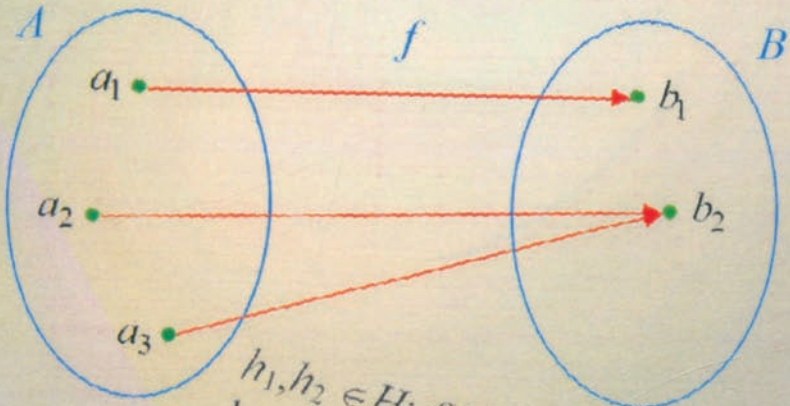
Л. В. Ковальчук, Ю. Є. Яремчук

ПРИКЛАДНА АЛГЕБРА

Частина 1. Основи абстрактної алгебри



$h_1, h_2 \in H: f(h_1 \cdot h_2) = f(h_1) \times f(h_2)$

$\ker f = \{g \in G: f(g) = e_H\}$

$\operatorname{Im} f = \{h \in H: \exists g \in G, f(g) = h\}$

$\forall s_1, s_2, s_3 \in S: (s_1 \otimes s_2) \otimes s_3 = s_1 \otimes (s_2 \otimes s_3)$

$s_1 \otimes s_2 = s_2 \otimes s_1$

$\exists g \in G \; \forall a = G \; \exists k \in \mathbb{Z}: a = g^k$

$|G| = (G:H)\,|H|$

$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} (a_i - a_k)^{-1}(x - a_k)$

Міністерство освіти і науки України
Вінницький національний технічний університет

ПРИКЛАДНА АЛГЕБРА

Частина 1. Основи абстрактної алгебри

Навчальний посібник

Вінниця
ВНТУ
2015

УДК 512.5(075)
ББК 22.144я73
К56

Автори:
Ковальчук Л. В., Яремчук Ю. Є.

Рекомендовано до друку Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 5 від 25.12.2014 р.).

Рецензенти:
О. В. Рибальський, доктор технічних наук, професор
А. М. Коломієць, доктор педагогічних наук, професор
В. І. Клочко, доктор педагогічних наук, професор

Ковальчук, Л. В.
К56 Прикладна алгебра. Частина 1. Основи абстрактної алгебри : навчальний посібник / Л. В. Ковальчук, Ю. Є. Яремчук – Вінниця : ВНТУ, 2015. – 99 с.

У посібнику викладено основні положення та властивості алгебраїчних систем. Розглянуто основні поняття абстрактної алгебри, зокрема, групи, кільця та поля, з їх властивостями та різного роду взаємними відображеннями. Посібник є першою з трьох частин курсу "Прикладна алгебра" і є базовим при вивченні теорії чисел (друга частина курсу) та теорії скінченних полів (третя частина). Разом ці розділи алгебри утворюють так звану прикладну алгебру і є, зокрема, математичною базою для симетричної та асиметричної криптографії.

Посібник призначено для тих, хто цікавиться вивченням абстрактної алгебри, для студентів та аспірантів вищих навчальних закладів, що вивчають та займаються інформаційною безпекою.

УДК 512.5(075)
ББК 22.144я73

ЗМІСТ

ПЕРЕДМОВА

Цей посібник є першою з трьох частин курсу "*Прикладна алгебра*". Він охоплює основні поняття *абстрактної алгебри* (групи, кільця, поля), їхні властивості та відображення між ними. Матеріал цього посібника є базовим при вивченні *теорії чисел* (друга частина курсу) та *теорії скінченних полів* (третя частина).

Розділи алгебри, що увійшли до усіх трьох частин курсу, в першу чергу орієнтовані на створення математичної бази, необхідної (а в багатьох випадках і достатньої) для вивчення різних розділів криптології – як симетричної, так і несиметричної; як класичної, так і сучасної. Ці розділи алгебри є основними для дисципліни, яку в останні роки прийнято називати прикладною алгеброю.

Значною мірою посібник орієнтований на студентів та аспірантів прикладних спеціальностей, таких як "Прикладна криптологія", "Безпека інформаційно-комунікаційних систем", "Управління інформаційною безпекою", "Системи технічного захисту інформації" тощо. Але він також буде корисним і для тих, хто окремо планує вивчати абстрактну алгебру, оскільки містить найважливіші базові результати, оформлені у вигляді теорем, та допоміжні, сформульовані у вигляді лем. Усі твердження наводяться з повними та строгими доведеннями.

Автори намагались дотримуватись такої послідовності викладення матеріалу: означення – приклади – лема – теорема – наслідки – приклади застосування. Велика кількість прикладів допомагає кращому розумінню матеріалу.

Вважаємо, що повноцінне засвоєння матеріалу неможливе без великого обсягу розв'язаних задач. Тому до кожного параграфа надається не лише перелік питань для самоконтролю, а й значна кількість задач, багато з яких є авторськими. Також у кінці посібника наводяться додаткові

задачі до різних параграфів. Задачі підвищеної складності відмічені зірочками. Їх розв'язання, як правило, вимагає (декількох) нетривіальних кроків, хоча за рівнем складності вони різні.

Для тих, хто бажає детальніше ознайомитись з матеріалом за темами посібника, рекомендуємо таку літературу: §0 – [1, 2]; §§1–4 та §6 – [1–4]; §5 – [5].

Додатково можна використати літературу [6–9].

Наведений у посібнику матеріал, як і весь курс "*Прикладна алгебра*", має вагоме прикладне застосування, зокрема у криптології. У роботах [10–13] автори посібника показують можливість такого застосування.

§0 МНОЖИНИ І ВІДОБРАЖЕННЯ (замість вступу)

Предметом алгебри є так звані *алгебраїчні системи* (або *структури*), тобто *множини* з заданими на них *операціями*. Алгебра вивчає як властивості цих операцій, так і *відображення* між різними алгебраїчними системами. Тому для вивчення основ абстрактної алгебри необхідно спочатку ознайомитись з поняттями множини та відображення.

0.1 Множини та операції з множинами

Поняття множини є одним з тих математичних понять, які приймаються без строгого означення (наприклад, точка, пряма, відстань,...). Інтуїтивно означення множини можна сформулювати так: це набір елементів, що мають певну властивість, або певну ознаку; або сукупність елементів, об'єднаних за певною ознакою. Засновник теорії множин, німецький математик Г. Кантор (185–1918) сформулював це означення так: "Під множиною розуміють об'єднання в одне загальне тих об'єктів, що добре розрізняються інтуїтивно або думкою". Всі об'єкти, що входять до деякої множини, вважаються різними. Вони називаються *елементами* множини. Елементи множини позначають малими латинськими буквами (часто – з індексами), а самі множини – великими латинськими буквами. Наприклад, множини A, B, C, ...; елементи a, b, c, a_1, a_1, ... Для запису того факту, що деякий елемент *належить* або *не належить* множині A, використовують символи "$\in$" та "$\notin$". Наприклад: $a \in A$ – "елемент a належить множині A"; $a \notin B$ – "елемент a не належить множині B"; Aэ a – "множина A *містить* елемент a".

Означення 0.1: нехай A, B – деякі множини. Будемо казати, що множина A є *підмножиною* множини B (або множина B містить множину

A, або множина A міститься у множині B), якщо всі елементи множини A належать множині B, тобто $\forall a \in A : a \in B$.

Для позначення підмножини використовують символ "$\subset$". Наприклад, запис $A \subset B$ або $B \supset A$ означає "множина A є підмножиною множини B", або "множина B містить множину A". Наприклад, множина парних натуральних чисел є підмножиною множини усіх натуральних чисел.

Якщо A – підмножина B, яка відрізняється від B, то A називають *власною* підмножиною B, записуючи $A \subsetneq B$. Іноді, навпаки, замість "$\subset$" пишуть "$\subseteq$", використовуючи "$\subset$" для власних підмножин, замість "$\subsetneq$".

Означення 0.2: множини A і B називають *рівними* (і записують $A=B$), якщо одночасно $A \subset B$ і $B \subset A$.

В протилежному випадку пишуть $A \neq B$ і кажуть, що множини A і B *не є рівними.*

Означення 0.3: якщо множина містить скінченну кількість елементів, то вона називається *скінченною*. У протилежному випадку множина називається *нескінченною*. Кількість елементів множини називається *порядком* цієї множини. Порядок множини може дорівнювати нулю, або будь-якому натуральному числу, або нескінченності.

Множини можна задавати кількома різними способами: переліком усіх її елементів; правилом, яке задає цей перелік; описом властивостей, які мають всі елементи множини. Для задання множини використовують фігурні дужки. Наприклад, переліком можна задавати лише скінченні множини: $A = \{3,4,7\}$ – "множина A складається з елементів 3, 4, та 7"; $B = \{b\}$ – "множина B складається з одного елемента b".

Якщо правило переліку є досить простим, і його можна зрозуміти за першими кількома елементами, то множину можна задавати так: $C = \{2,4,6,..\}$ – "множина C складається з усіх парних натуральних чисел". Множина C є нескінченною.

Найбільш універсальним способом задання множини є задання з використанням опису властивостей. Наприклад, запис $D=\{d \mid P_1,...,P_k\}$ або $D=\{d : P_1,...,P_k\}$ означає, що множина D складається з усіх таких елементів, що мають властивості $P_1,...,P_k$. Зокрема, множину $C=\{2,4,6,..\}$ можна цим способом задати так: $C=\{d \mid d \in N, d=2k\}$ або $C=\{d \mid d \in N, d \vdots 2\}$.

Означення 0.4: множина, яка не містить ніяких елементів, називається *порожньою* і позначається символом "$\varnothing$". Вважається, що порожня множина є підмножиною будь-якої множини.

Для деяких множин, що є особливо важливими у математиці, використовують загальноприйняті позначення. Наприклад:

N – множина натуральних чисел;

$\mathbf{N_0}$ – множина невід'ємних цілих чисел;

Z – множина цілих чисел;

Q – множина раціональних чисел (нагадуємо, що $Q=\left\{\frac{m}{n} \mid m \in Z, n \in N\right\}$);

R – множина дійсних чисел;

C – множина комплексних чисел.

Також для визначення такої підмножини цілих чисел, що містить всі послідовні числа від m до n включно $(m<n)$, використовують позначення $\overline{m,n}$: запис $i=\overline{m,n}$ означає, що $i \in \{m,m+1,...,n\}$.

Над множинами можна виконувати різні операції, отримуючи в результаті нові множини.

Означення 0.5: *об'єднанням* $A \cup B$ двох множин A і B називається така множина C, що містить ті і тільки ті елементи, що належать хоча б одній з цих множин: $C=A \cup B=\{x \mid x \in A \text{ або } x \in B\}$.

Означення 0.6: *перерізом* $A \cap B$ двох множин A і B називається така множина C, що містить ті і тільки ті елементи, що одночасно належать обом з цих множин: $C = A \cap B = \{x \mid x \in A \text{ та } x \in B\}$.

Аналогічно до означень 5 та 6, можна визначити об'єднання та переріз довільної кількості множин. Такі дії позначаються як $\bigcup_{i=1}^{n} A_i$ та $\bigcap_{i=1}^{n} A_i$ – об'єднання та переріз множин $A_1,\ldots,A_n$.

Означення 0.7: *різницею* $A \setminus B$ двох множин A і B називається така множина C, що містить ті і тільки ті елементи, що одночасно належать множині A та не належать множині B: $C = A \setminus B = \{x \mid x \in A \text{ та } x \notin B\}$.

Приклад 0.1.

Нехай $A = \{x \mid -1 \le x < 4\} \cup \{7\}$, $B = \{x \mid -2 \le x < 1\} \cup \{3\}$. Тоді:

$A \cup B = \{x \mid -2 \le x < 4\} \cup \{7\}$, $A \cap B = \{x \mid -1 \le x < 1\} \cup \{3\}$,

$A \setminus B = \{x \mid 1 \le x < 3\} \cup \{x \mid 3 < x < 4\} \cup \{7\}$.

Означення 0.8: якщо $B \subset A$, то множина $A \setminus B$ називається *доповненням множини B до множини A*.

Вважається, що всі множини містяться у деякій *універсальній множині* U. Тоді *доповненням* $\overline{A}$ множини A називається множина всіх таких елементів, що не належать множині A: $\overline{A} = U \setminus A = \{x \mid x \notin A\}$. Зрозуміло, що $A \cup \overline{A} = U$ та $A \cap \overline{A} = \varnothing$.

Для операцій об'єднання та перерізу справедливі так звані *закони асоціативності*:

$$A \cup (B \cup C) = (A \cup B) \cup C,\ A \cap (B \cap C) = (A \cap B) \cap C;$$

комутативності:

$$A \cup B = B \cup A,\ A \cap B = B \cap A;$$

дистрибутивності:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

та *закони де-Моргана*:

$$\overline{A \cup B} = \overline{A} \cap \overline{B},\ \overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Означення 0.9: *декартовим добутком* $A \times B$ двох множин A та B називається множина всіх упорядкованих пар (a,b), де перший елемент пари належить першій множині, а другий – другій множині:
$A \times B = \{(a,b) : a \in A, b \in B\}$.

Аналогічно визначається декартовий добуток $A_1 \times A_2 \times ... \times A_n$ довільної (навіть нескінченної) кількості множин. Якщо у цьому добутку $A_1 = ... = A_n$, то замість $A \times A \times ... \times A$ пишуть A^n.

0.2 Відображення, типи відображень

Нехай A, B – деякі множини.

Означення 0.10: *відображенням* f множини A у множину B називають правило (закон), згідно з яким кожному елементу множини A ставиться у відповідність єдиний елемент множини B. Це відображення позначають як $f : A \to B$. Той факт, що відображення f елемента $a \in A$ ставить у відповідність деякий елемент $b \in B$, записують так: $b = f(a)$. При цьому елемент $b \in B$ називають *образом* елемента $a \in A$ при відображенні f, а елемент $a \in A$ – *прообразом* елемента $b \in B$. Множину всіх прообразів елемента $b \in B$ називають його *повним прообразом* і позначають $f^{-1}(b)$: $f^{-1}(b) = \{a \in A : f(a) = b\}$. Аналогічно визначається повний прообраз будь-якої підмножини множини B.

У множині B, взагалі кажучи, можуть існувати елементи, що мають більше одного прообразу, та елементи, що не мають жодного прообразу. Але кожен елемент множини A повинен мати рівно один образ.

Множину A називають *областю визначення* відображення f і позначають $A = D(f)$. Підмножину множини B, кожен елемент якої має хоча б один прообраз, називають *областю значень* відображення f та позначають $E(f)$ або $f(A)$: $E(f) = \{b \in B \mid \exists a \in A : b = f(a)\}$.

Розглянемо правила відповідності між двома множинами, задані графічно (рис. 1–3), та визначимо, які з них є відображеннями.

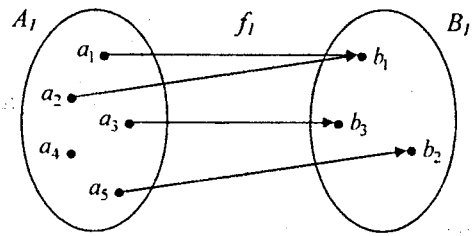


Рисунок 1

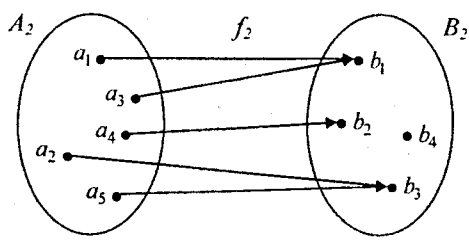


Рисунок 2

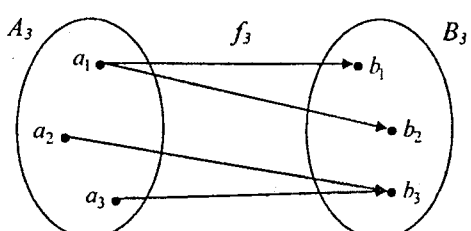


Рисунок 3

Правила відповідності, зображені на рис. 1–3, виглядають таким чином. На рис. 1: $f_1 : A_1 \to B_1$, при цьому $f_1(a_1) = b_1$, $f_1(a_2) = b_1$, $f_1(a_3) = b_3$, $f_1(a_5) = b_2$. Правило $f_1 : A_1 \to B_1$ не є відображенням, оскільки елементу a_4 немає відповідного у множині B.

На рис. 2: $f_2 : A_2 \to B_2$, при цьому $f_2(a_1) = b_1$, $f_2(a_2) = b_3$, $f_2(a_3) = b_1$, $f_2(a_4) = b_2$, $f_2(a_5) = b_3$. Правило $f_2 : A_2 \to B_2$ є відображенням.

На рис. 3: $f_3 : A_3 \to B_3$, при цьому $f_3(a_1) = b_1$, $f_3(a_1) = b_2$, $f_3(a_2) = b_3$, $f_3(a_3) = b_3$. Правило $f_3 : A_3 \to B_3$ не є відображенням, оскільки елементу a_1 ставиться у відповідність відразу два елементи b_1 та b_2 множини B.

Залежно від властивостей, розрізняють три типи відображень.

Означення 0.11: відображення $f : A \to B$ називається *сюр'єктивним* (або *сюр'єкцією*), якщо $\forall b \in B \, \exists a \in A : f(a) = b$, тобто для кожного елемента множини B існує принаймні один прообраз, або, що те ж саме, $f(A) = B$.

Означення 0.12: відображення $f : A \to B$ називається *ін'єктивним* (або *ін'єкцією*), якщо $\forall a_1, a_2 \in A \, (a_1 \neq a_2) : f(a_1) \neq f(a_2)$, тобто різні елементи множини А мають різні образи.

Означення 0.13: відображення $f : A \to B$ називається *бієктивним* (або *бієкцією*, або *взаємно-однозначним відображенням*), якщо воно є одночасно сюр'єктивним та ін'єктивним.

Наведемо рисунки різних типів відображень.

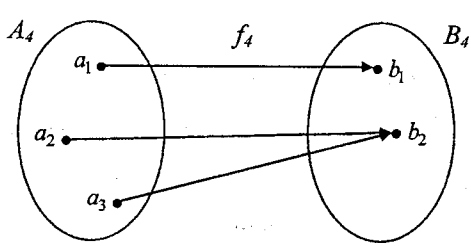


Рисунок 4

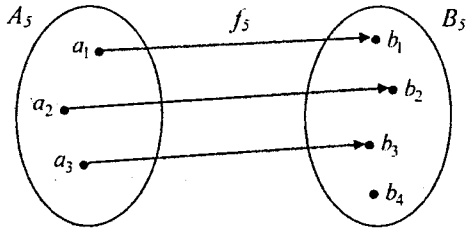


Рисунок 5

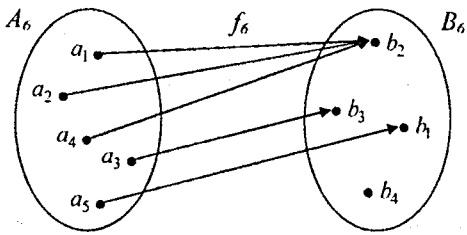


Рисунок 6

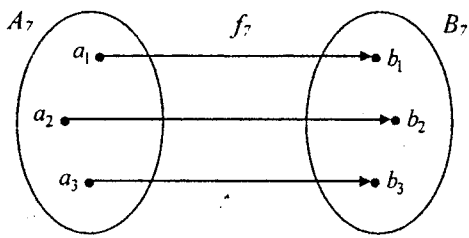


Рисунок 7

Відображення f_4 є сюр'єктивним, але не ін'єктивним. Відображення f_5 є ін'єктивним, але не сюр'єктивним. Відображення f_6 не є сюр'єктивним і не є ін'єктивним. Відображення f_7 є і сюр'єктивним, і ін'єктивним, а, отже, воно є бієктивним.

Рекомендується самостійно обґрунтувати перелічені властивості відображень f_4, f_5, f_6, f_7.

Типи відображень можна також показати на таких простих прикладах.

Приклад 0.2. Якщо визначити відображення f_1: $\mathbf{Z} \to \mathbf{N}_0$, поклавши для $a \in \mathbf{Z}$:

$$f_1(a) = |a|,$$

де $|a|$ – абсолютна величина числа a,

то, очевидно, що f_1 – сюр'єктивне, але не ін'єктивне відображення.

Приклад 0.3. Відображення f_2: $\mathbf{Z} \to \mathbf{N}_0$, що визначається рівнянням

$$f_2(a) = \begin{cases} 2a, & \text{if } a \geq 0 \\ |2a| - 1, & \text{if } a < 0 \end{cases},$$

є бієктивним відображенням.

