n - 1 = 220 = 4 \cdot 55$, отже $s = 2$ і $d = 55$. Візьмемо основу $a = 2$. Обчислення дають $2^{55} \pmod{221} = 128$. Це не 1 і не 220. Далі підносимо 128 до квадрата за модулем 221: $128^2 \pmod{221} = 30$. Значення 30 теж не дорівнює 220.

Оскільки ланцюжок вичерпано, число 221 викривається як складене. Саме такого типу обчислення і реалізує тест Міллера–Рабіна.

Перевага тесту Міллера–Рабіна полягає не лише в його надійності, а й у швидкодії. Основні обчислення зводяться до модульного піднесення до степеня, яке можна реалізувати дуже ефективно. Саме тому цей тест використовується в бібліотеках комп'ютерної алгебри, криптографічних пакетах та генераторах ключів. На практиці кілька незалежних раундів тесту дають настільки малу ймовірність помилки, що нею можна знехтувати для більшості прикладних задач.

Важливо підкреслити, що в навчальному курсі тест Міллера–Рабіна варто розглядати не як «чорну скриньку», а як наслідок конкретних алгебраїчних властивостей. Його коректність спирається на будову групи одиниць у кільці лишків за простим модулем, на властивості квадратних коренів з одиниці та на структуру ланцюжка квадратів у скінченній групі. Таким чином, навіть сучасний прикладний алгоритм органічно продовжує ті поняття, які вивчалися в попередніх розділах посібника.

Для повноти картини варто згадати, що існують і детерміновані алгоритми перевірки простоти. Найвідомішим теоретичним прикладом є алгоритм AKS, який доводить, що простоту можна перевіряти за поліноміальний час без використання ймовірнісних припущень. Проте в практичній криптографії саме тест Міллера–Рабіна та споріднені з ним процедури залишаються значно ефективнішими, а отже – реальнішими для щоденного використання.

§6.5. ВИКОРИСТАННЯ ПРОСТИХ ЧИСЕЛ У КРИПТОГРАФІЇ. СИСТЕМА RSA

Найвідомішим прикладом застосування простих чисел у криптографії є система RSA. Її ідея полягає в тому, щоб побудувати пару ключів: відкритий ключ, який можна публікувати, і закритий ключ, який залишається відомим лише власнику. Безпека RSA пов'язана з тим, що добуток двох великих простих чисел легко обчислити, але розкласти його назад на прості множники в загальному випадку дуже важко. У результаті класичні понят-

тя простого числа, взаємної простоти, функції Ейлера та оборотності класів лишків переходять у прикладну сферу захисту інформації [16].

Побудова ключів RSA має кілька кроків. Спочатку вибирають два великі прості числа p і q та обчислюють їх добуток $n = p \cdot q$. Далі знаходять значення функції Ейлера: $\varphi(n) = (p - 1)(q - 1)$. Після цього вибирають число e таке, що $1 < e < \varphi(n)$ і $\gcd(e, \varphi(n)) = 1$. Число e слугує показником відкритого ключа. Потім знаходять число d , яке є оберненим до e за модулем $\varphi(n)$, тобто $ed \equiv 1 \pmod{\varphi(n)}$. Пара (n, e) утворює відкритий ключ, а пара (n, d) – закритий. Наявність оберненого елемента d забезпечується саме взаємною простотою e і $\varphi(n)$.

Шифрування повідомлення m , яке інтерпретують як число з діапазону $0 \leq m < n$, здійснюють за формулою $c \equiv m^e \pmod{n}$. Розшифрування виконують за формулою $m \equiv c^d \pmod{n}$. Чому це працює? Оскільки $ed \equiv 1 \pmod{\varphi(n)}$, існує ціле k таке, що $ed = 1 + k \cdot \varphi(n)$. Тоді для повідомлень, взаємно простих з n , за теоремою Ейлера маємо $m^{ed} = m^{1 + k\varphi(n)} = m \cdot (m^{\varphi(n)})^k \equiv m \pmod{n}$. У більш точному доведенні використовують розгляд за модулями p і q окремо та китайську теорему про лишки [17].