Означення 0.14: нехай A, B, C – деякі множини, на яких задані такі відображення: $f_1 : A \to B$, $f_2 : B \to C$.

Відображення $f : A \to C$, визначене за правилом:

$$\forall a \in A : f(a) = f_2(f_1(a)),$$

називається *композицією* (або *суперпозицією*, або *добутком*) відображень f_2 та f_1.

Композиція відображень f_2 та f_1 позначається $f_1 \circ f_2$, або $f_1 \cdot f_2$, або просто $f_1 f_2$. Наприклад, замість $f_2(f_1(a))$ можна писати $(f_1 \circ f_2)(a)$ або $(f_1 f_2)(a)$.

Приклад 0.4: нехай задані відображення

$$f_1 : R \to R_+, \quad f_1(x) = x^2 \text{ та } f_2 : R_+ \to R, \quad f_2(x) = \ln x.$$

Тоді композиція f відображень f_1 та f_2 діє таким чином:

$$f = f_1 \circ f_2 : R \to R,\ f(x) = \ln(x^2) = 2\ln|x|,$$

а композиція g відображень f_2 та f_1 визначається так:

$$f = f_2 \circ f_1 : R_+ \to R_+,\ g(x) = (\ln x)^2.$$

Означення 0.15: відображення $f : A \to B$ називається *оборотним*, якщо виконується така умова:

$$\forall b \in B\ \exists! a \in A : f(a) = b.$$

Якщо f – оборотне, то можна побудувати *обернене до* f відображення $f^{-1} : B \to A$, яке визначається таким чином: $\forall b \in B\ f^{-1}(b) = a$ для деякого $a \in A$ тоді і тільки тоді, коли $f(a) = b$.

Зауваження 0.1: якщо $f : A \to B$ є оборотним, то відображення $f^{-1} \circ f$ є *тотожним* відображенням на множині A, тобто $f^{-1} \circ f : A \to A,\ \ \forall x \in A : (f^{-1} \circ f)(x) = x$.

Аналогічно, відображення $f \circ f^{-1}$ є тотожним відображенням на множині B, тобто $f \circ f^{-1} : B \to B,\ \ \forall x \in B : (f \circ f^{-1})(x) = x$.

Твердження 0.1: нехай $f : A \to B$. Тоді такі твердження рівносильні:

1) відображення f є бієктивним;

2) існує обернене до f відображення (тобто відображення f є оборотним);

3) $\forall b \in B\ \exists! a \in A : f(a) = b$.

Рекомендується дане твердження довести самостійно.

§1 ОСНОВНІ ОЗНАЧЕННЯ ТА ВЛАСТИВОСТІ АЛГЕБРАЇЧНИХ СИСТЕМ

1.1 Алгебраїчні системи з однією операцією

На початку даного параграфа ми введемо ряд означень, з якими будемо працювати протягом даного курсу, а потім сформулюємо та доведемо їх основні властивості.

Означення 1.1: нехай S – деяка множина. *Бінарна операція*, визначена на множині S – це відображення $\otimes: S\times S\to S$, яке кожній парі елементів $(s_1, s_2)\in S\times S$ ставить у відповідність єдиний елемент $s = s_1\otimes s_2\in S$.

В такому випадку кажуть, що множина S *замкнена відносно операції* "$\otimes$". Також множину S називають *носієм* операції.

Означення 1.2: *алгебраїчна система* (з однією операцією) – це множина, на якій визначена операція. Аналогічно визначається алгебраїчна система з довільною кількістю операцій.

Операція, визначена на множині S, називається:

- *асоціативною*, якщо $\forall s_1, s_2, s_3\in S$: $(s_1\otimes s_2)\otimes s_3 = s_1\otimes(s_2\otimes s_3)$;

- *комутативною*, якщо $\forall s_1, s_2\in S$: $s_1\otimes s_2 = s_2\otimes s_1$.

Означення 1.3: *півгрупою* $(S, \otimes)$ називається множина S із асоціативною операцією $\otimes$. Якщо зрозуміло, про яку операцію йде мова, то півгрупу можна позначати просто S.

Означення 1.4: *моноїдом* $(M, \otimes)$ називається множина M з операцією $\otimes$ такою, що

1) $\otimes$ – асоціативна операція,

2) $\exists e\in M\ \forall m\in M$: $e\otimes m = m\otimes e = m$.

Елемент e називають *одиничним*, або *нейтральним* елементом, або просто одиницею.

Іншими словами, моноїд – це півгрупа з одиницею.

Означення 1.5: *групою* $(G, \otimes)$ називається множина G з операцією $\otimes$ такою, що

1) $\otimes$ – асоціативна операція;

2) $\exists e \in G \ \forall g \in G$: $e \otimes g = g \otimes e = g$;

3) $\forall g \in G \ \exists g^{-1} \in G$: $g^{-1} \otimes g = g \otimes g^{-1} = e$.

Елемент g^{-1} називають елементом, *оберненим* до g. Таким чином, групою є моноїд, в якому для кожного елемента існує обернений. Операція $\otimes$ у групі називається *груповою операцією*.

Часто групову операцією називають *множенням* і замість $a \otimes b$ використовують позначення ab для спрощення позначень, якщо це не викликає непорозумінь. Але при цьому слід розуміти, що елементи a, b, як і добуток ab, не є, взагалі кажучи, числами, і добуток ab не є звичайним числовим добутком.

Одиничний елемент групи часто позначають 1 або, якщо треба підкреслити, що даний елемент належить саме групі G, то використовують позначення 1_G.

Група називається *абелевою*, якщо операція $\otimes$ комутативна.

У абелевій групі групову операцію часто називають *додаванням* і замість $a \otimes b$ використовують позначення $a+b$. При цьому також слід пам'ятати, що вирази a, b та $a+b$ не є, взагалі кажучи, числами; це елементи довільної групи. Також у абелевій групі одиничний елемент часто називають *нульовим* елементом, або *нулем* групи, і позначають 0; елемент, обернений до елемента a, часто замість a^{-1} (читається "a в мінус першому степені") позначають $-a$ (читається "мінус a") і називають *протилежним* елементом елемента a. Замість $b + (-a)$ пишуть $b - a$.

Приклади 1.1.

1. Множина S_n підстановок довжини n утворює групу відносно операції суперпозиції. Ця група має назву симетричної групи.

2. Множина дійсних чисел **R** утворює абелеву групу відносно операції додавання +.

3. Множина **R**/{0} дійсних чисел без нуля утворює абелеву групу відносно операції множення.

4. Множина **N** натуральних чисел утворює півгрупу відносно операції додавання +.

5. Множина **N** натуральних чисел утворює моноїд відносно операції множення.

6. Множина цілих чисел **Z** утворює абелеву групу відносно операції додавання.

7. Множина цілих чисел **Z** утворює моноїд відносно операції множення.

8. Множина M_n матриць розмірності $n \times n$ утворює абелеву групу відносно операції додавання.

9. Множина M_n матриць розмірності $n \times n$ утворює моноїд відносно операції множення.

Твердження 1.1 (властивості елементів групи).

1. Одиничний елемент e у моноїді єдиний.

Доведення: нехай e' – також одиничний елемент. Тоді $e = ee' = e'$.

2. Нехай $(G, \cdot)$ – група. Тоді $\forall a, b \in G \ \exists! c \in G$: $a = b \cdot c$ і $\exists! d \in G$: $a = d \cdot b$.

Доведення: $c = b^{-1} \cdot a$; $d = a\, b^{-1}$.

3. Нехай $(G, \cdot)$ – група. Тоді:

а) $\forall a \in G \ \exists! a^{-1}$; б) $\forall a \in G \ (a^{-1})^{-1} = a$; в) $\forall a, b \in G \ (a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

4. Нехай $(S, \otimes)$ – група, $G \subset S$. Тоді $(G, \otimes)$ – група тоді й тільки тоді, якщо $\forall a, b \in G$: $a \cdot b^{-1} \in G$.

Пункти 3, 4 твердження 1.1 рекомендується довести самостійно.

Приклад 1.2: розглянемо важливий приклад групи – *групу лишків* за модулем n.

Для будь-яких $a \in \mathbf{Z}$, $n \in \mathbf{N}$ позначимо $a \bmod n$ лишок від (цілочислового) ділення a на n: $0 \le a \bmod n < n$, $a = kn + a \bmod n$ для деякого $k \in \mathbf{Z}$, де k називається часткою від ділення a на n. Також позначимо $\mathbf{Z}_n = \{0, 1, ..., n-1\}$. Множина $\mathbf{Z}_n$ з операцією $\oplus$ (іноді просто $+$), де $a \oplus b = (a + b) \bmod n$, називається *групою лишків за модулем n*.

Доведемо, що множина $\mathbf{Z}_n$ є групою відносно операції $\oplus$.

Очевидно, що множина $\mathbf{Z}_n$ замкнена відносно заданої операції. Далі, операція $\oplus$ – асоціативна, оскільки

$$(a \oplus b) \oplus c = (a + b + c) \bmod n = a \oplus (b \oplus c).$$

Нейтральним елементом відносно заданої операції є елемент $e = 0$; до кожного елемента $a \in \mathbf{Z}_n$ існує протилежний елемент $-a = n - a$. Доведення закінчено.

Розглянемо відображення $\mathbf{Z} \to \mathbf{Z}_n$, визначене таким чином:

$$a \in \mathbf{Z} \to a \bmod n \in \mathbf{Z}_n. \qquad (1.1)$$

Таке відображення розбиває множину $\mathbf{Z}$ на класи, що не перетинаються:

$$\mathbf{Z} = [0] \cup [1] \cup [2] \cup [3] \cup \ldots \cup [n-1], \qquad (1.2)$$

де клас $[i]$ складається з усіх прообразів елемента i при вказаному відображенні, тобто всіх таких цілих чисел, які дають залишок i при діленні на n.

Означення 1.6: нехай $a, b \in \mathbf{Z}$, $n \in \mathbf{N}$. Будемо записувати $a \equiv b \bmod n$ і говорити, що "*a конгруентно b* за модулем *n*", якщо образи a, b при відображенні (1.1) належать одному класу з розбиття (1.2).

Легко помітити, що нижченаведені три твердження є еквівалентними:

1) $a \equiv b \bmod n$; 2) $a - b = kn$ для деякого $k \in \mathbf{Z}$; 3) $a \bmod n = b \bmod n$.

Вираз $a \equiv b (\bmod n)$ називається *конгруенцією*, або *порівнянням*.

Означення 1.7: група G називається *скінченною* (*нескінченною*), якщо вона складається із скінченної (нескінченної) кількості елементів. *Порядком* скінченної групи G називається число елементів групи; порядок групи позначається $|G|$. Порядок нескінченної групи вважається рівним нескінченності.

Скінченні групи можна задавати у вигляді таблиці групової операції, або таблиці Келі.

Приклад 1.3: таблиця Келі для $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ відносно операції додавання за модулем 5.

$\oplus$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Таблиця Келі для групи є симетричною відносно головної діагоналі тоді і тільки тоді, коли група є абелевою.

Таблиця Келі для групи порядку n утворює так званий *латинський квадрат* розмірності $n \times n$, тобто таку квадратну таблицю, у якій кожен з n елементів зустрічається рівно один раз у кожному стовпці і у кожному рядку.

1.2 Підгрупи, класи суміжності. Теорема Лагранжа

Означення 1.8: *підгрупою* H групи G називається така її підмножина H, що теж є групою відносно тієї ж самої групової операції, що визначена у групі G.

Кожна група G має дві *тривіальні* підгрупи: $\{e\}$ і G. Всі інші підгрупи (якщо вони існують) називаються *власними*.

Приклади 1.4.

1. $(\mathbf{Z}, +)$ є підгрупою групи $(\mathbf{R}, +)$.

2. Нехай G – група, $a \in G$. Розглянемо множину $\langle a \rangle = \{a^k, k \in \mathbf{Z}\}$, де $a^k = \underbrace{a \cdot a \cdot \ldots \cdot a}_{k \text{ разів}}$, $a^{-k} = (a^{-1})^k$, $a^0 = e$. Очевидно, що $\langle a \rangle$ – підгрупа групи G. Таку підгрупу називають підгрупою, *породженою* елементом a.

Означення 1.9: нехай G – група, $a \in G$. Якщо існує таке $n \in \mathbf{N}$, що $a^n = e$, то число $\operatorname{ord} a = \min\{n \in \mathbf{N}: a^n = e\}$ називається *порядком* елемента a (у групі G). У іншому випадку (якщо не існує такого $n \in \mathbf{N}$, що $a^n = e$) вважається, що $\operatorname{ord} a = \infty$. Якщо $\operatorname{ord} a < \infty$, то a називається *елементом скінченного порядку*; в іншому випадку a – *елемент нескінченного порядку*.

Зрозуміло, що при $|G| < \infty$ для будь-якого елемента $a \in G$ виконується: $\operatorname{ord} a < \infty$. Дійсно, за означенням операції, $\forall k \geq 1$: $a^k \in G$, тому кількість різних степенів елемента a скінченна. Відповідно, для деяких $l, m \in \mathbf{N}$ $(l > m)$: $a^l = a^m$, тобто $a^{l-m} = e$.

Також очевидно, що $\operatorname{ord} a \leq |G|$, і якщо $\operatorname{ord} a = n$, то $a^{n-1} = a^{-1}$.

В абелевій групі замість a^n пишуть *na*.

В нескінченній групі можуть існувати елементи скінченного порядку. Наприклад, порядок нейтрального елемента будь-якої групи дорівнює 1.

Приклади 1.5.

1) Нехай $G = \mathbf{Z}_5$ (групова операція – додавання за модулем 5); $a = 3$. Тоді $\operatorname{ord} a = 5$. Дійсно, $\operatorname{ord} a \neq 1$, оскільки $a \neq 0$; далі, $a + a = 1$, $a + a + a = 4$, $a + a + a + a = 2$, $a + a + a + a + a = 0$, отже, $\operatorname{ord} a = 5$.

2) У групі $(\mathbf{Z}, +)$ будь-який елемент $a \neq 0$ є елементом нескінченного порядку.

Означення 1.10: група G називається *циклічною* групою, якщо

$$\exists g \in G \; \forall a \in G \; \exists k \in \mathbf{Z} : a = g^k.$$

Тоді елемент g називають *твірним* (*породним*, *утворювальним*) елементом групи G, або її *генератором*, а групу G – циклічною групою, *породженою* елементом g.

Іншими словами, група G називається циклічною, якщо існує такий елемент $g \in G$, що $G = \langle g \rangle$.

Якщо g – твірний елемент групи G, то зрозуміло, що ord $g = |G|$ (у тому числі для нескінченної групи).

Зауваження 1.1: в наших позначеннях $a \equiv b \pmod{n} \Leftrightarrow a - b \in \langle n \rangle$, де $\langle n \rangle$ – підгрупа групи $(\mathbf{Z}, +)$, породжена елементом n, тобто $\langle n \rangle = \{kn, k \in \mathbf{Z}\}$.

Приклад 1.6. Група $(\mathbf{Z}, +)$ – нескінченна циклічна група, яка має два твірні елементи: $+1$ та -1. Для будь-якого $n \in \mathbf{Z}$ підгрупа $\langle n \rangle$ групи $\mathbf{Z}$ також є циклічною з твірними елементами n та $-n$.

Будь-яка нескінченна циклічна група G з твірним елементом a взаємно-однозначно відображається на $(\mathbf{Z}, +)$ відображенням $a^k \to k$, $k \in \mathbf{Z}$, $a \in G$.

Нехай далі H – підгрупа групи G; $g_1, g_2 \in G$.

Означення 1.11 (узагальнення конгруенції (порівняння): будемо говорити, що $g_1 \equiv g_2 \bmod H$ ("елемент g_1 *конгруентний* елементу g_2 *за модулем підгрупи* H"), якщо $g_1^{-1} \cdot g_2 \in H$.

Останній вираз рівносильний кожному з виразів $g_2^{-1} \cdot g_1 \in H$ та $\exists h \in H: g_2 = g_1^{-1} \cdot h$.

Вирази $g_2^{-1} \cdot g_1$ та $g_1^{-1} \cdot g_2$ називають *лівими різницями* елементів g_1 та g_2; вирази $g_2 \cdot g_1^{-1}$ та $g_1 \cdot g_2^{-1}$, відповідно, *правими різницями*. Легко довести, що $g_2^{-1} \cdot g_1 \in H$ тоді і тільки тоді, коли $g_1^{-1} \cdot g_2 \in H$; аналогічне твердження виконується і для правих різниць.

Теорема 1.1: відношення $g_1 \equiv g_2 \bmod H$ є відношенням еквівалентності.

Доведення:

1) рефлексивність: $g_1 = g_1 e$, $e \in H$;

2) симетричність: $g_1 \equiv g_2 \bmod H \Rightarrow g_1 = g_2 h$, $h \in H \Rightarrow g_2 = h^{-1} g_1$, $h^{-1} \in H \Rightarrow g_2 \equiv g_1 \bmod H$;

3) транзитивність: $g_1 \equiv g_2 \bmod H$, $g_2 \equiv g_3 \bmod H \Rightarrow g_1 = g_2 h_1$, $g_2 = g_3 h_2 \Rightarrow g_1 = g_3 h_2 h_1$, $h_2 h_1 \in H \Rightarrow g_1 \equiv g_3 \bmod H$. Теорему доведено.

Означення 1.12: нехай $a \in G$. *Лівим класом суміжності* (або *суміжним класом*), що містить елемент a, групи G за підгрупою H називається множина $aH = \{ah_i,\ h_i \in H\}$. Елемент $a \in G$ називається *представником* класу суміжності aH.

Аналогічно визначається *правий клас суміжності*.

Клас суміжності за підгрупою H, який містить елемент $a \in G$, позначають $[a]$. Зрозуміло, що один і той же клас суміжності за підгрупою H можна і отримати, і позначити різними способами.

Теорема 1.2 (властивості класів суміжності): нехай H – підгрупа групи G. Тоді справедливі такі твердження.

1. Клас суміжності aH складається рівно з $|H|$ елементів, тобто кількість елементів кожного класу суміжності за групою H однакова і $\forall a \in G$: $|aH| = |H|$. (Для нескінченного класу суміжності ми говоримо, що множини H і aH рівнопотужні).

2. $\forall a, b \in G : aH = bH \Leftrightarrow b^{-1} a \in H$, тобто два класи суміжності за підгрупою збігаються тоді й тільки тоді, коли ліва різниця їх представників належить цій підгрупі.

3. $\forall a, b \in G$: або $aH = bH$, або $aH \cap bH = \varnothing$, тобто два класи суміжності за підгрупою або збігаються, або не перетинаються.

Доведення. 1. Достатньо довести, що відображення $H \to aH$, задане за правилом $H \ni h \to ah \in aH$, є взаємно однозначним. Воно є сюр'єктивним за побудовою. Доведемо ін'єктивність (від супротивного). Нехай для деяких

елементів $h_1 \neq h_2$ підгрупи H виконується $ah_1 = ah_2$. Домножимо рівність зліва на a^{-1} і отримаємо $h_1 = h_2$, що призводить до суперечності. Першу властивість доведено.

2. Нехай $aH = bH$. Тоді $\forall h_1 \in H \quad \exists h_2 \in H$: $ah_1 = bh_2$, звідки $b^{-1}a = h_2 h_1^{-1} \in H$.

Нехай тепер $b^{-1}a = h' \in H$. Тоді $a = bh'$ і $\forall ah \in aH$: $ah = bh'h \in bH$, оскільки $h'h \in H$, тобто $aH \subset bH$. Аналогічно доводиться, що $bH \subset aH$, звідки $aH = bH$. Другу властивість доведено.

3. Нехай $aH \bigcap bH \neq \varnothing$. Тоді $\exists u \in aH \bigcap bH$, тобто $\exists h_1, h_2 \in H$: $u = ah_1 = bh_2$. Але тоді $b^{-1}a = h_2 h_1^{-1} \in H$, та, за властивістю 2, $aH = bH$. Третю властивість доведено.

Наслідок 1.1: або $b^{-1}a \in H$; або $aH \bigcap bH = \varnothing$.

Наведемо ще одну властивість класів суміжності.

Твердження 1.2: нехай H – підгрупа групи G. Тоді для будь-яких $m_1, m_2 \in G$ справедливо твердження: m_1, $m_2 \in aH$ для деякого $a \in G$ (тобто обидва елементи належать одному класу суміжності за підгрупою H) тоді і тільки тоді, коли $m_2^{-1}m_1 \in H$.

Доведення: нехай $m_1, m_2 \in aH$ для деякого $a \in G$. Це означає, що $m_1 = ah_1$, $m_2 = ah_2$ для деяких $h_1, h_2 \in H$. Тоді $m_2^{-1}m_1 = h_2^{-1}a^{-1}ah_1 = h_2^{-1}h_1 \in H$ за теоремою 1.2 (властивістю 2).

Нехай $m_2^{-1}m_1 \in H$. Тоді $m_1 = m_2 h$ для деякого $h \in H$. Нехай $m_2 \in aH$, тобто $m_2 = ah_1$ для деякого $h_1 \in H$. Тоді $m_1 = ah_1 h \in aH$, оскільки $h_1 h \in H$, внаслідок замкненості підгрупи H відносно операції. Твердження доведено.

Означення 1.13: якщо H – підгрупа групи G і кількість (різних) лівих суміжних класів групи G за підгрупою H скінченна, то *індексом* підгрупи H у групі G називається кількість різних суміжних класів групи G за підгрупою H. Індекс підгрупи H у групі G позначається $(G: H)$. Якщо

кількість (різних) лівих суміжних класів G по H нескінченна, то $(G: H) = \infty$.

Якщо G – скінченна, то індекс групи G за будь-якою підгрупою теж скінченний. В противному випадку індекс групи може бути і скінченною, і нескінченною величиною. Наприклад: $(\mathbf{Z}: <n>) = n$, оскільки різні суміжні класи $\mathbf{Z}$ по $<n>$ – це класи $<n> + 0, <n> + 1, \ldots, <n> + (n-1)$; при цьому $|\mathbf{Z}| = \infty$, $|<n>| = \infty$.

Теорема 1.3 (теорема Лагранжа): нехай G – скінченна група. Тоді

$$|G| = (G: H) \cdot |H|. \qquad (1.3)$$

Доведення: нехай $(G: H) = k$. З теореми 1.2 (властивість 3) випливає, що групу G можна подати у вигляді об'єднання різних лівих класів суміжності за підгрупою H: $G = \bigcup_{i=1}^{k} a_i H$ для деяких $a_i \in G$, $i = \overline{1,k}$, причому $a_i H \cap a_j H = \varnothing$. Кожен з класів суміжності (властивість 1) містить $|H|$ елементів. Отже, $|G| = k \cdot |H|$, і теорему доведено.

Наслідок 1.2: порядок будь-якої підгрупи H групи G ділить порядок групи G.

Доведення випливає безпосередньо з формули (1.3).

Наслідок 1.3: порядок елемента скінченної групи ділить порядок групи.

Доведення: 1) Спочатку доведемо, що порядок елемента скінченної групи є скінченним. Нехай G – група, $|G| = n$, $a \in G$. Розглянемо множину $\{a, a^2, \ldots, a^n, a^{n+1}\}$. Всі елементи даної множини є елементами G; оскільки їх $n+1$, то серед них є однакові: $\exists 1 \le i < j \le n+1 : a^i = a^j$, звідки $a^{j-i} = e$, отже, $\operatorname{ord} a \le j - i \le n$.

2) Нехай $\operatorname{ord} a = l$. Розглянемо підгрупу $H = \langle a \rangle$. Легко довести, що $|H| = \operatorname{ord} a$, і за наслідком 1.2 $|H| \,\big|\, |G|$, отже, $\operatorname{ord} a \,\big|\, |G|$.

Наслідок 1.4: нехай $|G| = n$. Тоді $\forall a \in G : a^n = e$.

Доведення випливає з наслідку 1.3 та з означення порядку елемента.

Питання для самоконтролю до §1

1. Які операції називають бінарними? Поясніть, що таке комутативність та асоціативність операції, а також дистрибутивність однієї операції відносно іншої.

2. Що називають алгебраїчною системою?

3. Дайте означення півгрупи, моноїда, групи, нейтрального елемента, оберненого елемента.

4. В чому різниця понять "порядок елемента" та "порядок групи"?

5. Що таке таблиця Келі для групової операції?

6. Дайте означення класу суміжності та назвіть властивості класів суміжності.

7. Сформулюйте теорему Лагранжа та її наслідки.

Задачі до §1

(Тут і надалі задачі підвищеної складності позначено зірочками).

1. Довести пункти 3, 4 твердження 1.1 §1.

2. Довести асоціативність множення в $(\mathbf{Z}_n, \otimes)$, де під операцією $\otimes$ розуміється множення за модулем n. Чи буде дана алгебраїчна система групою?

3. Нехай $(H, \otimes)$ – деякий моноїд. Елемент $h \in H$ будемо називати *оборотним*, якщо $\exists h' \in H : hh' = h'h = e$ (тобто якщо у моноїді H існує елемент, обернений до h).

Довести, що множина всіх оборотних елементів моноїда H утворює групу відносно заданої на ньому операції.

Зокрема, множина оборотних елементів в моноїді $(\mathbf{Z}_n, \otimes)$, де $\otimes$ є операцією множення за модулем n, утворює групу відносно цієї операції. Ця група позначається $\mathbf{Z}_n^*$.

4. Які з наведених нижче алгебраїчних систем $(\mathbf{Z}_n\backslash\{0\}, \otimes)$ є групами відносно операції $a \otimes b = ab \bmod n$? Чи будуть вони всі моноїдами?

$$\mathbf{Z}_4, \mathbf{Z}_5, \mathbf{Z}_6, \mathbf{Z}_7, \mathbf{Z}_9, \mathbf{Z}_{11}.$$

5. Побудувати таблиці Келі для $\mathbf{Z}_5^*$, $\mathbf{Z}_9^*$, $\mathbf{Z}_{11}^*$ (див. задачу 3) відносно операції, визначеної в задачі 4, та визначити порядки всіх елементів у цих групах.

6. У групах із завдання 4 знайти порядки всіх елементів.

7. Знайти твірні елементи у групах $(\mathbf{Z}_{13}, \oplus)$ та $(\mathbf{Z}_{13}^*, \otimes)$, з операціями додавання та множення за модулем n, відповідно.

8. Нехай G – група, $a \in G$, ord $a = k$. Довести: $a^m = e \Leftrightarrow k \mid m$. (Дане твердження варто було б назвати четвертим наслідком теореми Лагранжа, оскільки воно випливає з цієї теореми і дуже часто використовується при аналізі властивостей елементів скінченних груп).

9. Нехай $(\mathbf{Z},+)$ – множина цілих чисел з операцією додавання, $k, n \in Z$, $k\mathbf{Z}$ та $n\mathbf{Z}$ – циклічні підгрупи групи $\mathbf{Z}$, породжені елементами k та n, відповідно. Довести: $k\mathbf{Z}$ є підгрупою $n\mathbf{Z}$ тоді і тільки тоді, коли число n є дільником числа k.

10*. Навести приклад групи, в якій є елементи будь-яких натуральних порядків і елементи нескінченного порядку.

11. Сформулювати та довести аналог теорем 1.2 та 1.3 для правих класів суміжності.

12. Нехай H – підгрупа групи G. Чи справедливі нижченаведені твердження:

1) кількість лівих класів суміжності групи G за підгрупою H дорівнює кількості правих класів суміжності групи G за цією підгрупою;

2) $aH = bH \Leftrightarrow Ha = Hb$?

Довести або навести контрприклади.

13. Довести, що таблиця Келі для групової операції утворює латинський квадрат.

§2 ВЛАСТИВОСТІ ЦИКЛІЧНИХ ГРУП. ВІДОБРАЖЕННЯ ГРУП

2.1 Властивості циклічних груп

Для подальшого викладення нам потрібно нижченаведене означення.

Означення 2.1: функція φ: $\mathbf{N}\to\mathbf{N}$, де $\varphi(n)$ дорівнює кількості натуральних чисел від 1 до n, взаємно простих з n, називається *функцією Ейлера.*

Теорема 2.1 (про властивості циклічних груп): нехай G – циклічна група, H – її підгрупа, a – твірний елемент групи G. Тоді справедливі такі твердження.

1. Кожна підгрупа циклічної групи також є циклічною.

2. Нехай G скінченна, $|G| = m$. Тоді:

2.1 $\operatorname{ord}(a^k) = \dfrac{m}{(k,m)}$;

2.2 для будь-якого натурального числа d, що є дільником числа m, група G містить:

2.2.1 єдину підгрупу індексу d;

2.2.2 єдину підгрупу порядку d;

2.2.3 рівно $\varphi(d)$ елементів порядку d (де $\varphi(\cdot)$ – функція Ейлера): це елементи вигляду a^{kr}, де $k = \dfrac{m}{d}$ та $(r, d) = 1$; зокрема, існує рівно $\varphi(m)$ твірних елементів: це елементи вигляду a^r, де $(r, m) = 1$.

Доведення. 1. Нехай H – підгрупа циклічної групи G, $H \neq \{e\}$. Якщо $H \supset a^k$, то $H \supset a^{-k}$; отже, H містить хоча б один елемент a^k, де $k > 0$.

Нехай $l = \min\{k > 0: a^k \in H\}$. Необхідно довести, що a^l – генератор H. Це рівносильно нижчевикладеному: якщо $a^n \in H$ для деякого натурального

n, то існує таке натуральне s, що $a^n = (a^l)^s$. Тобто, $a^n \in H$ тоді й тільки тоді, коли $l|n$. Доведення проводитимемо від супротивного. Нехай $n = sl + r$, $0 < r < l$. Тоді $a^r = a^n (a^{-l})^s$, де вираз у правій частині рівності належить H внаслідок замкненості підгрупи H відносно множення. Отже, $a^r \in H$, що суперечить вибору l та означенню r.

2.1. За означенням $\text{ord}(a^k) = \min\{n: a^{kn} = e\} = \min\{n: m|kn\}$. Позначимо $(m, k) = d$. Тоді $\text{ord}(a^k) = \min\{n: \frac{m}{d} | \frac{k}{d} n\} = \min\{n: \frac{m}{d} | n\} = \frac{m}{d}$ (оскільки $\left(\frac{m}{d}, \frac{k}{d}\right) = 1$).

Доведемо твердження з пункту 2.2. За теоремою Лагранжа, $|G| = (G: H) \cdot H$. Нехай $m = kd$. Тоді елемент a^d породжує підгрупу індексу d, її порядок дорівнює $\frac{m}{d} = k$, і за теоремою Лагранжа $(G: H) = \frac{m}{k} = d$. Така підгрупа єдина, оскільки дві підгрупи циклічної групи одного порядку збігаються. Дійсно, нехай $|\langle a^k \rangle| = |\langle a^l \rangle| \Rightarrow \frac{m}{(m,k)} = \frac{m}{(m,l)} \Rightarrow$ $\Rightarrow (m, k) = (m, l) = d$, де $d|m$, $d|l$, $d|k$. Але $(d, m) = d$ і $d|k$, отже, $|\langle a^k \rangle| \subset |\langle a^d \rangle|$, і їх порядок збігається: $|\langle a^k \rangle| = |\langle a^d \rangle|$, тому $\langle a^k \rangle = \langle a^d \rangle$. Аналогічно доводиться $\langle a^l \rangle = \langle a^d \rangle$; таким чином, отримаємо $\langle a^k \rangle = \langle a^l \rangle$. Твердження 2.2.1 доведено.

Твердження 2.2.2 доводиться аналогічно.

Доведемо 2.2.3. Нехай $m = dk$, тоді $\text{ord}\, a^k = d$. Нехай для деякого n $(1 \le n \le m)$ $\text{ord}(a^n) = d$. Тоді $\frac{m}{(n,m)} = d$ лише за умови $(n, m) = k$. Знайдемо кількість таких n $(1 \le n \le m)$, що $(n, m) = k$. Це будуть всі такі числа, що мають вигляд rk, де $r \le d$ і r взаємно просте з d (кількість таких r якраз і дорівнює $\varphi(d)$). Дійсно, за цієї умови $(rk, m) = (rk, dk) = k(r, d) = k$. Теорему доведено.

2.2 Відображення груп. Нормальні підгрупи. Терема про ізоморфізм груп

При порівнянні структур двох груп важливу роль відіграють такі відображення, що зберігають групові операції.

Нехай $(H, \cdot)$, $(G, \times)$ – групи.

Означення 2.2: відображення f: $H \to G$ називається:

- *гомоморфізмом*, якщо для будь-яких $h_1, h_2 \in H$: $f(h_1 \cdot h_2) = f(h_1) \times f(h_2)$;
- *мономорфізмом*, якщо f – гомоморфізм і ін'єкція;
- *ендоморфізмом*, якщо f – гомоморфізм і $H = G$;
- *епіморфізмом*, якщо f – гомоморфізм і сюр'єкція;
- *ізоморфізмом*, якщо f – гомоморфізм і бієкція;
- *автоморфізмом*, якщо f – ізоморфізм і $H = G$.

Будемо говорити, що група H *ізоморфна* групі G, і позначати $H \cong G$, якщо існує відображення $f: H \to G$, яке є ізоморфізмом. При цьому, внаслідок бієктивності відображення f, існує обернене відображення $f^{-1}: G \to H$; легко довести, що воно також є ізоморфізмом. Тому якщо H ізоморфна групі G, то G ізоморфна групі H. В цьому випадку кажуть, що групи G і H ізоморфні.

Поняття ізоморфізму та ізоморфних об'єктів є одним з центральних понять у алгебрі. Групи, що є ізоморфними, мають однакові (з точністю до позначень) таблиці Келі, і тому вважаються однаковими. Наприклад, кажуть, що існує єдина (з точністю до ізоморфізму) група порядку 2; існує єдина (з точністю до ізоморфізму) група порядку 3; існує єдина (з точністю до ізоморфізму) нескінченна циклічна група – це група цілих чисел з операцією додавання.

Приклад 2.1: розглянемо групи $(\mathbf{Z}, +)$, $(\mathbf{Z}_n, \oplus)$ та відображення f: $\mathbf{Z} \to \mathbf{Z}_n$; $f(a) = a \bmod n$. Тоді

$$f(a+b) = (a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n = f(a) \oplus f(b),$$

отже, задане відображення є гомоморфізмом. Воно також є епіморфізмом, але не є ізоморфізмом.

Твердження 2.1: якщо f: $H \to G$ – гомоморфізм, то $f(e_H) = e_G$ і $f(a^{-1}) = f(a)^{-1}$, де під e_H та e_G розуміємо одиничні елементи груп H і G, відповідно, під a^{-1} розуміємо елемент групи H, обернений до елемента $a \in H$, а під $f(a)^{-1}$ розуміємо елемент групи G, обернений до елемента $f(a) \in G$.

Твердження 2.2: автоморфізми групи G утворюють групу відносно операції композиції.

Твердження 2.1, 2.2 рекомендується довести самостійно.

Означення 2.3: нехай f: $G \to H$ – гомоморфізм.

Ядром гомоморфізму f називається множина $\ker f = \{g \in G: f(g) = e_H\}$ (зрозуміло, що $e_G \in \ker f$).

Образом гомоморфізму f називається множина $\operatorname{Im} f = \{h \in H: \exists g \in G, f(g) = h\}$.

Приклад 2.2: розглянемо відображення f: $\mathbf{Z} \to \mathbf{Z}_n$, $f(a) = a \bmod n$. Тоді $\ker f$ = {всі числа, кратні n} = $n\mathbf{Z}$.

Означення 2.4: підгрупа $H \subset G$ називається *нормальною* підгрупою групи G (або *нормальним дільником* групи G; позначається $H \lhd G$), якщо $\forall h \in H \; \forall g \in G$: $ghg^{-1} \in H$ (або, що рівносильно, $g^{-1}Hg \subset H$).

Приклад 2.3: нормальною підгрупою є будь-яка підгрупа абелевої групи; нормальною підгрупою є ядро гомоморфізму груп.

Теорема 2.2 (критерій нормальності): нижченаведені умови рівносильні:

1) $H \subset G$ – нормальна підгрупа;

2) $H = g^{-1}Hg$, тобто H інваріантна відносно всіх внутрішніх автоморфізмів;

3) $\forall a \in G$: $aH = Ha$ (лівий клас суміжності за підгрупою H збігається з правим).

Доведення: доведемо, що з першого твердження випливає друге. Якщо H – нормальна підгрупа, то для будь-якого $g \in G$ співвідношення $g^{-1}Hg \subset H$ справедливе за означенням. Покажемо, що $H \subset g^{-1}Hg$, тобто $\forall h \in H\ \exists g \in G\ \exists h_1 \in H$: $h = g^{-1}h_1 g$. Оберемо довільні елементи $h \in H$ і $g \in G$ і покладемо $h_1 = ghg^{-1}$. Тоді $h_1 \in H$, за означенням нормальної підгрупи, і, крім того, для нього виконується співвідношення $h = g^{-1}h_1 g$. Тоді $h_1 = ghg^{-1}$ і є шуканий елемент.

Доведемо, що з другого твердження випливає третє. Нехай $H = g^{-1}Hg$. Якщо всі елементи обох множин у лівій і правій частині рівності домножити зліва на один і той же елемент g, то отримані множини також будуть рівними, тобто отримаємо рівність $gH = Hg$.

Аналогічно доводиться, що з третього твердження випливає перше. Теорему доведено.

Нехай і надалі H підгрупа деякої групи G. На множині (лівих) класів суміжності групи G за підгрупою H задамо наступну операцію:

$$(aH)(bH) = (ab)H. \qquad (2.1)$$

Нижченаведена терема є надзвичайно важливою при подальшому вивченні алгебраїчних структур.

Теорема 2.3: якщо H – нормальна підгрупа групи G, то множина (лівих) класів суміжності утворює групу відносно операції (2.1).

Доведення: достатньо довести, що операція (2.1) задана коректно. Виконання інших умов, таких як асоціативність заданої операції, наявність одиничного елемента (eH – одиничний елемент) та оберненого елемента відносно даної операції ($(aH)^{-1}=a^{-1}H$), а також замкненість відносно неї множини класів суміжності перевіряється безпосередньо за означенням операції.

Під коректністю операції розуміється нижчевикладене. Оскільки один клас суміжності можна отримати різними способами (за властивістю 2 класів суміжності, теорема 1.2, $a_1H = a_2H \Leftrightarrow a_2^{-1}a_1 \in H$), необхідно довести, що операція (2.1) не залежить від того, як саме буде подано клас суміжності. Тобто, нам необхідно довести: якщо $a_1H = a_2H$ та $b_1H = b_2H$ для деяких $a_1, a_2, b_1, b_2 \in G$, то $(a_1H)(b_1H)=(a_2H)(b_2H)$, тобто $a_1b_1H=a_2b_2H$.

Якщо виконуються рівності $a_1H = a_2H$ та $b_1H = b_2H$, тоді, за властивістю 2 класів суміжності (теорема 1.2), $\exists h_1, h_2 \in H : a_2^{-1}a_1 = h_1, b_2^{-1}b_1 = h_2$. За тією ж властивістю, для доведення рівності $a_1b_1H=a_2b_2H$ достатньо довести, що $(a_2b_2)^{-1}(a_1b_1) \in H$. Позначимо $(a_2b_2)^{-1}(a_1b_1) = h$. Тоді $h = b_2^{-1}a_2^{-1}a_1b_1 = b_2^{-1}h_1b_1 = b_2^{-1}h_1h_2b_2$, оскільки $b_1 = h_2b_2$. Але $h_1h_2 \in H$ внаслідок замкненості підгрупи H відносно операції, і тому, внаслідок нормальності підгрупи H, $b_2^{-1}h_1h_2b_2 \in H$. Теорему доведено.

Зауважимо, що умова нормальності підгрупи H є суттєвою при доведенні даної теореми.

З теореми 2.3 випливає, що операцію над класами суміжності можна виконувати таким чином:

- вибрати представника ah_1 класу aH;

- вибрати представника bh_2 класу bH;

- визначити, в який клас суміжності потрапить елемент ah_1bh_2, і цей клас суміжності назвати результатом операції $(aH)(bH)$.

При цьому результат операції не залежатиме від вибору представників класів суміжності, тобто, незалежно від вибору h_1 і h_2 буде виконуватись співвідношення $ah_1bh_2 \in abH$. Дійсно, для доведення цього співвідношення достатньо довести, що $\exists h \in H$: $ah_1bh_2 = abh$, тобто, $b^{-1}h_1bh_2 = h$. Але за означенням нормальної підгрупи $b^{-1}h_1b \in H$, відповідно $h=b^{-1}h_1bh_2 \in H$.

Така інтерпретація операції над класами суміжності дає можливість від операції над множинами (класами суміжності) перейти до операції над

їх елементами. З кожного класу суміжності групи G за підгрупою H обираємо по одному елементу; обрані елементи утворюють так звану *систему представників*. Для будь-якого $a \in G$ представник класу суміжності $[a]$ позначається $\bar{a}$. Далі від операції над класами суміжності ми переходимо до операції над їх представниками таким чином: якщо $\bar{a} \in [a]$ та $\bar{b} \in [b]$, то $\bar{a}\bar{b} = \bar{c}$, де $\bar{c}$ – представник класу суміжності, що містить елемент.

Означення 2.5: нехай H – нормальна підгрупа G. *Факторгрупою* групи G за підгрупою H називається група, утворена (лівими) класами суміжності, з операцією (2.1). Ця група позначається G/H.

Зауваження 2.1: порядок факторгрупи G/H дорівнює кількості класів суміжності групи G за підгрупою H (індексу $(G: H)$ підгрупи H у групі G). Якщо $|G| < \infty$, то $|G/H| = \dfrac{|G|}{|H|}$, за теоремою Лагранжа.