Для навчального розуміння зручно розглянути малий приклад. Нехай $p = 61$, $q = 53$. Тоді $n = 3233$, $\varphi(n) = 3120$. Виберемо $e = 17$; легко перевірити, що $\gcd(17, 3120) = 1$. Обернений елемент до 17 за модулем 3120 дорівнює $d = 2753$, бо $17 \cdot 2753 \equiv 1 \pmod{3120}$. Якщо повідомлення $m = 123$, то шифротекст обчислюється як $123^{17} \pmod{3233}$. Після цього розшифрування за допомогою степеня 2753 повертає вихідне повідомлення. Попри малі числа, цей приклад точно відтворює логіку реальної системи RSA.

Практична реалізація RSA знову повертає нас до проблеми перевірки простоти. Щоб згенерувати ключі, потрібно отримати великі прості числа p і q . Без швидких тестів простоти це було б майже неможливо. На практиці генерація простого числа відбувається так: випадково вибирають велике непарне число, перевіряють його на подільність малими простими, а далі застосовують кілька раундів тесту Міллера–Рабіна. Якщо число проходить перевірки, його приймають як просте з дуже високою імовірністю [16].

З погляду сучасної алгебри RSA є чудовим прикладом того, як абстрактні поняття набувають прикладного змісту. Тут задіяно кільця лиш-

ків, мультиплікативні групи одиниць, оборотні елементи, функцію Ейлера, розклади чисел на прості множники і навіть китайську теорему про лишки. Тобто система RSA не просто «використовує прості числа», а спирається на цілу систему алгебраїчних ідей, що утворюють єдину логічну конструкцію.

Водночас важливо розуміти, що в сучасній криптографії безпека визначається не самою формулою шифрування, а коректним вибором параметрів, реалізацією та математичними припущеннями щодо складності задачі факторизації. Тому при вивченні RSA доречно поєднувати алгебраїчну частину з алгоритмічним мисленням: які саме операції виконуються швидко, які – повільно, які дані є відкритими, а які мають залишатися прихованими.

Система RSA використовується не лише для шифрування, а й для цифрового підпису. У такому разі власник закритого ключа застосовує показник d до хешу повідомлення, а перевірка виконується за відкритим показником e . І тут знову проявляється важливість алгебри: коректність перевірки забезпечується тими самими властивостями оборотності й степеневих відображень у кільці лишків. У підсумку один і той самий математичний апарат працює відразу в кількох криптографічних сценаріях.

§6.6. ГРУПИ В СУЧАСНІЙ КРИПТОГРАФІЇ ТА ЦИФРОВОМУ ПІДПИСІ

Після системи RSA природно перейти до ширшого питання: чому саме теорія груп настільки важлива для сучасної криптографії? Відповідь полягає в тому, що криптографічний протокол потребує середовища, де групова операція виконується легко, а деяка пов'язана з нею обернена задача є складною. Одним із найвідоміших прикладів є задача дискретного логарифмування. Нехай G – скінченна циклічна група з породжувальним елементом g . Якщо задано елемент $h = g^x$, то обчислити h за відомим x легко, а знайти x за відомими g і h в загальному випадку важко. Саме на цій асиметрії будують низку криптографічних схем.

Класичний приклад – протокол Діффі–Геллмана для узгодження спільного секрету. У спрощеному вигляді сторони працюють у циклічній групі великого простого порядку. Одна сторона вибирає секретний показник a і надсилає g^a , інша вибирає b і надсилає g^b . Після цього обидві сторони можуть обчислити спільний елемент g^{ab} , але сторонньому спостерігачу, який знає лише g , g^a і g^b , відновити цей секрет вважається складним. Тут знову працює структура групи: степені одного породжувального елемента породжують всю циклічну підгрупу.

Теорія груп лежить і в основі цифрового підпису. Ідея цифрового підпису полягає в тому, щоб власник секретного ключа міг побудувати короткий об'єкт – підпис – який можна перевірити за допомогою відкритого ключа, але не можна підробити без знання секрету. У багатьох схемах цифрового підпису використовується саме складність задачі дискретного логарифмування в певній групі. Практичний сенс цього полягає в тому, що алгебраїчна структура дозволяє швидко перевіряти правильність підпису, але не дає простої можливості його відтворити.

Окремо слід згадати еліптичні криві, які стали одним із найважливіших сучасних носіїв групових структур у криптографії. Множина точок еліптичної кривої над скінченним полем разом із спеціально означеною операцією утворює абелеву групу. Ці групи мають ту перевагу, що забезпечують високий рівень безпеки за відносно малих розмірів ключів. Для навчального курсу достатньо зрозуміти головну ідею: теорія груп не вичерпується перестановками чи класами лишків, а переходить у геометризовані структури, де групова операція визначається через побудову на кривій [18].

Слід також наголосити на ролі скінченних полів. Багато криптографічних груп будують не просто «на великих числах», а на елементах поля $GF(p)$ або $GF(2^m)$. Алгебраїчні операції в цих полях забезпечують ефективні обчислення, тоді як структура групи на їх основі дозволяє формувати складні обернені задачі. Таким чином, матеріал попередніх розділів про кільця та поля виявляється безпосередньо пов'язаним з протоколами захисту даних.

Порівнюючи RSA і схеми на дискретному логарифмі, можна побачити дві різні моделі використання алгебри. У RSA ключову роль відіграє оборотність у кільці лишків і складність факторизації. У протоколах

Діффі–Геллмана та цифрових підписах типу DSA чи ECDSA головною є циклічна група та складність дискретного логарифмування. Обидва підходи є алгебраїчними, але спираються на різні «тверді задачі» сучасної криптографії.

Таким чином, групи в сучасній криптографії виступають не декоративним додатком, а центральним математичним механізмом. Саме вони забезпечують побудову ключів, обчислення спільних секретів, перевірку цифрових підписів та аналіз складності криптографічних задач. Тому розділи про циклічні групи, порядок елемента, підгрупи та класи лишків мають пряме продовження у сучасних інформаційних технологіях.

Для студентів особливо корисно усвідомити, що тут ми маємо приклад справжньої єдності математики. Теорія груп, теорія чисел, алгоритми, ймовірність і навіть елементи геометрії працюють не окремо, а разом. Саме така міждисциплінарність і є однією з характерних рис сучасної алгебри.

§6.7. АЛГЕБРАЇЧНІ ІДЕЇ В БЛОКЧЕЙНІ

У масовій культурі блокчейн часто сприймається як суто технічна або фінансова технологія. Насправді ж його математичний фундамент значною мірою спирається на алгебру, теорію чисел та криптографію. Блокчейн – це розподілений реєстр, у якому записи об'єднуються в блоки, а блоки зв'язуються між собою за допомогою криптографічних хешів. Проте сама ідея незмінності, перевірюваності й автентичності даних ґрунтується на криптографічних механізмах, а ті, своєю чергою, будуються на алгебраїчних структурах [20].

Найпростіше простежити цей зв'язок на прикладі цифрового підпису транзакцій. У багатьох криптовалютних системах власник гаманця підтверджує право розпоряджатися активом, створюючи цифровий підпис за допомогою секретного ключа. Верифікація підпису виконується за відкритим ключем і спирається на арифметику в скінченних полях та на групі операції. З практичного погляду це означає, що кожна транзакція є не просто рядком даних, а об'єктом, коректність якого перевіряється засобами сучасної алгебри.

Ще одним важливим компонентом є криптографічна хеш-функція. Хоча хешування не є груповою операцією, воно тісно пов'язане з дискретними структурами і використовується разом із цифровим підписом для захисту цілісності даних. Хеш блоку залежить від його вмісту і від хешу попереднього блоку. Тому зміна навіть одного біта в старому блоці призводить до зміни всього ланцюга хешів. Саме ця властивість робить підробку історії транзакцій вкрай складною без перерахунку великої кількості даних.