Покажемо, що з кожною нормальною підгрупою H групи G пов'язаний деякий гомоморфізм. Має місце така теорема.

Теорема 2.4: (про ізоморфізм груп).

1) Нехай $\varphi: G \to G_1$ – гомоморфізм груп. Тоді $\ker\varphi$ – нормальна підгрупа в G і $G/\ker\varphi \cong \mathrm{Im}\varphi$. (Тобто, факторгрупа за ядром гомоморфізму ізоморфна образу цього гомоморфізму).

2) Нехай H нормальна підгрупа групи G. Тоді відображення $\varphi: G \to G/H$, де $\varphi(g) = gH$, є гомоморфізмом, і при цьому $\ker\varphi = H$. (Іншими словами, кожна нормальна підгрупа H групи G задає деякий гомоморфізм з групи G у її факторгрупу G/H).

Доведення. 1) Доведемо, що $\ker\varphi$ – нормальна підгрупа в G. Потрібно довести, що для будь-яких $g \in G, h \in \ker\varphi: g^{-1}hg \in \ker\varphi$, тобто, $\varphi(g^{-1}hg) = e_{G_1}$. Дійсно, за означенням гомоморфізму та внаслідок того, що $\varphi(h) = e_{G_1}$, отримаємо:

$$\varphi\left(g^{-1}hg\right)=\varphi\left(g^{-1}\right)\varphi(h)\varphi(g)=\varphi\left(g^{-1}\right)e_{G_1}\varphi(g)=$$

$$=\varphi(g)^{-1}e_{G_1}\varphi(g)=\varphi(g)^{-1}\varphi(g)=e_{G_1}.$$

Доведемо ізоморфність $G/\ker f\cong \mathrm{Im} f$. За означенням ізоморфних груп, нам треба побудувати відображення $\varphi: G/\ker f\to \mathrm{Im} f$, яке є ізоморфізмом. Побудуємо це відображення так:

$$\forall g\in G:\varphi\left(g\ker\varphi\right)=\varphi(g)\in \mathrm{Im}\,\phi.$$

Зауважимо, що відображення задано коректно. Дійсно, за п. 2 властивостей класів суміжності (теорема 1.2), для кожного прообразу існує єдиний образ, який не залежить від виду подання аргументу.

Легко бачити, що дане відображення є гомоморфізмом. Також воно буде сюр'єктивним, оскільки за означенням образу гомоморфізму $\forall a\in \mathrm{Im}\varphi\exists g\in G:\varphi(g)=a$, тоді $\varphi\left(g\ker\varphi\right)=a$, тобто для будь-якого $a\in \mathrm{Im}\varphi\exists g\in G:\varphi\left(g\ker\varphi\right)=a$.

Доведемо ін'єктивність даного відображення. Нехай для деяких $g_1,g_2\in G$ виконується рівність $\varphi\left(g_1\ker\varphi\right)=\varphi\left(g_2\ker\varphi\right)$. За означенням відображення φ це означає, що $\varphi\left(g_1\right)=\varphi\left(g_2\right)$. Але при цьому буде виконуватись $\varphi\left(g_2^{-1}g_1\right)=e_{G_1}$, тобто $g_2^{-1}g\in\ker\varphi$, що означає рівність прообразів $g_1\ker\varphi=g_2\ker\varphi$, за властивістю 2 класів суміжності (теорема 1.2).

2) Нехай H нормальна підгрупа групи G. Доведемо, що відображення $\varphi: G\to G/H$, де $\varphi(g)=gH$, є гомоморфізмом. Дійсно, $\varphi\left(g_1g_2\right)=g_1g_2H=\left(g_1H\right)\left(g_2H\right)=\varphi\left(g_1\right)\varphi\left(g_2\right)$, де перша рівність виконується за означенням відображення φ, а друга – за означенням операції (2.1) на класах суміжності.

Доведемо, що $\ker \varphi = H$. Нехай $h \in H$. Тоді $\varphi(h) = hH = H = eH$, де клас суміжності eH і є нейтральним елементом групи G/H, що й означає $h \in \ker \varphi$. І навпаки, якщо $h \in \ker \varphi$, то $\varphi(h) = hH = H = eH$, і за властивістю 2 класів суміжності (теорема 1.21) $e^{-1}h = eh = h \in \ker \varphi$. Теорему доведено.

2.3 Внутрішні автоморфізми групи та спряжені елементи

Означення 2.6: *внутрішнім автоморфізмом* групи G називається відображення f_a: $G \to G$, побудоване за правилом: $f(g) = aga^{-1}$, для деякого $a \in G$. Автоморфізми групи, які не є внутрішніми, інколи називають зовнішніми.

Кожен елемент групи $a \in G$ задає деякий внутрішній автоморфізм цієї групи, проте не обов'язково різні елементи задають різні автоморфізми.

Означення 2.7: нехай G – група, $g \in G$, $S \subset G$.

Елемент g називають *спряженим* з елементом $h \in G$, якщо існує такий елемент $a \in G$, що $h = aga^{-1}$. Очевидно, що при цьому $g = a^{-1}ha$, тобто елемент h також є спряженим з елементом g (тоді кажуть, що елементи h та g спряжені).

Означення 2.8: клас елементів, спряжених з елементом a, або *клас спряженості* групи G, який містить елемент a – це множина усіх елементів, спряжених з $a \in G$.

Відношення спряженості у групі G є відношенням еквівалентності на множині G (доведіть це самостійно), тому класи спряженості розбивають G на множини, які або збігаються, або не перетинаються, як і класи суміжності.

Множину P називають *спряженою* з множиною S, якщо існує такий елемент $a \in G$, що $P = aSa^{-1}$ (тобто $P = \{asa^{-1} : s \in S\}$). У цьому випадку множини S та P називають спряженими.

2.4 Нормалізатор множини. Центр групи

Нехай G – група, $S \subset G$.

Означення 2.9: *нормалізатором множини* $S \subset G$ називається множина

$$N(S) = \{a \in G: aSa^{-1} = S\}.$$

Приклад 2.4: нормалізатор нормальної підгрупи H – це вся група G.

Теорема 2.5: 1) $N(S)$ – підгрупа G;

2) $\forall a \in G: aN(S) = bN(S) \Leftrightarrow aSa^{-1} = bSb^{-1}$, тобто два класи суміжності за нормалізатором множини рівні тоді й лише тоді, коли рівні відповідні спряжені множини, а різним класам суміжності за підгрупою $N(S)$ відповідають різні множини, спряжені з S (інакше кажучи, існує бієкція між різними (лівими) суміжними класами $aN(S)$ за підгрупою $N(S)$ та різними множинами aSa^{-1}, спряженими з S).

Доведення: твердження 1) теореми доводиться безпосередньою перевіркою. Доведемо твердження 2). Покажемо, що рівності $aN(S) = bN(S)$ та $aSa^{-1} = bSb^{-1}$ рівносильні. Дійсно, домножуючи всі елементи рівних множин (у другій рівності) на однаковий елемент та скориставшись властивістю 2 класів суміжності (теорема 1.2), отримаємо такі рівносильні рівності:

$$aSa^{-1} = bSb^{-1} \Leftrightarrow S = a^{-1}bSb^{-1}a = (b^{-1}a)^{-1}S(b^{-1}a) \Leftrightarrow$$
$$\Leftrightarrow b^{-1}a \in N(S) \Leftrightarrow bN(S) = aN(S),$$

що й треба було довести.

Означення 2.10: *центром* групи G називається множина

$$C = \{c \in G: \forall a \in G,\ ca = ac\}.$$

Інакше кажучи, центр групи – це множина всіх таких елементів даної групи, які комутують з усіма її елементами.

Твердження 2.3: центр групи G є нормальною підгрупою.

Рекомендується довести дане твердження самостійно.

Теорема 2.6 (рівняння класів спряженості): нехай $|G| < \infty$. Тоді

$$|G| = |C| + \sum_{i=1}^{k} n_i, \qquad (2.2)$$

де n_i – потужності класів спряженості групи $|G|$, які містять не менше двох елементів ($n_i \geq 2$), і n_i є дільниками $|G|$.

Доведення: як було зазначено раніше, відношення спряженості є відношенням еквівалентності, тому воно розбиває групу на класи спряженості, що не перетинаються. Тому кількість елементів у групі дорівнює сумі кількостей елементів у цих класах спряженості. Очевидно, що клас спряженості деякого елемента a містить лише цей один елемент тоді і тільки тоді, коли $a \in C$, що доводить рівність (2.2) і той факт, що $n_i \geq 2$. Покажемо, що n_i є дільниками $|G|$. Нехай n_i – кількість елементів, спряжених з деяким елементом $a \in G$; тоді, за теоремою 2.5, кількість (різних) спряжених з a елементів дорівнює кількості (різних) лівих класів суміжності за підгрупою $N(a)$, тобто індексу підгрупи $N(a)$ у групі G. За теоремою Лагранжа (1.3) індекс підгрупи є дільником порядку групи G. Теорему доведено.

Питання для самоконтролю до §2

1. Яке значення приймає функція Ейлера, якщо її аргумент є простим числом?

2. Дайте означення циклічної групи та сформулюйте теорему про її властивості.

3. Дайте означення гомоморфізму груп. Наведіть приклади різних типів гомоморфізмів груп.

4. Чи можна у означенні 2.2 сказати, що відображення f: $H \to G$ називається автоморфізмом, якщо f – епіморфізм і $H = G$? Відповідь обгрунтуйте.

5. Дайте означення ядра гомоморфізму та образу гомоморфізму груп.

6. В чому різниця понять "факторгрупа" та "клас суміжності"?

7. Сформулюйте означення факторгрупи. Обгрунтуйте коректність операції у факторгрупі.

8. Які автоморфізми групи називають внутрішніми? зовнішніми?

9. Дайте означення нормальної підгрупи.

10. Сформулюйте теорему про ізоморфізм груп.

Задачі до §2

1. Довести: якщо f: $H \to G$ – гомоморфізм груп, то $f(e_H) = e_G$, $f(a^{-1}) = f(a)^{-1}$.

2. Довести: якщо f: $H \to G$ – ізоморфізм груп, то обернене до f відображення теж буде ізоморфізмом.

3. Довести: автоморфізми групи G утворюють групу відносно операції композиції.

4. Довести: ядро гомоморфізму є нормальною підгрупою.

5. Довести: два елементи групи належать одному лівому класу суміжності за підгрупою тоді і тільки тоді, коли їх ліва різниця (відносно групової операції) належить даній підгрупі. Сформулювати та довести аналогічне твердження для правих класів суміжності.

6. Довести: центр групи – нормальна підгрупа.

7. Нехай G – деяка група, $a, b \in G$. Довести: $f_a = f_b \Leftrightarrow a^{-1}b \in C$, де C – центр групи G, f_a та f_b – внутрішні автоморфізми.

8. Довести: кількість різних внутрішніх автоморфізмів скінченної групи G дорівнює числу класів суміжності групи G за центром C, тобто $\frac{|G|}{|C|}$.

9. Навести приклад автоморфізму групи, що не є внутрішнім.

10. Нехай p – просте число. Довести: $\varphi(p) = p - 1$; $\varphi(p^s) = p^s(1 - p^{-1})$, де φ – функція Ейлера.

11. Нехай m, n – різні прості. Довести:

$$\varphi(mn) = \varphi(m)\varphi(n) = (m-1)(n-1).$$

12. Знайти $\varphi(1155)$.

13. Довести: якщо для деякої групи G виконується $|G| = p^s$, де p – просте число, то порядок центра групи G ділиться на p.

14. Довести малу теорему Ферма: для простого p виконано $a^p \equiv a \pmod{p}$.

15. Довести теорему Вільсона: для простого p виконано $(p-1)! \equiv -1 \pmod{p}$.

16. Довести: будь-яка циклічна група є абелевою.

17. Нехай G – скінченна група, H – її підгрупа. Довести: кількість елементів у кожному класі суміжності за підгрупою H ділить порядок групи G.

18. Нехай G – деяка група, $a, b \in G$. Довести: елементи a, b належать одному класу спряженості тоді і тільки тоді, коли існує такий елемент $g \in G$, що $ga = bg$.

19. Довести: відображення f: $H \to G$ є ізоморфізмом тоді і тільки тоді, коли це відображення є епіморфізмом і його ядро складається з єдиного елемента (цей елемент є одиничним елементом групи H). Чи може ядро гомоморфізму бути порожньою множиною?

20. Довести: якщо відображення f: $H \to G$ є гомоморфізмом, то у кожного елемента, що належить Im f, кількість прообразів однакова; вона дорівнює кількості елементів ядра цього гомоморфізму.

21. Довести, що будь-яка нескінченна циклічна група ізоморфна групі цілих чисел з операцією додавання.

22. Довести, що відношення спряженості елементів у групі є відношенням еквівалентності.

23. Нехай f: $H \to G$ – гомоморфізм груп, $a \in H$, $ord\, a = m$. Довести: $ord\, f(a)$ ділить m. Зокрема, якщо f – ізоморфізм, то $ord\, f(a) = ord\, a$.

24. Нехай H – нормальна підгрупа групи G, $a, b \in G$, $aH = bH$. Довести: для будь-якого $c \in G$ виконується $acH = bcH$.

25. Нехай група G складається з матриць: $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $a_1 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $a_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $a_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $a_4 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $a_5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, а груповою операцією є множення матриць, причому всі дії з матричними елементами виконуються за модулем 2. Виконайте наведені нижче завдання.

25.1. Побудувати таблицю Келі для групи G.

25.2. Знайти порядки всіх її елементів, перевірити виконання наслідку 1.3 з теореми Лагранжа.

25.3. Знайти центр групи.

25.4. Розбити групу на класи спряженості та визначити їх потужності (тобто кількості елементів у кожному класі). Перевірити виконання рівняння класів спряженості (з §2).

25.5. Для всіх елементів групи знайти $N(a_i)$.

25.6. Чи буде група G циклічною? Знайти всі її циклічні підгрупи.

25.7. Знайти всі підгрупи даної групи. Для кожної підгрупи знайти її класи суміжності, обчислити індекс підгрупи та перевірити виконання теореми Лагранжа.

25.8. На прикладі однієї з підгруп перевірити виконання властивостей класів суміжності.

25.9. Знайти всі нормальні підгрупи даної групи.

26. Нехай G – циклічна група, g – її утворювальний елемент (генератор). $|G| = n$. Використовуючи теорему про властивості циклічної групи, для $n = 15, 16, \ldots, 25$ виконати подані нижче завдання.

26.1. Подати всі елементи групи G як степені її генератора.

26.2. Знайти значення всіх можливих порядків елементів цієї групи та кількості елементів кожного порядку.

26.3. Для кожного $k = \overline{1,n}$ знайти $ord\left(g^k\right)$. Перевірити виконання наслідку 1.3 теореми Лагранжа.

26.4. Знайти всі підгрупи групи G, вказати їх порядки. Перевірити виконання наслідку 1.2 теореми Лагранжа. Використовуючи теорему Лагранжа, знайти індекси всіх підгруп.

26.5. Переконатись, що підгрупи однакових порядків збігаються.

26.6. Назвати всі генератори групи G.

27. Довести наслідок теореми про властивості циклічної групи: $\forall n \in N : \sum_{d|n} \varphi(d) = n$ (позначення "$d \mid n$" означає "d ділить n"; це те ж саме, що "d є дільником n" або "n ділиться на d", тобто "$n \vdots d$").

§3 АЛГЕБРАЇЧНІ СИСТЕМИ З ДВОМА ОПЕРАЦІЯМИ. ІДЕАЛ КІЛЬЦЯ, ФАКТОРКІЛЬЦЕ ЗА ІДЕАЛОМ

3.1 Означення та основні властивості кілець

Досить часто алгебраїчна система наділена одразу двома операціями, які умовно називають "множенням" і "додаванням" та позначають відповідним чином.

Приклади 3.1: $(\mathbf{R}, +, \cdot)$ – множина дійсних чисел з операціями додавання і множення; $(\mathbf{Z}, +, \cdot)$ – множина цілих чисел з операціями додавання і множення; $(M_n, +, \cdot)$ – множина квадратних матриць з операціями додавання і множення.

Нехай R – деяка множина.

Означення 3.1: Алгебраїчна система з двома операціями $(R, +, \cdot)$, де $|R| \geq 2$, називається *кільцем*, якщо виконуються умови:

1) $(R, +)$ – абелева група;
2) $(R, \cdot)$ – півгрупа;
3) виконуються закони дистрибутивності:

$$\forall a, b, c \in R: a \cdot (b + c) = a \cdot b + a \cdot c; \ (b + c) \cdot a = b \cdot a + c \cdot a.$$

Операції + та · у кільці R називають операціями *додавання* та *множення*, відповідно (хоча множина R, взагалі кажучи, не є числовою і ці назви є досить умовними). Групу $(R, +)$ називають *адитивною групою* кільця. Порядок елемента цієї групи, тобто порядок елемента кільця відносно операції додавання, називають *адитивним порядком елемента.* Нейтральний елемент у групі $(R, +)$ називають *нульовим елементом* або *нулем.* Якщо у кільці існує нейтральний елемент відносно операції

множення (тобто якщо $(R, \cdot)$ є моноїдом), то такий елемент називають *одиничним елементом*, або *одиницею кільця*.

Слід зазначити, що часто під кільцем розуміють алгебраїчну систему, яка крім вимог у означенні 3.1 задовольняє ще одну вимогу, а саме: наявність нейтрального елемента відносно операції множення. Ми будемо користуватись означенням 3.1 як більш загальним.

Твердження 3.1 (властивості елементів кільця): нехай $(R, +)$ – кільце. Тоді виконуються нижченаведені рівності:

1) $\forall a \in R$: $0 \cdot a = a \cdot 0 = 0$;

2) $\forall a, b \in R$: $(-a) \cdot b = a \cdot (-b) = -a \cdot b$.

Доведення. 1) За означенням нейтрального елемента, $0 + 0 = 0$, тому $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$; віднімемо $0 \cdot a$ від правої та лівої частин рівності; отримаємо $0 \cdot a = 0$. 2) Достатньо показати, що $(-a) \cdot b$ є оберненим до $a \cdot b$, тобто $(-a) \cdot b + a \cdot b = 0$. Дійсно, згідно з законом дистрибутивності: $(-a) \cdot b + a \cdot b = ((-a) + a) \cdot b = 0 \cdot b = 0$.

Аналогічно доводиться $(-b) \cdot a + a \cdot b = 0$. Твердження доведено.

Приклади кілець 3.2: всі алгебраїчні структури, наведені у прикладі 3.1, є кільцями.

Означення 3.2: нехай R – деяке кільце. Елемент $a \in R$ $(a \neq 0)$ називається *дільником нуля*, якщо існує такий елемент $b \in R$ $(b \neq 0)$, що $a \cdot b = 0$ (тоді a – *лівий дільник нуля*) або $b \cdot a = 0$ (тоді a – *правий дільник нуля*). Для комутативного кільця, очевидно, поняття лівого і правого дільників нуля збігаються.

Означення 3.3 (типи кілець):

– кільце $(R, +, \cdot)$ називається *кільцем з одиницею*, якщо $(R, \cdot)$ – моноїд;

– кільце $(R, +, \cdot)$ називається *комутативним*, якщо операція множення у цьому кільці є комутативною;

– кільце $(R, +, \cdot)$ називається *кільцем без дільників нуля*, якщо $\forall a, b \in R$: $ab = 0 \Rightarrow (a = 0 \vee b = 0)$;

– кільце $(R, +, \cdot)$ називається *цілісним кільцем*, якщо воно є комутативним кільцем з одиницею та без дільників нуля;

– кільце $(R, +, \cdot)$ називається *полем*, якщо $(R\backslash\{0\}, \cdot)$ є абелевою групою.

Зауваження 3.1: нульовий та одиничний елементи кільця є різними (див. твердження 3.1).

Приклади 3.3:

1. $(\mathbf{R}, +, \cdot)$ – множина дійсних чисел утворює поле відносно операцій додавання та множення;

2. $(\mathbf{Z}, +, \cdot)$ – цілісне кільце;

3. $(\mathbf{Z}_n, +, \cdot)$ – комутативне кільце з одиницею; воно містить дільники нуля, якщо n – складене число;

4. множина парних чисел з операціями додавання та множення утворює комутативне кільце без одиниці та без дільників нуля;

5. множина функцій $\mathbf{R}\to\mathbf{R}$ утворює комутативне кільце з одиницею, в якому операції задані таким чином:

$$(f+g)(x)=f(x)+g(x);\ (f\cdot g)(x)=f(x)\cdot g(x);$$

6. $(M_n, +, \cdot)$ – множина матриць розмірності $n\times n$ з операціями додавання і множення матриць утворює некомутативне кільце з одиницею та з дільниками нуля;

7. множина $R[X]$ поліномів над кільцем R утворює кільце, причому властивості кільця $R[X]$ визначаються властивостями кільця R, а саме:

$R[X]$ комутативне тоді і тільки тоді, коли R комутативне;

$R[X]$ кільце з одиницею тоді і тільки тоді, коли R є кільцем з одиницею;

$R[X]$ цілісне тоді і тільки тоді, коли R є цілісним.