У багатьох блокчейн-системах використовують дерева Меркла. Вони дозволяють об'єднати велику кількість транзакцій в один кореневий хеш і швидко доводити належність конкретної транзакції до блока. Тут ми знову бачимо поєднання дискретної математики, алгоритмів та криптографії. Хоча дерево Меркла не є алгебраїчною структурою в класичному розумінні, його практичне використання спирається на ті самі принципи ефективного опрацювання дискретних об'єктів, що характерні для сучасної алгебри й суміжних дисциплін.

У деяких системах блокчейн поєднується з механізмом доказу виконаної роботи, де вузол мережі має знайти такий заголовок блоку, щоб його хеш задовольняв задану умову. Хоча тут на перший план виходить обчислювальна складність, з математичного боку ми знову маємо справу з дискретними алгоритмами, великими цілими числами, залишками та комп'ютерною арифметикою. Тому блокчейн є доброю ілюстрацією того, як різні розділи сучасної алгебри і суміжних дисциплін працюють у спільному технологічному середовищі.

Для цілей даного посібника важливо не стільки заглиблюватися в інженерні деталі блокчейн-протоколів, скільки побачити загальну картину. Групи забезпечують математичну основу цифрових підписів. Кільця лишків і скінченні поля лежать в основі арифметики ключів. Простота великих чисел, ефективне модульне піднесення до степеня, поняття оберненого елемента та алгоритмічна складність – усі ці категорії, які в класичному курсі можуть здаватися абстрактними, у блокчейн-середовищі набувають прикладної сили.

Блокчейн також демонструє, що сучасні математичні застосування рідко спираються лише на один результат або одну структуру. Тут одноча-

сно працюють хешування, цифрові підписи, правила мережевого консенсусу, формати подання даних та механізми перевірки. Саме тому для майбутнього вчителя, математика чи фахівця з комп'ютерних наук важливо бачити за окремими формулами ширшу архітектуру математичних ідей.

З методичного погляду тема блокчейну корисна ще й тим, що вона мотивує вивчення алгебри. Коли студент бачить, що поняття групи, поля або оберненого елемента лежать в основі сучасних цифрових систем, абстрактний матеріал перестає сприйматися як відірваний від реальності. Таким чином, коротке ознайомлення з блокчейн-технологіями може виконувати роль мосту між теоретичною математикою та сучасними інформаційними практиками.

§6.8. ДОДАТКОВІ ПРИКЛАДИ ЗАСТОСУВАННЯ АЛГЕБРИ

Сучасні застосування алгебри не обмежуються криптографією. Теорія груп широко використовується у фізиці, де симетрії описують інваріантність систем відносно певних перетворень. Групи Лі, матричні групи та їх представлення лежать в основі математичної мови квантової механіки й теорії елементарних частинок. Хоча ці сюжети виходять за межі даного посібника, саме вони показують, наскільки глибоко поняття групи проникло в сучасну науку.

У хімії теорія груп використовується для класифікації симетрій молекул і передбачення властивостей спектрів. Тут алгебраїчна структура дозволяє компактно описувати можливі перетворення, які зберігають форму молекули. У кристалографії групи симетрій визначають просторові типи кристалічних решіток. Таким чином, навіть у природничих науках групи виконують роль універсальної мови симетрії.

У теорії кодування кільця, поля та многочлени допомагають будувати коди, здатні виявляти й виправляти помилки. Наприклад, циклічні коди описують за допомогою ідеалів у кільцях многочленів над скінченними полями. Тут попередні розділи про кільця, фактор-кільця та многочлени знаходять цілком природне продовження. У цифрових комунікаціях саме такі алгебраїчні конструкції роблять передачу даних надійнішою.

У комп'ютерній алгебрі алгоритми на кшталт знаходження найбільшого спільного дільника многочленів, побудови базисів Гребнера чи факторизації поліномів над скінченними полями спираються на тонку структуру алгебраїчних об'єктів. Саме поєднання теорії та ефективного алгоритму робить можливими системи символьних обчислень, які сьогодні використовують у науці, техніці та освіті.

Наведені приклади важливі для загального висновку: алгебра – це не лише сукупність означень і теорем, а ще й універсальний спосіб організації математичних моделей. Там, де виникає поняття операції, симетрії, оборотності, інваріанта або породження складного об'єкта з простіших, дуже часто з'являється відповідна алгебраїчна структура. У цьому сенсі сучасна алгебра є не вузькою дисципліною, а одним з фундаментальних способів мислення в математиці.

ВИСНОВКИ

Навчально-методичний посібник «Алгебраїчні структури і їх застосування» присвячений систематичному викладу основних положень сучасної алгебри та демонстрації їх теоретичного і прикладного значення. У посібнику розглянуто фундаментальні алгебраїчні структури – групи, кільця, ідеали, кільця многочленів від однієї та кількох змінних, симетричні многочлени, а також алгебраїчні розширення числових полів. Особливу увагу приділено сучасним напрямкам застосування алгебраїчних ідей, зокрема в обчислювальній алгебрі, теорії простих чисел, криптографії, цифровому підписі та технологіях блокчейну.

Структура посібника побудована за принципом поступового ускладнення навчального матеріалу. Виклад розпочинається з базових означень і найпростіших властивостей алгебраїчних об'єктів, після чого послідовно переходить до складніших понять і теоретичних конструкцій. Такий підхід дає змогу здобувачам освіти не лише засвоїти окремі означення, теореми й методи доведення, а й побачити внутрішні зв'язки між різними розділами алгебри, зрозуміти логіку побудови математичної теорії та її роль у розвитку сучасної науки.

Кожен розділ посібника містить теоретичний матеріал, що супроводжується доведеннями, характерними прикладами та системою вправ різного рівня складності. Це створює умови як для аудиторного опрацювання тем під керівництвом викладача, так і для самостійної роботи здобувачів освіти. Приклади й вправи спрямовані на формування навичок математичного мислення, уміння аналізувати алгебраїчні об'єкти, встановлювати їхні властивості, працювати з абстрактними структурами та застосовувати отримані знання до розв'язання теоретичних і прикладних задач.

Важливою особливістю посібника є поєднання класичного змісту курсу алгебри з матеріалом, що демонструє сучасні напрями використання алгебраїчних методів. Розгляд малої теореми Ферма, свідків і лжеців Ферма, чисел Кармайкла, тесту Міллера–Рабіна, системи RSA, алгебраїчних основ цифрового підпису та блокчейн-технологій показує, що абс-

трактні алгебраїчні поняття мають не лише теоретичне, а й практичне значення. Це сприяє усвідомленню ролі алгебри як інструмента для розв'язання актуальних задач сучасної математики, інформатики та інформаційної безпеки.

Опрацювання матеріалу посібника спрямоване на розвиток здатності коректно використовувати математичну символіку, будувати логічно обґрунтовані міркування, застосовувати основні методи доведення та працювати з абстрактними математичними структурами. Сформовані в процесі вивчення компетентності є необхідною основою для подальшого опанування суміжних математичних і прикладних дисциплін, зокрема теорії чисел, математичної логіки, дискретної математики, теоретичної інформатики, криптографії та комп'ютерних наук.