Означення 3.4: елемент a кільця з одиницею R називається *оборотним*, якщо існує такий елемент $b\in R$, що $ab=ba=1$. Тоді елемент

$b \in R$ називають оберненим до елемента a і позначають a^{-1}. Оборотні елементи кільця також називають *дільниками одиниці*.

Означення 3.5: множина оборотних елементів кільця R з операцією множення називається *мультиплікативною групою кільця* R і позначається R^*. Порядок елемента даної групи (тобто порядок елемента кільця відносно операції множення) називається *мультиплікативним порядком елемента кільця*.

Зауваження 3.2: дане означення можна вважати коректним, лише якщо ми доведемо, що множина оборотних елементів кільця дійсно утворює групу відносно операції множення.

Доведення полягає у перевірці нижчевказаних простих тверджень:

1) одиничний елемент e завжди є оборотним, отже, $e \in R^*$;

2) добуток двох оборотних елементів є оборотним елементом;

3) обернений до оборотного елемента також є оборотним.

Наведені нижче дві теореми демонструють зв'язок між поняттями поля і цілісного кільця.

Теорема 3.1: нехай R – поле. Тоді R – цілісне кільце.

Доведення: достатньо довести, що в полі немає дільників нуля (тобто таких елементів $a, b \in R$; $a, b \neq 0$, що $a \cdot b = 0$). Нехай $a, b \in R$; $a, b \neq 0$ і при цьому $a \cdot b = 0$. Оскільки R – поле, то $\forall a \in R\ (a \neq 0)\ \exists a^{-1}$, тому, домноживши обидві частини останньої рівності на a^{-1}, отримаємо: $a^{-1}ab = eb = b = 0$, звідки $b = 0$, що призводить до суперечності. Теорему доведено.

Зауваження 3.3: обернене твердження у загальному випадку не достовірне, але воно виконується у випадку скінченного кільця.

Теорема 3.2: нехай $(R, +, \cdot)$ – скінченне цілісне кільце. Тоді $(R, +, \cdot)$ – поле.

Доведення: нехай R – цілісне скінченне кільце. Позначимо $R' = R \setminus \{0\} = \{a_1, a_2, \ldots, a_n\}$ множину, що складається з n різних (ненульових) елементів кільця R; зазначимо, що до цієї множини належить,

зокрема, нейтральний елемент e кільця R. Покажемо, що для будь-якого елемента цієї множини існує обернений. Виберемо довільний елемент $a_i \neq 0$ і покажемо, що $\exists a_i^{-1}$: $a_i^{-1} a_i = e$. Для цього розглянемо множину $a_i R' = \{a_i a_1, \ldots, a_i a_n\}$. Оскільки дане кільце не містить дільників нуля та замкнене відносно операції множення, то $a_i R' \subset R'$. Покажемо, що $|a_i R'| = |R'|$. Для цього достатньо показати, що всі елементи множини $a_i R'$ є різними. Дійсно, якщо для деяких k,l $(1 \leq k < l \leq n)$ виконується $a_i a_k = a_i a_l$, то, внаслідок закону дистрибутивності, $a_i(a_k - a_l) = 0$, отже $a_k - a_l = 0$ внаслідок відсутності дільників нуля, тобто $a_k = a_l$, що призводить до суперечності.

Оскільки R – скінченне, $a_i R' \subset R'$ та $|a_i R'| = |R'|$, то $a_i R' = R'$, а отже $\exists a_j \in R$: $a_i a_j = e$. Внаслідок комутативності кільця також виконується $a_j a_i = e$. Теорему доведено.

Означення 3.6: кількість елементів кільця називають *порядком* кільця. Залежно від порядку кільце називається *скінченним* або *нескінченним*.

Зауваження 3.4: внаслідок наявності у кільці двох різних операцій та внаслідок означення 3.5 можемо вважати, що з кожним кільцем з одиницею пов'язано дві різні групи: *адитивна* група $(R,+)$, що складається з усіх елементів кільця, з операцією додавання, та *мультиплікативна* група $(R^*,\times)$, що складається з оборотних елементів кільця, з операцією множення. Порядок скінченного кільця дорівнює порядку його адитивної групи. Для кожного елемента a кільця визначений його *адитивний* порядок $ord_+ a$: це його порядок як елемента групи $(R,+)$. Для кожного оборотного елемента a кільця визначений його *мультиплікативний* порядок $ord_\times a$: це його порядок як елемента групи $(R^*,\times)$.

Означення 3.7: $(S, +, \cdot)$ є *підкільцем* кільця $(R, +, \cdot)$, якщо виконуються умови: $S \subset R$ і $(S, +, \cdot)$ – кільце, де операції додавання і множення в S такі ж, як і в $(R, +, \cdot)$.

3.2 Ідеал кільця. Факторкільце за ідеалом

Означення 3.8: *ідеалом* (двостороннім ідеалом) кільця $(R, +, \cdot)$ називається множина $I \subset R$, така, що виконуються умови:

1) $(I, +, \cdot)$ – підкільце кільця R;

2) $\forall a \in I, \forall r \in R$: $ar \in I$, $ra \in I$.

Означення 3.9: *найменшим* (*мінімальним*) *ідеалом* кільця R, *що містить елемент* $a \in R$, називається такий ідеал I кільця R, для якого виконуються умови:

1) $a \in I$; 2) якщо L – також ідеал кільця R, який містить елемент a, то $I \subset L$.

Приклади 3.4:

1) кільце цілих чисел $\mathbf{Z}$ є підкільцем поля раціональних чисел $\mathbf{Q}$, але не є його ідеалом;

2) нехай R – комутативне кільце, $a \in R$. Тоді найменший ідеал цього кільця, який містить a, позначається (a) і визначається так:

$$(a) = \{ra + ka: r \in R, k \in \mathbf{Z}\}, \qquad (3.1)$$

де вираз ka для додатного k означає k-кратне додавання елемента a, а для від'ємного k означає, відповідно, додавання k разів елемента $(-a)$.

Доведемо, що множина (3.1) дійсно визначає найменший ідеал, що містить елемент $a \in R$.

Доведення: очевидно, що $a \in (a)$ та що множина (3.1) є підкільцем кільця R. Покажемо, що (a) – ідеал. Нехай $b \in R$, $t \in (a)$. Покажемо, що $bt \in (a)$. Оскільки $t = sa + na$, $n \in \mathbf{Z}$, то $bt = bsa + bna = (bs + bn)a \Rightarrow bt \in (a)$

(при $r = bs + bn$ і $k = 0$). Далі доведемо, що (a) – найменший ідеал, який містить a. Тобто, якщо інший ідеал I містить a, то $I \supset (a)$. Нехай $I \ni a$. Оскільки I – ідеал, то $I \ni ra$, $r \in R$, I є також підкільцем, тому $I \ni na$, $n \in \mathbf{Z}$ і $I \ni (ra + na) \Rightarrow I \supset (a)$.

Зауваження 3.5: якщо R – кільце з одиницею, то $(a) = \{ra,\ r \in R\}$. Якщо R – кільце без одиниці, то множина $\{ra,\ r \in R\}$ теж буде утворювати ідеал, але, взагалі кажучи, він не буде містити елемент a.

Означення 3.10: *ідеалом, породженим елементом* $a \in R$, називається мінімальний ідеал (a), який містить a.

Означення 3.11: нехай R – комутативне кільце. Ідеал I називається *головним ідеалом* кільця R, якщо $\exists a \in R$: $I = (a)$.

Означення 3.12: *кільцем головних ідеалів* називається цілісне кільце R, в якому всі ідеали є головними, тобто для $\forall I \subset R$ (де I – ідеал) $\exists a \in R$: $I = (a)$.

Нехай I – ідеал кільця R. За означенням $(R, +)$ – абелева група, тому $(I, +)$ є нормальною підгрупою $(R, +)$. Отже, можна визначити операцію на множині класів суміжності за нормальною підгрупою $(I, +)$ групи $(R, +)$ та побудувати факторгрупу R/I. Далі буде показано, що у даній факторгрупі можна ввести також операцію множення, внаслідок чого R/I стане *факторкільцем*.

Означення 3.13: *класами лишків* кільця R *за ідеалом* I є означені вище класи суміжності (відносно додавання) за ідеалом I як за нормальною підгрупою.

Клас лишків, що містить елемент $a \in R$ і складається з елементів $a + c$, $c \in I$, будемо позначати $[a] = a + I$. Як було доведено раніше, елементи кільця a, b належать до одного класу лишків тоді і тільки тоді, коли $(a - b) \in I$.

Означення 3.14: елементи кільця $a, b \in R$ називаються *конгруентними за модулем ідеалу* I, якщо $(a-b) \in I$. Конгруентність елементів позначається $a \equiv b \pmod{I}$.

Твердження 3.2: якщо $a \equiv b \bmod I$, $r \equiv s \bmod I$, то:

1) $(a+r) \equiv (b+s) \bmod I$;

2) $\forall u \in R$: $au \equiv bu \bmod I$. $(au - bu = (a-b)u \in I)$;

3) $ra \equiv sb \bmod I$, $(ar - sb = ar - br + br - bs = (a-b)r + b(r-s) \equiv \equiv 0 \bmod I$;

4) $na \equiv nb \bmod I$.

На множині класів лишків кільця R за ідеалом I визначимо такі операції:

$$(a+I)+(b+I)=(a+b)+I; \tag{3.2}$$

$$(a+I)(b+I)=ab+I. \tag{3.3}$$

Теорема 3.3: множина класів лишків кільця R за ідеалом I з операціями (3.2) та (3.3) утворює кільце.

Доведення є аналогічним доведенню теореми 2.2. Відмінність полягає лише у тому, що у даному випадку додатково необхідно показати, що операція множення на класах лишків визначена коректно. Для цього необхідно довести таке: якщо $(a_1 + I) = (b_1 + I)$ та $(a_2 + I) = (b_2 + I)$, то $(a_1 + I)(a_2 + I) = (b_1 + I)(b_2 + I)$, тобто $a_1 a_2 + I = b_1 b_2 + I$.

За властивістю 2 класів суміжності маємо: $b_1 - a_1 = r_1 \in I$ та $b_2 - a_2 = r_2 \in I$. Тоді $b_1 b_2 - a_1 a_2 = b_1(b_2 - a_2) + a_2(b_1 - a_1) \in I$ за означенням ідеалу, отже, $a_1 a_2 + I = b_1 b_2 + I$. Теорема доведена.

Означення 3.15: *факторкільцем* кільця R за ідеалом I (позначається R/I) називається множина класів лишків кільця R за модулем ідеалу I з операціями (3.2), (3.3).

Приклад 3.5: побудуємо факторкільце $\mathbf{Z}/(n)$. Нехай (n) – найменший ідеал кільця цілих чисел, що містить елемент n: $(n) = \{0, \pm n, \pm 2n, \ldots\}$; в

цьому випадку $[a] := a + (n)$. Тоді $\mathbf{Z}/(n) = \{[0], [1], \ldots, [n-1]\}$, де $[i] = i + (n)$.

Теорема 3.4: факторкільце $\mathbf{Z}/(p)$ кільця $\mathbf{Z}$ за головним ідеалом, породженим простим p, є полем.

Доведення: оскільки $\mathbf{Z}/(p)$ є скінченним кільцем, то за теоремою 3.1 достатньо показати, що воно цілісне. Комутативність кільця очевидна. Одиничним елементом кільця є [1]. Покажемо відсутність дільників нуля: $[a]\cdot[b] = 0 \Leftrightarrow [ab] = 0 \Leftrightarrow ab \equiv 0 \bmod p \Leftrightarrow ab = kp$ для деякого $k \in \mathbf{Z}$, тобто p ділить ab. Але p – просте, отже, $p|a$ або $p|b$, тобто $[a] = [0]$ або $[b] = [0]$.

Наслідок 3.1: $(\mathbf{Z}_n, +, \cdot)$ – поле $\Leftrightarrow$ n – просте число.

Приклад 3.6: $\mathbf{Z}/(3) = \{[0], [1], [2]\}$ з операціями додавання та множення за модулем 3 є полем.

Зауваження 3.6: властивості вихідного кільця можуть не переноситися на факторкільце. Наприклад, $\mathbf{Z}$ є цілісним кільцем, а кільце $\mathbf{Z}/(n)$, де n не є простим, не є цілісним; в той же час кільце $\mathbf{Z}/(p)$ для простого p є не тільки цілісним кільцем, але й полем. Тобто факторизація кільця за ідеалом може як покращувати, так і погіршувати властивості кільця.

3.3 Відображення кілець

Означення 3.16: *гомоморфізм* φ кільця $(R, +, \cdot)$ у кільце $(S, +, \cdot)$ – це відображення $\varphi: R \to S$, при якому для операцій додавання і множення у кільцях R та S виконуються умови:

$$\forall a, b \in R: \varphi(a+b) = \varphi(a)+\varphi(b); \varphi(ab) = \varphi(a)\varphi(b),$$

де у лівих частинах рівностей розуміються операції у кільці R, а у правих – операції у кільці S.

Зокрема, таке відображення є гомоморфізмом адитивних груп кілець; при цьому

$$\ker \varphi = \{a \in R: \varphi(a) = 0_S\};\ \operatorname{Im} \varphi = \{g \in S \mid \exists a \in R: g = \varphi(a)\}.$$

Аналогічно до відображень груп визначаються: епіморфізм кілець, ендоморфізм, мономорфізм, ізоморфізм та автоморфізм кілець, а також поняття ізоморфних кілець.

Теорема 3.5 (про ізоморфізм кілець).

1. Якщо $\varphi: R \to S$ – гомоморфізм кілець, то $\ker \varphi$ – ідеал кільця R, і $R/\ker\varphi \cong \operatorname{Im}\varphi$ (факторкільце за ядром гомоморфізму ізоморфно образу цього гомоморфізму). При цьому ізоморфізм $\psi: R/\ker\varphi \to \operatorname{Im}\varphi$ визначається таким чином: $\psi(r + \ker \varphi) := \varphi(r)$.

2. Якщо I – ідеал кільця R, то відображення $\varphi: R \to R/I$ побудоване за правилом $\varphi(a) = a + I$, де $a \in R$ – гомоморфізм, і при цьому $\ker \varphi = I$, $\operatorname{Im} \varphi = R/I$.

Доведення теореми є аналогічним доведенню теореми 2.4.

Зауваження 3.7: бієктивні відображення можна використовувати для введення алгебраїчної структури на деякій множині. Нехай, наприклад, існує бієктивне відображення φ між кільцем S і деякою множиною R: $\varphi: S \to R$. Тоді на множині R ми можемо ввести структуру кільця таким чином: для будь-яких $r_1, r_2 \in R$, де $\varphi(s_1) = r_1$; $\varphi(s_2) = r_2$, визначимо їх суму й добуток за правилом: $r_1 + r_2 = \varphi(s_1 + s_2)$; $r_1 r_2 = \varphi(s_1 s_2)$, а також покладемо $0_R = \varphi(0_S)$, $-r_1 = -\varphi(s_1)$. Тоді множина R з введеними на ній операціями буде кільцем, причому це кільце буде ізоморфне кільцю S.

Приклад 3.7: нехай p – просте число. Згадаємо позначення $\mathbf{Z}_p = \{0, 1, \ldots, p-1\}$ та визначимо відображення $\varphi: \mathbf{Z}/(p) \to \mathbf{Z}_p$, де $\varphi(a + (p)) = a$, $a \in \{0, 1, \ldots, p-1\}$.

Оскільки $\mathbf{Z}/(p)$ – поле, то і $\mathbf{Z}_p$ буде мати структуру поля, індуковану відображенням φ.

Поле $\mathbf{Z}_p$ є частковим випадком так званого поля Галуа. Замість позначення $\mathbf{Z}_p$ також часто використовують позначення $GF(p)$ та $\mathbf{F}_p$.

Питання для самоконтролю до §3

1. Чи є серед перелічених у прикладах 3.1. алгебраїчних систем такі, що задовольняють означення кільця? Відповідь обґрунтуйте.

2. Чому нульовий та одиничний елементи кільця не є рівними?

3. Що таке ідеал кільця?

4. Сформулюйте означення гомоморфізму кілець.

5. Наведіть приклади різних типів гомоморфізмів кілець.

6. Дайте означення факторкільця за ідеалом. Чому операції, визначені на класах лишків за ідеалом, є коректними?

7. Наведіть приклад (відмінний від прикладу, наведеного в зауваженні 3.6), який демонструє, що властивості вихідного кільця можуть не переноситися на факторкільце.

8. Сформулюйте теорему про ізоморфізм кілець.

9. Подумайте, як сформулювати означення найменшого ідеалу, що містить деяку множину елементів; означення найменшого ідеалу, що має деяку задану властивість.

Задачі до §3

1. Нехай $(R, +, *)$ – кільце, 0 та 1 – його нульовий та одиничний елементи. Довести:

а) $\forall\ a \in R$: $0*a = a*0 = 0$; б) $0 \neq 1$; в) $\forall\ a, b \in R$: $(-a)*b = a*(-b) = -a*b$, $(-a)*(-b) = a*b$.

2. Довести: $(R, +, *)$ – поле $\Rightarrow (R, +, *)$ – цілісне кільце.

3. Навести приклади кілець з дільниками нуля та кілець без дільників нуля.

4. Нехай $(R, +, *)$ – кільце з одиницею e, I – його ідеал, $e \in I$. Довести, що $I = R$.

5. Довести, що будь-яка циклічна група порядку n ізоморфна групі лишків $\mathbf{Z}_n$ з операцією додавання за модулем n.

6. Довести: якщо індекс деякої підгрупи дорівнює 2, то ця підгрупа є нормальною.

7. Довести, що в кільці без дільників нуля можна скорочувати однакові ненульові множники, а саме: якщо $(R, +, *)$ – кільце без дільників нуля та $a, b, c \in R \setminus \{0\}$, то з рівності $ab = ac$ випливає рівність $b = c$.

8. Нехай $(R, +, *)$ – кільце без дільників нуля, з одиницею e (взагалі кажучи, некомутативне). Нехай $a, b \in R$, причому $ab = e$. Довести: $ba = e$.

9. Позначимо nZ – підкільце кільця $\mathbf{Z}$ цілих чисел, $nZ = \{kz \mid z \in Z\}$. Довести: 1) nZ – ідеал кільця $\mathbf{Z}$ цілих чисел; 2) $Z/nZ \cong Z_n$.

10. Доведіть теорему про ізоморфізм кілець.

§4 ХАРАКТЕРИСТИКА КІЛЬЦЯ, ХАРАКТЕРИСТИКА СКІНЧЕННОГО ПОЛЯ. ФАКТОРКІЛЬЦЯ ЗА РІЗНИМИ ІДЕАЛАМИ, ЇХ ВЛАСТИВОСТІ

4.1 Характеристика кільця, її властивості

Нехай R – довільне кільце.

Означення 4.1: нехай $\exists n \in \mathbf{N}\ \forall r \in R$: $nr = 0$. *Характеристикою* кільця R називається таке $n_0 \in \mathbf{N}$, що $n_0 = \min\{n \in \mathbf{N}: nr = 0, \forall r \in R\}$, а саме R називається кільцем характеристики n_0. Характеристика кільця R позначається char R; наприклад, в цьому означенні char $R = n_0$

Якщо $\forall n \in \mathbf{N}\ \exists r \in R$: $nr \neq 0$ (тобто умова у означенні 4.1 не виконується), то вважається, що характеристика кільця дорівнює нулю, а кільце R називається кільцем характеристики 0 (char $R = 0$).

Зауваження 4.1: тут і далі під позначенням nr, де n – натуральне число, а r – елемент кільця, ми розуміємо елемент кільця, отриманий в результаті n-кратного додавання елемента r кільця: $nr = \underbrace{r + r + \ldots + r}_{n \text{ разів}}$.

Наведемо кілька простих, але корисних властивостей характеристики кільця.

Теорема 4.1: нехай R – кільце з одиницею e, без дільників нуля і його характеристика не дорівнює нулю. Тоді його характеристика – просте число.

Доведення: за означенням кільця, $R \neq \{0\}$, тому char $R = n \geq 2$.

Доведення проводитимемо від супротивного. Нехай char $R = n$, де $n = km$, $k, m \in Z$, $1 < k, m < n$. Тоді $0 = ne = (km)e = (ke)(me)$; оскільки дільники нуля в кільці R відсутні за умовою, то $ke = 0$ або $me = 0$.

Припустимо, що $ke = 0$. Але тоді $\forall r \in R$: $kr = (ke)r = 0$, звідки випливає, що char $R \le k < n$, що суперечить припущенню char $R = n$.

Теорема 4.2: нехай R – скінченне кільце з одиницею. Тоді char $R \neq 0$.

Доведення: нехай R містить k елементів; розглянемо елементи $e, 2e, 3e, \ldots, k\,e, (k+1)e$. Усі вони належать кільцю R, а їх кількість більша за k. Отже, $\exists l, m \in N$ $(1 \le m < l \le k+1)$: $le = me$. Тоді $(le - me) = (l-m)\,e = 0$, причому $(l-m) > 0$, і, аналогічно до доведення теореми 4.1, $\forall a \in R : (l-m)a = 0$, отже, $0 <$ char $R \le (l-m)$. Теорему доведено.

Наслідок 4.1: характеристика цілісного кільця або дорівнює нулю, або є простим числом. Характеристикою скінченного цілісного кільця є просте число. Характеристика скінченного кільця з одиницею не більша за його порядок.

Наслідок 4.2: характеристика поля або дорівнює нулю, або є простим числом. Характеристикою скінченного поля є просте число.

Приклади 4.1:

1) char F_p = (char $\mathbf{Z}/(p)$) = p; 2) char $\mathbf{Z} = 0$; 3) char $\mathbf{Q} = 0$.

Зауваження 4.2: якщо кільце скінченне, то його характеристика не дорівнює нулю. Але обернене твердження несправедливе: існують нескінченні кільця, що мають скінченну характеристику: наприклад, кільця поліномів над полями Галуа.

Теорема 4.3: нехай R – комутативне кільце; char $R = p$ – просте число. Тоді $\forall a, b \in R$: $(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$, $\forall n \in \mathbf{N}$.

Для доведення теореми сформулюємо лему.

Лема 4.1: нехай p – просте число. Тоді для будь-якого натурального k від 1 до $p-1$ включно виконується порівняння:

$$C_p^k = \frac{p(p-1)\ldots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} \equiv 0 (\mathrm{mod}\, p).$$

Доведення: скористаємось фактом, який ми доведемо трохи пізніше при вивченні евклідових кілець (§5): якщо для деяких цілих чисел a,b,c виконано: $c \mid ab$ та $(c,a)=1$, то $c \mid b$.

Зауважимо, що

$$C_p^k = \frac{p(p-1)\ldots(p-k+1)}{1\cdot 2\cdot\ldots\cdot k} = p\cdot\frac{(p-1)\ldots(p-k+1)}{1\cdot 2\cdot\ldots\cdot k},$$

де знаменник другого множника є взаємно-простим з першим множником. Але оскільки C_p^k є цілим числом (отже, $k!\mid p(p-1)\ldots(p-k+1)$), то, враховуючи $(k!,p)=1$, отримаємо $k!\mid (p-1)\ldots(p-k+1)$, звідки й випливає твердження леми.

Доведення теореми 4.3: покажемо, що $(a+b)^p = a^p + b^p$; далі доведення виконується індукцією за n (повторним піднесенням до степеня p).

Застосовуючи формулу піднесення суми до степеня, а також лему 4.1 і означення 4.1, отримаємо:

$$(a+b)^p = a^p + C_p^1 a^{p-1}b + \ldots + C_p^{p-1} ab^{p-1} + b^p = a^p + b^p.$$

Далі, оскільки $a^p = ((a-b)+b)^p = (a-b)^p + b^p$, то $(a-b)^p = a^p - b^p$. Теорему доведено.

Цю теорему можна також сформулювати так: у комутативному кільці простої характеристики піднесення до степеня, що дорівнює характеристиці, є лінійною операцією.

4.2 Залежність властивостей факторкільця від ідеалу

Як вказувалось раніше, при побудові факторкільця за ідеалом властивості вихідного кільця можуть як "покращитись", так і

"погіршитись". Наприклад, кільце цілих чисел є цілісним кільцем (але не є полем), а його факторкільце за ідеалом в деяких випадках є полем, а в інших – кільцем з дільниками нуля (наведіть приклади самостійно). Далі ми розглянемо різні типи ідеалів та визначимо, як певні властивості ідеалу кільця впливають на властивості відповідного факторкільця. Спочатку введемо ряд означень.

Нехай надалі R – комутативне кільце з одиницею.

Означення 4.2: елемент $a \in R$ називається *дільником* елемента $b \in R$, якщо $\exists c \in R$: $ac = b$.

Зокрема, дільники одиниці називаються *оборотними* елементами. Інакше кажучи, елемент a кільця R називається оборотним, якщо існує такий елемент $a^{-1} \in R$, що $a\,a^{-1} = a^{-1}\,a = e$.

Зауваження 4.3: надалі при розв'язуванні задач ми будемо користуватись поняттям подільності і у некомутативному кільці. У цьому випадку розрізняють *ліві* та *праві дільники* елемента кільця. Зокрема, елемент є дільником нуля, якщо він є або лівим, або правим дільником нуля. У нескінченних некомутативних кільцях (наприклад, у кільці матриць) існують елементи, що є лише лівими або лише правими дільниками одиниці.

Означення 4.3: елементи $a, b \in R$ називаються *асоційованими*, якщо існує $\varepsilon \in R^*$ такий, що $a = b\varepsilon$. Асоційовані елементи позначаємо так: $a \sim b$.

Означення 4.4: елемент $c \in R$ називається *простим*, якщо одночасно виконуються нижченаведені умови:

1) c не є оборотним;

2) всі дільники c є або оборотними, або асоційованими з ним.

Приклад 4.2: прості елементи у кільці $\mathbf{Z}$ – це прості числа. Оскільки у цьому кільці лише два оборотних елементи (1 та –1), то кожен елемент $a \in \mathbf{Z}$ має рівно два асоційованих з ним елементи: a та $-a$.

Означення 4.5: ідеал P кільця R (такий, що $P \neq R$) називається *простим*, якщо виконується умова: $\forall a, b \in R$: $ab \in P \Leftrightarrow (a \in P) \vee (b \in P)$.

Означення 4.6: ідеал M кільця R (такий, що $M \neq R$) називається *максимальним*, якщо для будь-якого ідеалу I кільця R виконується умова: якщо $M \subseteq I$, то або $M = I$, або $R = I$ (тобто в R немає ідеалу, більшого за M, крім самого R).

Використовуючи введені означення, сформулюємо та доведемо теорему про властивості факторкільця у залежності від властивостей ідеалу.

Теорема 4.4: нехай R – комутативне кільце з одиницею. Тоді:

1) ідеал $M \subset R$ – максимальний $\Leftrightarrow$ R/M – поле;

2) ідеал $P \subset R$ – простий $\Leftrightarrow$ R/P – цілісне кільце;

3) ідеал $P \subset R$ – максимальний $\Rightarrow$ ідеал $P \subset R$ – простий;

4) якщо R – кільце головних ідеалів, $c \in R$, то $R/(c)$ – поле $\Leftrightarrow$ c – простий елемент кільця R.

Доведення. 1. Нехай M – максимальний ідеал. Розглянемо множину $I = \{ar + m | r \in R, m \in M\}$ для фіксованого $a \notin M$, $a \in R$. Легко перевірити, що така множина є ідеалом, отже, якщо $M \subset I$, то $I = R$. Звідси випливає, що $I \ni e$, отже $\exists (r \in R, m \in M)$: $ar + m = e$, де e – одиничний елемент. Тоді $(a + M)(r + M) = ar + M = e + M$, тобто клас лишків $a + M$ має обернений відносно множення у факторкільці. Отже, R/M – поле.

І навпаки, нехай R/M – поле, а ідеал I такий, що $I \supseteq M$, $I \neq M$. Покажемо, що $I = R$. Оскільки R/M – поле, то для $a \in I/M$ $\exists r \in R$: $(a + M)(r + M) = e + M$, звідси $ar + m = 1$ для деякого $m \in M$. Але тоді $1 \in I$, отже, $I = R$ і M – максимальний ідеал.

2. Нехай P – простий ідеал R, тоді R/P – комутативне кільце з одиницею: $1 + P \neq 0 + P$ (раніше було доведено, що нейтральний елемент за операцією "+" у кільці не збігається з нейтральним елементом за операцію "·").

Нехай $(a+P)(b+P)=0+P=ab+P$, а це рівносильне тому, що $ab\in P$. Отже, $a\in P$ або $b\in P$. Тобто $a+P=0$ або $b+P=0$, і дільники нуля в R/P відсутні.

У зворотному напрямку твердження доводиться аналогічно.

3. Дане твердження є наслідком пунктів 1 і 2, оскільки поле є цілісним кільцем.

4. Нехай $R/(c)$ – поле, тоді елемент c не може бути оборотним, оскільки для оборотного елемента $R/(c)=\{0\}$.

Нехай c не є оборотним і не є простим елементом. Тоді існує таке $a\in R$, що a – дільник c, причому a не асоційований з c і не є оборотним (а також $a\neq 0$, оскільки тоді було б $c=0$ і елемент a був би асоційованим з c). Нехай $c=ab$, $b\in R$; покажемо, що $a\notin(c)$. Дійсно, якщо $a\in(c)$, то $a=cd=abd$, $d\in R$, звідки отримаємо $a(1-bd)=0$, $a\neq 0$. Отже, $bd=1$, b – оборотний і c асоційований з a, що призводить до суперечності. Але $c=ab$, отже, $(c)\subset(a)\subset R$, де всі включення власні (оскільки $(c)\not\subset(a)$, $(a)\neq R$). Звідси (c) – не максимальний ідеал, а отже $R/(c)$ – не поле.

Нехай c – простий. Тоді $(c)\neq R$, оскільки c – не оборотний. Якщо I – ідеал, $I\supset(c)$, то $I=(a)$ для деякого a – дільника c (оскільки R – кільце головних ідеалів). Таким чином, або a – оборотний, або асоційований з c, тоді або $I=R$, або $I=(c)$, і (c) – максимальний ідеал; отже, за пунктом 1), $R/(c)$ – поле.

Теорему доведено.

Приклад 4.3: кільце $\mathbf{Z}$ цілих чисел з операціями додавання та множення є кільцем головних ідеалів. Дійсно, оскільки ідеал – підгрупа циклічної групи $(\mathbf{Z},+)$, то за теоремою 2.1 будь-який ідеал в $\mathbf{Z}$ є також циклічною групою відносно операції додавання, тому він буде породжуватись відповідним утворювальним елементом.

Нехай $p\in\mathbf{Z}$ – простий елемент в $\mathbf{Z}$, тоді за теоремою 4.4 $\mathbf{Z}/(p)$ – поле, отже, простий ідеал (p) є максимальним ідеалом.

Якщо $n = ab \in \mathbf{Z}$, де $a, b \neq \pm 1$, то (n) не є простим ідеалом, отже, $\mathbf{Z}/(n)$ – не поле.

Питання для самоконтролю до §4

1. Сформулюйте означення характеристики кільця.

2. Наведіть приклад, коли характеристика цілісного кільця дорівнює нулю.

3. Що таке дільник елемента в комутативному кільці?

4. Нехай R – деяке комутативне кільце, і $a \in R$ є дільником елемента $b \in R$. Чи обов'язково b є дільником елемента a?

5. Який зв'язок між полем та цілісним кільцем?

6. Сформулюйте теорему про властивості факторкільця в залежності від властивостей ідеалу.

7. Які елементи є оборотними у кільці цілих чисел? Які є простими? Навести приклади асоційованих елементів у цьому кільці.

8. Чи справедливо, що якщо характеристика кільця не дорівнює нулю, то кільце є скінченним? Довести або навести контрприклад.

Задачі до §4

1. Нехай G – група, C – її центр. Довести: $\forall S \subset G: C \subset N(S)$.

2. Нехай I – ідеал кільця R. Довести:

$$\forall a,b \in R: (a_1 \in a + I, b_1 \in b + I) \Rightarrow a_1 b_1 \in ab + I.$$

3. Нехай G – група. Довести, що $\forall a \in G: \langle a \rangle \subset N(a)$.

4. Нехай G – група, $a,b \in G$. Довести: $b \in N(a) \Leftrightarrow ab = ba$.

5. Нехай G – група, $a,b,c \in G$. Чи вірно, що якщо $c \in N(S)$, де $S = \{a,b\}$, то c комутує з a та b? (Довести або навести контрприклад.)

6. Нехай $\phi: R \to S$ – епіморфізм груп. Довести:

а) $\forall s \in S$ кількість його прообразів дорівнює $|\ker \phi|$;

б) відображення $\psi: R/\ker \phi \to S$, де $\psi(r \cdot \ker \phi) = \phi(r)$, є ізоморфізмом.

7. Довести: характеристика скінченного кільця ділить його порядок.

8. Довести: якщо характеристика кільця з одиницею не дорівнює нулю, то вона дорівнює адитивному порядку одиниці (тобто порядку одиничного елемента як елемента адитивної групи кільця).

9. Довести: характеристика кільця з одиницею дорівнює нулю тоді й тільки тоді, коли адитивний порядок одиниці дорівнює нескінченності.

10*. Довести, що характеристика скінченного кільця з одиницею не дорівнює нулю. Чи справедливо дане твердження для скінченого кільця без одиниці? Як буде в цьому випадку виражатись характеристика кільця через адитивні порядки його елементів?

11*. Довести, що в скінченному некомутативному кільці будь-які (і ліві, і праві) дільники оборотного елемента є оборотними елементами.

12. Нехай R – комутативне кільце, $a,b,c \in R$. Довести: якщо a – дільник b, b – дільник c, то a – дільник c. Чи є справедливим твердження: якщо a – дільник b, то b – дільник a?

13. Довести, що оборотні елементи кільця з одиницею є дільниками будь-яких елементів цього кільця. Довести, що будь-який елемент кільця ділиться на всі елементи, асоційовані з ним. Такі дільники (оборотні та асоційовані з деяким елементом кільця) називають *тривіальними* дільниками цього елемента.

14. Довести, що відношення асоційованості елементів комутативного кільця є відношеннями еквівалентності.

15. Довести, що в комутативному кільці добуток дільників одиниці є дільником одиниці.

16. Чи справедливо, що два асоційованих елементи комутативного кільця одночасно або оборотні, або необоротні?

17*. Довести, що в скінченному (у тому числі і у некомутативному) кільці з одиницею виконано: a не є дільником нуля (ні лівим, ні правим) тоді й тільки тоді, коли a є оборотним елементом (тобто існує такий елемент a^{-1}, що $aa^{-1}=a^{-1}a=e$). Чи справедливо це для нескінченного кільця з одиницею?

18. Чи справедливо, що два оборотних елемента комутативного кільця асоційовані?

19. Нехай $(\mathbf{R},+)$ – група дійних чисел з операцією додавання, $(\mathbf{Z},+)$ – її підгрупа. Як можна визначити факторгрупу $\mathbf{R}/\mathbf{Z}$? Наведіть її ізоморфний образ.

20. Довести: одиничний елемент кільця належить деякому ідеалу цього кільця тоді і тільки тоді, коли цей ідеал збігається з усім кільцем.

21*. При яких значеннях n всі необоротні елементи кільця $\mathbf{Z}_n$ утворюють ідеал?

22. Нехай R – комутативне кільце з одиницею. Довести: $c\in R^* \Rightarrow R/(c)=\{0\}$.

23. Нехай R – комутативне кільце з одиницею, $a,c\in R$. Довести: a – дільник $c \Rightarrow (c)\subset(a)$.

24. Довести, що кільце цілих чисел – кільце головних ідеалів.

25. Довести, що в кільці головних ідеалів ідеал є простим тоді й тільки тоді, коли він породжений простим елементом.

26. Довести, що ідеал кільця $\mathbf{Z}$ цілих чисел, породжений елементами 2 та 3 (тобто найменший ідеал, що містить ці числа), збігається з $\mathbf{Z}$.

27. Які ідеали в кільці цілих чисел є простими? максимальними?

28. Довести, що множина всіх оборотних елементів кільця з одиницею (в тому числі некомутативного) утворює групу відносно операції множення.

29. Довести, що в кільці головних ідеалів будь-який простий ідеал є максимальним (тобто в кільці головних ідеалів поняття максимального і простого ідеалів збігаються).

30*. Чи справедливо твердження задачі 29 для будь-якого комутативного кільця з одиницею? Довести істинність твердження або навести контрприклад.

31. Нехай R – комутативне кільце з одиницею, $|R^*| = k$. Скільки у цьому кільці оборотних елементів? Скільки елементів, асоційованих з деяким оборотним елементом? Скільки елементів, асоційованих з деяким необоротним елементом? Скільки дільників має кожен простий елемент цього кільця?

32. Довести, що елемент кільця, асоційований з деяким простим елементом, теж є простим.

§5 ФАКТОРІАЛЬНІ ТА ЕВКЛІДОВІ КІЛЬЦЯ

5.1 Означення факторіального кільця

Нехай K – довільне цілісне кільце.

Означення 5.1: цілісне кільце K називається *факторіальним* (або "з однозначним розкладом на прості множники"), якщо виконуються такі умови:

1) будь-який його ненульовий елемент a можна подати у вигляді:

$$a = up_1p_2...p_r, \tag{5.1}$$

де $u \in K^*$, $p_1,...,p_r$ – прості (не обов'язково різні) елементи кільця;

2) якщо існує ще одне таке подання

$$a = vq_1..q_l$$

де $v \in K^*$, $q_1,...,q_l$ – прості, то $l = r$ та (при належній нумерації) $p_i \sim q_i$, $i = \overline{1,r}$, тобто $\forall i = \overline{1,r} : q_i = u_i p_i$, де $u_i \in K^*$.

Тобто, факторіальне кільце – це таке кільце, в якому існує однозначний (з точністю до перестановки та асоційованості) розклад на прості множники.

Якщо ж для деякого кільця K виконується лише умова 1) означення 5.1, то таке кільце називається *кільцем з розкладом на прості множники* (але не обов'язково однозначним).

Зауваження 5.1: у формулі (5.1) можливо, щоб $r = 0$, тобто оборотні елементи кільця теж можна подати у вигляді (5.1).

Приклад 5.1: простими елементами у кільці Z цілих чисел є прості числа; оборотними – елементи 1 та –1.

Теорема 5.1 (критерій факторіальності): нехай K – цілісне кільце з розкладом на прості множники. Тоді нижченаведені умови рівносильні:

1) K – факторіальне кільце;

2) для будь-якого простого елемента $p \in K$ виконано:

$$p \mid ab \Leftrightarrow p \mid a \vee p \mid b.$$

Доведення: доведемо, що $1) \Rightarrow 2)$.

Нехай K – факторіальне, $a,b \in K$, $p \mid ab$. Тоді, за означенням 5.1, $\exists a_1,...,a_l,b_1,...b_m \in K$ – прості, $\exists u,v \in K^* : a = u\prod_{i=1}^{l} a_i$, $b = v\prod_{j=1}^{m} b_j$. Оскільки $p \mid ab$, то $\exists c \in K : ab = cp$, причому $\exists s \in K^*, \exists c_1,...,c_r \in K$ – прості, що $c = s\prod_{k=1}^{r} c_k$. Тоді

$$s \cdot p \cdot \prod_{k=1}^{r} c_k = u \cdot v \cdot \prod_{i=1}^{l} a_i \prod_{j=1}^{m} b_j . \qquad (5.2)$$

Оскільки кільце факторіальне, то, за означенням 5.1, p асоційований з деяким простим елементом у правій частині (5.2).

Нехай, наприклад, $\exists\ 1 \le t \le l : p \sim a_t$. Тоді $p \mid a$. Аналогічно, якщо $\exists\ 1 \le t \le m : p \sim b_t$, то $p \mid b$.

Доведемо, що $2) \Rightarrow 1)$.

Доведемо однозначність розкладу елемента $a \in K$ індукцією за кількістю множників у розкладі a. Якщо у розкладі один множник, то a є простим і його розклад однозначний. Нехай розклад на множники є однозначним, якщо елемент можна подати у вигляді добутку не більше ніж n множників. Доведемо, що якщо деякий елемент можна подати у вигляді добутку $n+1$-го множника, то його розклад також буде однозначним. Нехай

$$a = u\prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m+1} q_j,\ m \geq n. \tag{5.3}$$

Тоді $p_{n+1} \mid \prod_{j=1}^{m+1} q_j$, отже, $\exists\, 1 \leq j \leq m+1 : p_{n+1} \sim q_j$.

Не обмежуючи загальності, будемо вважати, що $p_{n+1} \sim q_{m+1}$. Тоді $q_{m+1} = zp_{n+1}$, для деякого $z \in K^*$, і після скорочення лівої і правої частин (5.3) на q_m (оскільки K – цілісне, то таке перетворення є коректним) отримаємо

$$u\prod_{i=1}^{n} p_i = vz\prod_{j=1}^{m} q_j. \tag{5.4}$$

У лівій частині виразу (5.4) лише n простих множників, отже, розклад елемента $b = u\prod_{i=1}^{n} p_i$ є однозначним. Тому $m = n$ та $q_j \sim p_j$, $j = \overline{1,n}$, при належній нумерації.

Приклад 5.2: зі шкільної програми відомо, що кільце Z цілих чисел є факторіальним. На відміну від кільця Z, кільце $\mathrm{Z}(\sqrt{-3}) = \{a + b\sqrt{-3}, a, b \in \mathrm{Z}\}$ не є факторіальним (доведіть це!).