Отже, посібник може бути використаний як основний або допоміжний навчальний ресурс під час вивчення курсу алгебри у закладах вищої освіти. Він буде корисним для студентів фізико-математичних спеціальностей, магістрантів, аспірантів, викладачів, а також усіх, хто прагне поглибити знання з алгебри та зрозуміти її зв'язок із сучасними науковими й технологічними застосуваннями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Требенко Д. Я., Требенко О. О. Алгебра і теорія чисел : навчальний посібник для студентів математичних спеціальностей педагогічних університетів. Ч. 1. Київ: НПУ імені М. П. Драгоманова, 2006. 400 с.
2. Волошина Т. В. Групи, кільця, поля : курс лекцій. Луцьк: Вежа-Друк, 2020. 84 с.
3. Гаврилків В. М. Елементи теорії груп та теорії кілець: навчальний посібник. Івано-Франківськ: Голіней, 2016. 148 с.
4. Безущак О. О., Ганюшкін О. Г. Теорія груп: навчальний посібник для студентів механіко-математичного факультету. Київ: ВПЦ «Київський університет», 2005. 123 с.
5. Безущак О. О., Ганюшкін О. Г. Завдання до практичних занять з алгебри і теорії чисел: теорія кілець і полів: для студентів університетів. Київ: ВПЦ «Київський університет», 2020. 137 с.
6. Бондаренко Є. В. Теорія кілець: навчальний посібник. Київ: ВПЦ «Київський університет», 2012. 64 с.
7. Волошина Т. В. Елементи теорії груп: навчальний посібник. Луцьк: Вежа-Друк, 2017. 144 с.
8. Бородін О. І. Теорія чисел. Львів: Вища школа, 1970. 162 с.
9. Лукашова Т. Д., Друшляк М. Г. Алгебра і теорія чисел: навчальний посібник для студентів спеціальності 014 «Середня освіта. Математика». Ч. І. Суми: СумДПУ імені А. С. Макаренка, 2022. 123 с.
10. Ковальчук Л. В., Конюшок С. М., Кучинська Н. В. Прикладна алгебра: основні поняття алгебри та теорії чисел: навчальний посібник. Київ: НТУУ «КПІ», 2011.
11. Завало С. Т. та ін. Алгебра і теорія чисел. Ч. 2. Київ: Вища школа, 1976. 352 с.
12. Shoup V. A Computational Introduction to Number Theory and Algebra. 2nd ed. Cambridge: Cambridge University Press, 2009. 580 p.
13. Koblitz N. A Course in Number Theory and Cryptography. 2nd ed. New York: Springer, 1994. 235 p.
14. Crandall R., Pomerance C. Prime Numbers: A Computational Perspective. 2nd ed. New York: Springer, 2005. 597 p.
15. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996. 816 p.
16. Stinson D. R., Paterson M. Cryptography: Theory and Practice. 4th ed. Boca Raton: Chapman and Hall/CRC, 2019. 538 p.
17. Hoffstein J., Pipher J., Silverman J. H. An Introduction to Mathematical Cryptography. 2nd ed. New York: Springer, 2014. 540 p.
18. Katz J., Lindell Y. Introduction to Modern Cryptography. 3rd ed. Boca Raton: CRC Press, 2020. 648 p.

19. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016. 336 p.
20. Antonopoulos A. M. Mastering Bitcoin: Programming the Open Blockchain. 2nd ed. Sebastopol: O'Reilly Media, 2017. 398 p.

Міністерство освіти і науки України
Кам'янець-Подільський національний університет імені Івана Огієнка

НАВЧАЛЬНЕ ЕЛЕКТРОННЕ ВИДАННЯ

ЗЕЛЕНСЬКИЙ Олексій Віталійович,
кандидат фізико-математичних наук, доцент,
доцент кафедри математики Кам'янець-Подільського
національного університету імені Івана Огієнка

СМОРЖЕВСЬКИЙ Юрій Людвігович,
кандидат педагогічних наук, доцент, завідувач
кафедри математики Кам'янець-Подільського
національного університету імені Івана Огієнка

ДИНИЧ Альона Юріївна,
викладачка ТОВ «Фаховий передвищий коледж «ОПТИМА»

АЛГЕБРАЇЧНІ СТРУКТУРИ І ЇХ ЗАСТОСУВАННЯ

НАВЧАЛЬНО-МЕТОДИЧНИЙ ПОСІБНИК

ЕЛЕКТРОННЕ ВИДАННЯ

Підписано 25.09.2026. Формат 60x84/16. Гарнітура «Cambria».
Об'єм даних 12,9 Мб. Обл.-вид. арк. 7,7. Зам. № 1278.

Кам'янець-Подільський національний університет
імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.
Свідоцтво серії ДК № 3382 від 05.02.2009 р.

Виготовлено в Кам'янець-Подільському національному
університеті імені Івана Огієнка,
вул. Огієнка, 61, м. Кам'янець-Подільський, 32300.