5.2 Найбільший спільний дільник та найменше спільне кратне у цілісному кільці

Нехай K – довільне цілісне кільце.

Означення 5.2: для довільних $a, b \in K$ їх *найбільшим спільним дільником* $НСД(a,b)$ (або просто (a,b)) будемо називати будь-який елемент $d \in K$, для якого виконуються умови:

1) $d \mid a$, $d \mid b$;

2) якщо для деякого $c \in K$ виконуються умови $c \mid a$, $c \mid b$, то тоді $c \mid d$.

Зауваження 5.2: взагалі кажучи, у довільному цілісному кільці $НСД(a,b)$ не єдиний. А саме: якщо $d = НСД(a,b)$ і $c \sim d$, то $c = НСД(a,b)$. І навпаки, якщо $c = НСД(a,b)$ і $d = НСД(a,b)$, то $c \sim d$. Тобто, для будь-якої пари $a,b \in K$ кількість елементів, які, за означенням, є найбільшими спільними дільниками елементів a,b, дорівнює кількості оборотних елементів кільця K і всі $НСД(a,b)$ асоційовані між собою та відрізняються один від одного на деякий множник з K^*.

Якщо $НСД(a,b) \in K^*$, то будемо казати, що a і b *взаємно прості.*

Приклад 5.3: у кільці Z цілих чисел, згідно з нашим означенням, кожна пара елементів має два *НСД*, які відрізняються між собою знаком. Наприклад, $НСД(9,12) = \pm 3$.

Твердження 5.1 (властивості *НСД*): нехай $a,b \in K$. Тоді:

1) $(a,b) = a \Leftrightarrow a \mid b$;

2) $(a,0) = a$;

3) $(ca,cb) = c(a,b)$;

4) $((a,b),c) = (a,(b,c))$.

Дане твердження рекомендується довести самостійно.

Означення 5.3: для довільних $a,b \in K$ їх *найменшим спільним кратним* $НСК(a,b)$ будемо називати будь-який елемент $m \in K$, для якого виконуються умови:

1) $a \mid m$, $b \mid m$;

2) якщо для деякого $c \in K$ виконується умова $a \mid c$, $b \mid c$, то $m \mid c$.

Зауваження 5.3: з п. 2) означення 5.3 випливає, зокрема, що $m \mid ab$.

Зауваження 5.4: для $НСК(a,b)$ справедливе зауваження, аналогічне зауваженню 5.2.

Приклад 5.4: у кільці Z цілих чисел $НСК(12,18) = \pm 36$.

Слід зазначити, що у довільному цілісному кільці K для деяких

$a,b\in K$ може не існувати $НСД(a,b)$ та $НСК(a,b)$.

Теорема 5.2: нехай $a,b\in K$, причому $\exists\, d=НСД(a,b)$ та $m=НСК(a,b)$. Тоді:

1) $m=0\Rightarrow a=0$ або $b=0$;

2) якщо $a,b\neq 0$, то $\exists t\in K: ab=tm$, причому $t\sim d$ (або, що те ж саме $t=НСД(a,b)$).

Доведення: виконання твердження 1) даної теореми випливає з того, що $m\,|\,ab$. Дійсно, якщо $m=0$, то $ab=s\cdot 0$ для деякого $s\in K$, тоді $ab=0$ і, за означенням цілісного кільця, $a=0$ або $b=0$.

Доведемо п. 2). Нехай $a,b\neq 0$, тоді $\exists t\in K: ab=tm$, оскільки $m\,|\,ab$. Покажемо, що $t=НСД(a,b)$. За означенням $НСК$, $m=aa_1=bb_1$ для деяких $a_1,b_1\in K$. Отже, $ab=tm=taa_1=tbb_1$, звідки, зокрема, $b=ta_1$ та $a=tb_1$ (після скорочення на a або b, відповідно). Отже, $t\,|\,a$ та $t\,|\,b$, і виконано п.1) означення 5.2.

Нехай для деякого $c\in K: c\,|\,a,\ c\,|\,b$. Покажемо, що $c\,|\,t$. Дійсно, тоді для деяких $a_1,b_2\in K$ виконано: $a=a_2c$, $b=b_2c$, отже, $ab=tm=b_2a_2c\cdot c=f\cdot c$, де $f=b_2a_2c$. Оскільки $a\,|\,f$ та $b\,|\,f$, то $m\,|\,f$, тобто, $\exists l\in K: f=lm$, звідки $tm=ab=fc=lmc$, тобто, $t=lc$ (після скорочення на $m\neq 0$), звідки отримаємо $c\,|\,t$ та виконання п. 2) означення 5.2.

Нехай тепер кільце K є факторіальним. Розіб'ємо всю множину простих елементів кільця K на класи асоційованих елементів (ці класи не перетинаються, оскільки відношення асоційованості – відношення еквівалентності). З кожного класу виберемо єдиного представника і позначимо $P=\{p_i\}_{i\geq 1}$ систему таких представників. Тоді кожен елемент $a\in K$ можна єдиним способом (з точністю до перестановки множників)

подати у вигляді добутку $a = u\prod_{i=1}^{r} p_i^{k_i}$ для деякого $u \in K^*$, $r \in N$, $p_i \in P$, $i = \overline{1,r}$ та $k_i \in N \cup \{0\}$.

Якщо при цьому для деякого $b \in K$ виконано $b = v\prod_{i=1}^{r} p_i^{l_i}$, $l_i \in N \cup \{0\}$, то справедливе нижченаведене твердження.

Твердження 5.2:

1) $a \mid b \Leftrightarrow k_i \le l_i$, $i = \overline{1,r}$;

2) $\exists НСД(a,b)$, причому $НСД(a,b) = \prod_{i=1}^{r} p_i^{s_i}$, де $s_i = \min(k_i, l_i)$;

3) $\exists НСК(a,b)$, причому $НСК(a,b) = \prod_{i=1}^{r} p_i^{t_i}$, де $t_i = \max(k_i, l_i)$.

Зокрема, якщо $(a,b) = 1$, то їх розклади не містять однакових простих елементів.

5.3. Евклідові кільця та їх властивості

Нехай K – довільне цілісне кільце.

Означення 5.4: нехай задана деяка функція $\delta : K \setminus \{0\} \to N \cup \{0\}$, що має властивості:

$$1)\ \forall a,b \in K \setminus \{0\} : \delta(ab) \ge \delta(a);$$

$$2)\ \forall a \in K, \forall b \in K \setminus \{0\}\ \exists q,r \in K : a = q \cdot b + r, \qquad (5.4)$$

причому або $r = 0$, або $\delta(r) < \delta(b)$. Тоді кільце K називається *евклідовим*. Функцію δ іноді називають *нормою на евклідовому кільці* K.

Приклад 5.5: Наведені нижче кільця є евклідовими:

– кільце Z, де $\forall a \in Z : \delta(a) = |a|$;

– кільце поліномів $F[x]$, де F – поле і $\forall f(x) \in F[x] : \delta(f) = \deg f$.

Твердження 5.3 (властивості норми):

1) якщо $a \sim b$, то $\delta(a) = \delta(b)$;

2) $\forall a \in K \setminus \{0\}: \delta(a) \geq \delta(e)$, де e – одиничний елемент K;

3) якщо $v \in K^*$, то $\delta(v) = \delta(e)$;

4) якщо для деякого $u \in K$: $\delta(u) = 0$, то $u \in K^*$.

Дане твердження рекомендується довести самостійно.

Неформально можна сказати, що кільце K є евклідовим, якщо в ньому можливе ділення з остачею. У виразі (5.4) елемент q називається часткою, а r – остачею від ділення a на b.

Якщо K – евклідове кільце, то $\forall a,b \in K\ \exists d = НСД(a,b)$.

Для знаходження НСД використовується алгоритм Евкліда, що базується на таких фактах:

1) якщо $a = bq + r$, де $r = 0$ або $\delta(r) < \delta(b)$, то $НСД(a,b) = НСД(b,r)$ (доведіть самостійно);

2) $НСД(a,0) = 0$.

Алгоритм Евкліда для знаходження $НСД(a,b)$ полягає у виконанні деякої послідовності ділень з остачею:

$$\begin{aligned} a &= q_0 b + r_1,\ \delta(r_1) < \delta(b); \\ b &= q_1 r_1 + r_2,\ \delta(r_2) < \delta(r_1); \\ r_1 &= q_2 r_2 + r_3,\ \delta(r_3) < \delta(r_2); \\ &\dots \\ r_{k-2} &= q_{k-1} r_{k-1} + r_k,\ \delta(r_k) < \delta(r_{k-1}); \\ r_{k-1} &= q_k r_k,\ r_{k+1} = 0. \end{aligned} \qquad (5.5)$$

Послідовність кроків є скінченною: оскільки $\delta(r_1) > \delta(r_2) > \dots > \delta(r_k) \geq 0$, то на деякому (не пізніше, ніж на $\delta(r_1)+1$-ому) кроці отримаємо $r_{k+1} = 0$. Тоді, очевидно, $r_k = НСД(a,b)$.

Дійсно, $r_k \mid r_{k-1}$ (випливає з останнього кроку), тому $r_k \mid r_{k-2}$ (з передостаннього кроку) і т. д., тому $r_k \mid a, r_k \mid b$. Далі, якщо для деякого $c \in K : c \mid a$ та $c \mid b$, то $c \mid r_1$ (випливає з першого кроку), $c \mid r_2$ (з другого) і т. д., тобто $c \mid r_k$.

Алгоритм Евкліда має багато важливих наслідків, які є базою для сучасної теорії чисел та суттєво використовуються у теорії скінченних полів.

5.4 Наслідки з алгоритму Евкліда

Наслідок 5.1: якщо $d = НСД(a,b)$, то $\exists u, v \in k : d = ua + vb$.

Доведення: розглянемо послідовність (5.5). З передостанньої рівності видно, що r_k є лінійною комбінацією r_{k-2} та r_{k-1}:

$$r_k = r_{k-2} - q_{k-1} r_{k-1};$$

аналогічно, $r_{k-1} = r_{k-3} - q_{k-2} r_{k-2}$, тому

$$r_k = r_{k-2} - q_{k-1}(r_{k-3} - q_{k-2} r_{k-2}) = (q_{k-1} q_{k-2} + 1) r_{k-2} - q_{k-1} r_{k-3},$$

тобто r_k також є лінійною комбінацією r_{k-2} та r_{k-3} і т. д., тобто, виконавши аналогічну процедуру відповідну кількість кроків, отримаємо вираз вигляду $r_k = ua + vb$ для деяких $u, v \in K$. Доведення закінчено.

Наслідок 5.2: якщо $НСД(a,b) = 1$, то $\exists u, v \in K : 1 = ua + vb$ (частковий випадок наслідку 5.19).

Наслідок 5.3: якщо $a \mid bc$ та $НСД(a,b) = 1$, то $a \mid c$.

Доведення: оскільки $НСД(a,b) = 1$, то $\exists u, v \in K : 1 = ua + vb$. Помножимо останню рівність на $c : uac + vbc = c$.

Оскільки, за умовою, a ділить обидва доданки у лівій частині останньої рівності, то $a \mid (uac + vbc)$, тобто $a \mid c$.

Наслідок 5.4: якщо $p \in K$ – простий елемент, то $p \mid ab \Rightarrow p \mid a$ або $p \mid b$.

Доведення: нехай $НСД(p,a) = d$. Тоді, оскільки $d \mid p$, то або $d \sim p$, або $d \sim 1$. Тобто можна вважати, що або $d = p$, або $d = 1$. Якщо $d = p$, то $p \mid a$; інакше, якщо $d = 1$, то, за наслідком 5.3, $p \mid b$.

Наслідок 5.5: якщо $a \mid b$, $c \mid b$ та $(a,c) = 1$, то $ac \mid b$.

Доведення: за наслідком 5.4 $\exists u, v \in K : au + cv = 1$. Помножимо рівність на b: $aub + cvb = b$. За умовою, ліва частина ділиться на ac, отже, $ac \mid b$.

Наслідок 5.6: якщо $(a,c) = 1$ та $(b,c) = 1$, то $(ab,c) = 1$.

Доведення: за наслідком 5.4

$$\exists u_1, v_1 \in K : u_1 a + v_1 c = 1,$$
$$\exists u_2, v_2 \in K : u_2 a + v_2 c = 1.$$

Перемножимо рівності: $u_1 u_2 ab + (u_1 a v_2 + u_2 b v_1 + v_1 v_2 c)c = 1$. Нехай $d = НСД(ab,c)$, тоді d ділить ліву частину останньої рівності, отже, $d \mid 1$, тобто $d \sim 1$ та $(a,b) = 1$.

Нижченаведене важливе твердження також є деякою мірою наслідком алгоритму Евкліда. Його рекомендується довести самостійно.

Твердження 5.4: евклідове кільце є кільцем головних ідеалів.

5.5 Факторіальність евклідових кілець

У цьому пункті доведемо, що евклідове кільце є факторіальним. Для цього знадобиться допоміжна лема.

Лема 5.1: нехай $a, b \in K$ і b є власним дільником елемента a (тобто, $b \notin K^*$ та b не асоційований з a). Тоді $\delta(b) < \delta(a)$.

Доведення: за означенням 5.4, оскільки $b \mid a$, то $\delta(a) \geq \delta(b)$. Доведемо (від супротивного), що $\delta(a) \neq \delta(b)$.

Нехай $\delta(a) = \delta(b)$. Розділимо b на a з остачею: $\exists q, r \in K : b = qa + r$, де $r = 0$ або $\delta(r) < \delta(a)$. Оскільки $b \mid a$, то $\exists c \in K : a = bc$.

Якщо $r \neq 0$, то $b = qbc + r \Rightarrow r = b(1 - qc) \Rightarrow \delta(r) \geq \delta(b) = \delta(a)$, що суперечить $\delta(r) < \delta(a)$.

Якщо $r = 0$, то $b = qa = qbc \Rightarrow b(1 - qc) = 0 \Rightarrow 1 - qc = 0$, оскільки K – цілісне та $b \neq 0$. Отже, $qc = 1$, тобто $q, c \in K^* \Rightarrow a \sim b$, що суперечить умові. Лему доведено.

Теорема 5.3: якщо K – евклідове кільце, то K – факторіальне кільце.

Доведення: з леми 5.1 випливає, що K є кільцем з розкладом на прості множники (тобто, для будь-якого $a \in K$ існує розклад вигляду (5.1), але, можливо, не єдиний). Дійсно, якщо a простий або $a \in K^*$, то очевидно, що такий розклад існує; якщо a не є простим, то будь-який його простий дільник є власним дільником, тому, за лемою 5.1, кількість його простих дільників не може бути більшою за $\delta(a)$.

Далі, за наслідком 5.4 та критерієм факторіальності (теорема 5.1), отримаємо, що K – факторіальне кільце. Теорему доведено.

Питання для самоконтролю до §5

1. Сформулюйте означення факторіального кільця. Чим це означення відрізняється від означення кільця з розкладом на прості множники?
2. Наведіть приклад факторіального кільця.
3. Сформулюйте означення факторіального кільця та наведіть приклад.
4. Який зв'язок між факторіальними та евклідовими кільцями?
5. Сформулюйте критерій факторіальності кільця.

Задачі до §5

5.1. Доведіть твердження 5.4.

5.2. Чи буде кільце $Z[X]$ поліномів з цілими коефіцієнтами факторіальним? евклідовим?

5.3. Довести: якщо елементи $a,b \in R$ є асоційованими, то $\delta(a)=\delta(b)$.

5.4. Нехай R – кільце з одиницею. Довести: 1) $\forall a \in R : \delta(e) \le \delta(a)$; 2) якщо v – оборотний елемент кільця, то $\delta(v)=\delta(e)$; 3) якщо $\delta(v)=0$, то v – оборотний елемент кільця.

5.5. Нехай R – евклідове кільце, $a,b,c \in R$. Чи справедливо, що якщо $a=bc$ та елементи a,b не є асоційованими, то $\delta(a)<\delta(b)$?

5.6. Довести, що всі оборотні елементи кільця асоційовані з одиничним елементом.

5.7*. Довести, що в скінченному (взагалі кажучи, некомутативному) кільці всі необоротні елементи є дільниками нуля, і навпаки: всі дільники нуля є необоротними елементами.

5.8. Довести зауваження 5.2.

5.9*. Чи буде факторіальним кільце $Z(\sqrt{-3})=\{a+b\sqrt{-3} \mid a,b \in Z\}$?

§6 ОЗНАЧЕННЯ ПОЛІНОМА НАД КІЛЬЦЕМ. КІЛЬЦЕ ПОЛІНОМІВ, ЙОГО ВЛАСТИВОСТІ. ФАКТОРКІЛЬЦЕ КІЛЬЦЯ ПОЛІНОМІВ. КОРЕНІ ПОЛІНОМА, ЇХ ВЛАСТИВОСТІ

6.1 Означення полінома. Дії над поліномами

Нехай R – довільне кільце.

Означення 6.1: формальна сума вигляду

$$f(x)=a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \text{ де } a_i \in R, i=\overline{0,n}, a_n \neq 0,$$

називається *поліномом над кільцем* R. Змінна x називається формальною змінною; $a_i, i=\overline{0,n}$ – коефіцієнтами полінома f; a_n – старший коефіцієнт; a_0 – вільний член. Максимальний степінь n змінної x будемо називати степенем полінома f та позначати $\deg f$. Вважається також, що $\deg O=-\infty$, де O – поліном, в якого всі коефіцієнти дорівнюють нулю кільця R.

Поліном, у якого старший коефіцієнт дорівнює одиниці, будемо називати *нормованим* або *унітарним*.

Будемо вважати, що два поліноми над кільцем R *рівні* тоді й тільки тоді, якщо рівні всі їх коефіцієнти, тобто $f(x)=g(x)$, де

$$f(x)=\sum_{i=0}^{n} a_i x^i, g(x)=\sum_{j=0}^{m} b_j x^j, a_i \in R, i=\overline{0,n}, \quad b_j \in R, j=\overline{0,m},$$

тоді й тільки тоді, якщо $m=n$ та $\forall i=\overline{0,n}: a_i=b_i$.

Зауваження 6.1: також будемо вважати, що $0\cdot x^n=0$, отже, якщо $m>n$, $a_i=0$ при $i=\overline{n+1,m}$, то $\sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{m} a_i x^i$.

Така домовленість дозволяє будь-які два поліноми записувати у вигляді сум з однаковим числом доданків (навіть якщо їх степені різні). Ми будемо використовувати такий запис лише тоді, коли він буде спрощувати викладення матеріалу.

Означення 6.2 (дії з поліномами):

1. *Додавання поліномів*: нехай

$$f(x)=\sum_{i=0}^{n} a_i x^i,\ g(x)=\sum_{i=0}^{n} b_i x^i,\ a_i, b_i \in R,\quad i=\overline{0,n},$$

причому або $a_n \neq 0$ або $b_n \neq 0$ (тут ми скористались зауваженням 6.1, хоча поліноми f та g, взагалі кажучи, можуть мають різні степені).

Тоді *сумою поліномів* $f(x)$ та $g(x)$ будемо називати поліном

$$h(x)=(f+g)(x)=\sum_{i=0}^{n} c_i x^i, \tag{6.1}$$

де $c_i = a_i + b_i$, а під операцією додавання у виразі для c_i розуміється операція додавання, визначена в кільці R.

2. *Множення поліномів*: нехай

$$f(x)=\sum_{i=0}^{n} a_i x^i,\ g(x)=\sum_{j=0}^{m} b_j x^j,\quad a_i \in R,\quad i=\overline{0,n},\quad b_j \in R,\quad j=\overline{0,m}.$$

Тоді добутком поліномів $f(x)$ та $g(x)$ будемо називати поліном

$$h(x)=(fg)(x)=\sum_{k=0}^{m+n} c_k x^k, \text{ де } c_k = \sum_{\substack{i,j=0 \\ i+j=k}}^{k} a_i b_j, \tag{6.2}$$

де під операціями додавання та множення у виразі для c_k розуміються відповідні операції в кільці R.

3. *Підстановка:* нехай $f(x)=\sum_{i=0}^{n} a_i x^i$, $b \in R$. Тоді вираз $f(b)=\sum_{i=0}^{n} a_i b^i$ перестає бути формальною сумою; оскільки він містить лише елементи кільця R та операції над цими елементами, то його значенням буде елемент кільця R. Значення виразу $f(b)$ називається *значенням полінома* $f(x)$ *у точці* $b \in R$ (або *при* $x=b$).

Зауваження 6.2: для степеня суми та добутку поліномів справедливі такі нерівності

$$\deg(f+g) \le \max\{\deg g, \deg f\};$$

$$\deg(f \cdot g) \le \deg f + \deg g, \tag{6.3}$$

причому, якщо R – цілісне кільце, то

$$\deg(f \cdot g) = \deg f + \deg g. \tag{6.4}$$

(Нерівності (6.3) та рівність (6.4) доведіть самостійно; нерівності можна довести за означенням, а рівність – наприклад, від супротивного).

6.2 Кільце поліномів та його властивості

З означення 6.2 випливає, що множина поліномів над кільцем R з операціями (6.1) та (6.2) утворює кільце. Дане кільце називається *кільцем поліномів над кільцем* R та позначається $R[x]$.

Елементи кільця R (не рівні нулю) можна вважати поліномами нульового степеня, тому вважаємо, що $R[x] \supset R$.

Теорема 6.1 (властивості кільця $R[x]$):

1) якщо R – комутативне, то $R[x]$ також комутативне;

2) якщо R – кільце з одиницею, то $R[x]$ також кільце з одиницею;

3) якщо R – цілісне, то $R[x]$ також цілісне.

Доведення: п. 1 випливає безпосередньо з означення комутативного кільця та добутку поліномів (5.2).

Для доведення п. 2 достатньо зазначити, що одиниця e кільця R є також одиницею кільця $R[x]$.

Доведемо п. 3. Нехай R – цілісне, тоді за пп. 1 і 2 $R[x]$ – комутативне кільце з одиницею. Залишилось довести, що в $R[x]$ відсутні дільники нуля. Припустимо супротивне: нехай для деяких ненульових поліномів $f(x)=\sum_{i=0}^{n} a_i x^i$ та $g(x)=\sum_{i=0}^{n} b_j x^i$, $a_n \neq 0, b_m \neq 0$, виконується $f(x)\cdot g(x)=0$. Тоді, за означенням добутку поліномів та означенням нульового полінома, $a_n b_m = 0$.

Але, за умовою, $a_n, b_m \in R$, де R – цілісне кільце, та $a_n \neq 0$, $b_m \neq 0$, тому, за означенням цілісного кільця, $a_n b_m \neq 0$, що суперечить нашому припущенню. Отже, в $R[x]$ відсутні дільники нуля. Теорему доведено.

Надалі ми будемо розглядати кільце поліномів $F[x]$ над полем F. В цьому випадку для будь-яких поліномів $f(x), g(x) \in F[x]$ можна визначити операцію ділення з остачею полінома $f(x)$ на поліном $g(x)$ (це можливо внаслідок того, що у полі F всі елементи, крім нуля, мають обернені відносно операції множення). Розглянемо ділення з остачею на прикладі.

Приклад 6.1:

Нехай $F = F_1$, $f(x) = x^5 + x^3 + 2x^2 + 2x + 1$, $g(x) = 2x^2 + x + 2$.

Тоді ділення $f(x)$ на $g(x)$ виконується так:

$$
\begin{array}{l|l}
x^5 + x^3 + 2x^2 + 2x + 1 & 2x^2 + x + 2 \\
\underline{x^5 + 2x^4 + x^3} & 2x^3 + 2x^2 + 2x + 1 \\
-x^4 + 2x^2 & \\
\underline{x^4 + 2x^3 + x^2} & \\
-x^3 + x^2 + 2x & \\
\underline{x^3 + 2x^2 + x} & \\
-2x^2 + x + 1 & \\
\underline{2x^2 + x + 2} & \\
2 &
\end{array}
$$

Тут ми скористались тим, що в полі F_3 $2 \cdot 2 = 1$, $-2 = 1$ та $-1 = 2$. Отже, часткою від ділення $f(x)$ на $g(x)$ є поліном $q(x) = 2x^3 + 2x^2 + 2x + 1$, а остачею – поліном нульового степеня $r(x) = 2$.

Результат ділення з остачею ми будемо записувати так: $f(x) = g(x)q(x) + r(x)$; для наведеного прикладу 6.1 запис буде мати вигляд $x^5 + x^3 + 2x^2 + 2x + 1 = (2x^2 + x + 2)(2x^3 + 2x^2 + 2x + 1) + 2$.

Остачу від ділення $f(x)$ на $g(x)$ ми позначатимемо $f(x) \bmod g(x)$ (зауважимо, що при $\deg f < \deg g$: $f(x) \bmod g(x) = f(x)$).

Отже, для будь-яких $f(x), g(x) \in F[x]$ існують такі $q(x), r(x) \in F[x]$, що $f(x) = q(x)g(x) + r(x)$, де $\deg r(x) < \deg g(x)$ або $r(x) \equiv 0$. Також зазначимо, що, згідно із зауваженням 6.4, $\deg(f \cdot g) \geq \deg f$ при $f(x), g(x) \neq 0$. Тому, згідно з означенням 5.1, кільце $F[x]$ поліномів над полем F є евклідовим з "нормою" $\delta(f) = \deg f$. Тоді, за теоремою 5.3, $F[x]$ – факторіальне кільце. У евклідовому кільці завжди існують НСД і НСК для будь-яких двох елементів. У кільці поліномів над полем під НСД або НСК ми, як правило, будемо вважати нормований поліном. При такому обмеженні НСД і НСК завжди існують і єдині.

Означення 6.3: прості елементи кільця $F[x]$ будемо називати *незвідними поліномами*.

Сформулюємо ще одне означення, еквівалентне означенню 6.3.

Поліном $f(x) \in F[x] (f(x) \neq 0)$ називається *незвідним*, якщо виконується така умова: якщо для деяких $g_1(x)$ та $g_2(x)$ виконується рівність $f(x) = g_1(x)g_2(x)$, то або $\deg g_1 = 0$, або $\deg g_2 = 0$.

Зазначимо, що *оборотними елементами кільця* $F[x]$ будуть всі елементи з F^* і тільки вони. Тому для будь-якого полінома $f(x) \in F[x]$ його дільниками завжди будуть всі елементи з F^*, а також всі асоційовані з ним елементи, тобто поліноми вигляду $a \cdot f(x)$, де $a \in F^*$. Такі дільники ми будемо називати *тривіальними*. Всі інші дільники будемо називати *нетривіальними*, або *власними*.

Тому означення незвідного полінома можна ще переформулювати так: поліном є незвідним, якщо він не має нетривіальних дільників.

Нагадаємо (твердження 5.4), що евклідове кільце завжди є кільцем головних ідеалів. Тому, згідно з п. 4 теореми 4.4, факторкільце $F[x]/(f)$ є полем тоді і лише тоді, коли поліном $f(x) \in F[x]$ є незвідним.

При подальшому вивченні теорії скінченних полів ми будемо весь час використовувати факторкільце вигляду $F[x]/(f)$, де $f(x) \in F[x]$, тому розглянемо структуру такого факторкільця більш детально.

Нагадаємо, що при визначенні факторкільця (означення 3.15) ми встановили, що операції на класах лишків визначені коректно, а саме: якщо I – ідеал кільця R, $a_1, a_2, b_1, b_2 \in R$, причому $a_1 + I = b_1 + I$, $a_2 + I = b_2 + I$, то $(a_1 + I) + (a_2 + I) = (b_1 + I) + (b_2 + I)$; $(a_1 + I)(a_2 + I) = (b_1 + I)(b_2 + I)$. Тобто, операції на класах лишків не залежать від того, як саме ці класи лишків представлені. Тому кожен клас

лишків у кільці $F[x]/(f)$ ми можемо замінити на деякий елемент цього класу, який називається його представником; при цьому встановиться взаємно однозначна відповідність між класами лишків та їх представниками, множина яких називається системою представників. Після цього всі обчислення у факторкільці можна замінити еквівалентними обчисленнями у системі представників. Нехай, наприклад, $f(x), g(x) \in F[x]$, I – деякий ідеал кільця $F[x]$, причому

$$(f(x)+I)+(g(x)+I)=h(x)+I, \qquad (6.5)$$

$$(f(x)+I)\cdot(g(x)+I)=u(x)+I,$$

для деяких $h(x), u(x) \in F[x]$. Оберемо представників: $f_1(x) \in f(x)+I$, $g_1(x) \in g(x)+I$, $h_1(x) \in h(x)+I$, $u_1(x) \in u(x)+I$. Тоді замість рівностей (6.5) будемо записувати: $f_1(x)+g_2(x)=h_1(x)$; $f_1(x)\cdot g_2(x)=u_1(x)$.

Нехай $f(x) \in F[x]$, $\deg f = n$. Зауважимо, що кожен клас лишків факторкільця $F[x]/(f)$ містить єдиний поліном, степінь якого менший за n (оскільки для будь-яких двох поліномів з одного класу лишків їх різниця ділиться на $f(x)$). Тому при побудові факторкільця $F[x]/(f)$ стандартною є така система представників: з кожного класу обирається поліном, степінь якого менший за n (це буде поліном найменшого степеня у даному класі лишків). Добуток двох представників (відносно множення у кільці $F[x]$), взагалі кажучи, не належить системі представників (його степінь може бути більшим за n). Тому, щоб знайти значення добутку представників $f_1(x)$ та $g_1(x)$ у кільці $F[x]/(f)$, потрібно спочатку перемножити їх як елементи кільця $F[x]$, отримавши деякий поліном $h(x) \in F[x]$, а потім

знайти відповідного представника як поліном найменшого степеня у тому класі лишків, що містить поліном $h(x)$; він буде мати вигляд $h(x) \bmod f(x)$.

Приклад 6.2: нехай $f(x) = 2x^3 + x + 2 \in F_3[x]$.

Побудуємо факторкільце $F_3[x]/(f)$. Порядок даного кільця дорівнює кількості поліномів над F_3, степені яких менші за 3. Дійсно, кожен клас лишків вигляду $g(x)+(f)$ містить єдиний поліном степеня, меншого за 3: це поліном $g(x) \bmod f(x)$. І навпаки, кожному поліному $u(x)$, де $\deg u < 3$, ставиться у відповідність клас лишків $u(x)+(f)$. Тому систему представників будуть утворювати всі поліноми вигляду $ax^2 + bx + c$, де $a,b,c \in F_3$, тобто факторкільце $F_3[x]/(f)$ складається з 27-ми елементів. Як було зазначено, операція множення представників виконується за модулем полінома $f(x)$:

$$(2x^2 + x)\cdot(x^2 + 2x + 1) = x + 1.$$

Приклад 6.3: побудувати факторкільце $F_2[x]/(f)$, де $f(x) = x^3 + x + 1 \in F_2[x]$, та скласти таблиці Келі додавання та множення його елементів.

Розв'язання: кільце $F_2[x]/(f)$, записане як система представників, складається з усіх лишків від ділення на поліном $f(x)$, тобто з усіх поліномів над F_2, степені яких менші за 3: $F_2[x]/(f) = \{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$.

Таблиця Келі додавання:

+	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Таблиця Келі множення:

×	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	$x+1$
x^2+1	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	x^2+x+1	x^2+1	x	$x+1$	x^2+x	x^2	1

Зауваження 6.3: факторкільце $F_p[x]/(f)$, де p – просте, $f(x)\in F_p[x]$, $\deg f=n$, містить p^n елементів; це поліноми вигляду $\sum_{i=0}^{n-1} a_i x^i$, де $a_i\in F_p[x]$.

6.3 Корені поліномів та їх властивості

Означення 6.4: нехай $f(x)\in F[x]$, $b\in F$. Якщо $f(b)=0$, то елемент b називається *коренем* або *нулем* полінома $f(x)$.

Приклад 6.4: елемент $2\in F_3$ є коренем полінома $f(x)=x^2+2x+1\in F_3[x]$.

Теорема 6.2 (теорема Безу): нехай $b \in F$, $f(x) \in F[x]$. Елемент b є коренем полінома $f(x)$ тоді і тільки тоді, коли $x-b \mid f(x)$.

Доведення: нехай $x-b \mid f(x)$, тобто $\exists g(x) \in F[x]: f(x) = (x-b)g(x)$. Тоді $f(b) = 0$, $g(b) = 0$.

Нехай тепер $f(b) = 0$. Припустимо, що $x-b$ не ділить поліном $f(x)$. Тоді при діленні полінома $f(x)$ на $x-b$ отримаємо ненульову остачу:

$$\exists g(x), r(x) \in F[x], r(x) \neq 0: \; f(x) = g(x)(x-b) + r(x).$$

За означенням ділення з остачею, $-\infty < \deg r(x) < \deg r(x-b) = 1$, тому $\deg r(x) = 0$, тобто $r(x) = r \in F$, тобто

$$f(x) = g(x)(x-b) + r, \; r \neq 0.$$

Але тоді $f(b) = g(b) \cdot 0 + r = r \neq 0$, що суперечить умові $f(b) = 0$. Теорему доведено.

Означення 6.5: нехай $f(x) \in F[x]$, $b \in F$, $f(b) = 0$. Якщо для деякого $k \in N$ виконується $(x-b)^k \mid f(x)$, але $(x-b)^{k+1}$ не ділить $f(x)$, то будемо говорити, що елемент b є k-кратним коренем полінома $f(x)$.

Якщо $k = 1$, то корінь називається простим; інакше – кратним.

Теорема 6.3: нехай $f(x) \in F[x]$, $\deg f = n > 0$, $b_1, \ldots, b_m \in F$ – різні корені полінома $f(x)$, $k_1, \ldots, k_m$ – їх кратності. Тоді:

1) $\prod_{i=1}^{m} (x-b_i)^{k_i} \mid f(x)$;

2) $k_1 + \ldots + k_m \leq n$; зокрема $m \leq n$.

Доведення: поліноми $(x-b_i)^{k_i}$ та $(x-b_j)^{kj}$ при $i \neq j$, $i, j = \overline{1,m}$, є взаємно простими. За теоремою Безу та означенням 6.5 $(x-b_j)^{k_j} \mid f(x), i = \overline{1,m}$.

Як було показано раніше, кільце $F[x]$ є евклідовим, тому, за наслідком 5.5 алгоритму Евкліда, $\prod_{i=1}^{m}(x-b_i)^{k_i} | f(x)$. Перший пункт доведено.

Доведемо п. 2) (від супротивного). Нехай $k_i + ... + k_m = l > n$. Тоді, за п. 1) $g(x) = \prod_{i=1}^{m}(x-b_i)^{k_i} | f(x)$. Але $\deg g(x) = m > n = \deg f(x)$, тому $g(x)$ не може ділити $f(x)$, що суперечить п. 1). Теорему доведено.

Означення 6.6: нехай $f(x) = \sum_{i=0}^{n} a_i x^i, a_i \in F$. *Похідною полінома* $f(x)$ називається поліном $f'(x) = \sum_{i=0}^{n} i a_i x^{i-1} \in F[x]$.

Твердження 6.1 (властивості похідної): нехай $f(x), g(x) \in F[x]$. Тоді

$$(f(x)+g(x))' = f'(x)+g'(x);$$
$$(f(x)\cdot g(x))' = f'(x)\cdot g(x)+f(x)\cdot g'(x).$$

Це твердження рекомендується довести самостійно (наприклад, безпосередньою перевіркою).

Теорема 6.4: нехай $f(x) \in F[x], b \in F, f(b) = 0$. Тоді

$$(x-b)^k \mid f(x) \Leftrightarrow (x-b)^{k-1} \mid f'(x).$$

Доведення: нехай $(x-b)^k \mid f(x)$, тобто $\exists g(x) \in F[x]: f(x) = (x-b)^k g(x)$. Тоді

$$f'(x) = k(x-b)^{k-1} g(x) + (x-b)^k g'(x) = (x-b)^{k-1} \cdot (k \cdot g(x) + (x-b) \cdot g'(x)),$$

тобто $(x-b)^{k-1} \mid f'(x)$.

Нехай тепер $f(b) = 0$ та $(x-b)^{k-1} \mid f'(x)$. Тоді за теоремою Безу $f(x) = (x-b)g(x)$, і $f'(x) = g(x) + (x-b)g'(x)$.

Зауваження 6.4:

1) всі поліноми першого степеня є незвідними;

2) всі поліноми першого степеня мають корені у полі F: дійсно, коренем полінома $f(x)=ax+b$, де $a,b\in F$, є елемент $-ba^{-1}\in F$;

3) будь-який поліном над полем F, який ділиться на деякий поліном першого степеня, має корінь у полі F (це буде корінь того полінома першого степеня, на який він ділиться);

4) якщо $\deg f\geq 2$ та поліном $f(x)$ незвідний, то він не має коренів в полі F. Дійсно, якщо b – корінь полінома $f(x)$, то, за теоремою Безу, $x-b|f(x)$, тобто $f(x)$ має нетривіальний дільник, оскільки $0<1=\deg(x-b)<\deg f$.

Теорема 6.5 (критерій незвідності поліномів 2-го та 3-го степенів): нехай $f(x)\in F[x]$, $\deg f=2$ або $\deg f=3$. Тоді нижчевказані твердження рівносильні:

1) $f(x)$ незвідний;

2) $f(x)$ не має коренів в F.

Доведення: твердження 2) випливає з твердження 1) без будь-яких обмежень на степінь полінома (див. зауваження 6.4). Доведемо від супротивного, що твердження 1) випливає з твердження 2).

Нехай $f(x)$ не має коренів в F, але не є незвідним. Тоді $f(x)$ можна розкласти на нетривіальні множники: $\exists u(x),v(x),1\leq\deg u,\deg v<\deg f: f(x)=u(x)v(x)$. Оскільки $\deg f=\deg u+\deg v$ та або $\deg f=2$, або $\deg f=3$, то або $\deg u=1$, або $\deg v=1$. Нехай $\deg(u)=1$, тобто $u(x)=ax+b; a,b\in F$. Тоді елемент $x_0=-ba^{-1}$ є коренем полінома $u(x)$, а отже і полінома $f(x)$, що суперечить умові. Теорему доведено.

Зауваження 6.5: умова $f(x) \in F[x]$, $\deg f = 2$ або $\deg f = 3$ у теоремі 6.5 є суттєвою. Наприклад, поліном четвертого степеня $f(x) = x^4 + x^2 + 1 \in F_2[x]$ не має коренів в F_2, але не є незвідним: $f(x) = (x^2 + x + 1)^2$.

Теорема 6.6 (інтерполяційна формула Лагранжа побудови полінома за його значенням): нехай $n \geq 0$, $a_0, a_1, ..., a_n \in F$ – різні, $b_0, b_1, ..., b_n \in F$.

Тоді $\exists! f(x) \in F[x]: \deg \leq n; f(a_i) = b_i, i = \overline{0,n}$.

Цей поліном має вигляд: $f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} \{(a_i - a_k)^{-1}(x - a_k)\}$.

Доведення: безпосередньою перевіркою легко переконатись, що $f(a_i) = b_i, i = \overline{0,n}$; крім того, за побудовою, $\deg f \leq n$, оскільки степінь кожного доданка не перевищує n. Доведемо єдиність такого полінома від супротивного. Припустимо, існує ще один поліном $g(x) \neq f(x)$ такий, що $\deg g \leq n$ і $g(a_i) = b_i, i = \overline{0,n}$. Розглянемо поліном $h(x) = f(x) - g(x)$. Оскільки $g(x) \neq f(x)$, то $h(x) \neq 0$ і $\deg h \leq n$. Але, оскільки $\forall_i = \overline{0,n}$: $f(a_i) = g(a_i)$, то $\forall_i = \overline{0,n}$: $h(a_i) = 0$, що суперечить п. 2 теореми 6.3. Теорему доведено.

Питання для самоконтролю до §6

1. Сформулюйте означення кільця поліномів. Наведіть приклади такого кільця та операцій у ньому.

2. Дайте означення незвідного полінома. Обґрунтуйте еквівалентність трьох означень, наведених у цьому параграфі.

3. Поясніть своїми словами, чому кільце поліномів над полем буде евклідовим, а над довільним кільцем, взагалі кажучи, – ні. Наведіть приклад кільця поліномів, що не буде евклідовим.

4. Сформулюйте критерій незвідності поліномів другого та третього степенів.

5. Сформулюйте теорему про кількість коренів полінома у полі.

6. Дайте означення похідної полінома та назвіть її властивості.

7. Сформулюйте означення кратного кореня та критерій наявності кратних коренів у полінома.

8. Сформулюйте теорему Безу.

Задачі до §6

6.1. Доведіть зауваження 6.2.

6.2. Доведіть твердження 6.1.

6.3. Нехай F – довільне поле. Довести: або $charF = p$, де p – деяке просте число, або $charF = 0$.

6.4. Нехай F – довільне поле. Довести: якщо $charF \neq 0$, то $charF = \min\{n \in N : n \cdot e = 0\}$.

6.5. Нехай R – комутативне кільце. Довести: оборотні елементи кільця $R[X]$ – це оборотні елементи кільця R і тільки вони.

6.6. Довести, що кількість кроків у алгоритмі Евкліда при діленні поліномів має порядок n, де n – більший зі степенів поліномів, і що цю оцінку не можна покращити.

6.7. Знайти найбільший спільний дільник заданих поліномів над F_3 та виразити його через їх лінійну комбінацію: $f(x) = x^3 + 2x + 1$, $g(x) = x^2 + x + 2$.

6.8. Для поліномів $f_1, \ldots, f_n$ довести:

а) $\deg(НОД(f_1, \ldots, f_n)) \leq \deg(НОД(f_1, \ldots, f_m))$ при $m \leq n$;

б) $(f_1, f_2, f_3) = (f_1, (f_2, f_3))$.

6.9. Довести, не використовуючи евклідність кільця $F[X]$ (де F – деяке поле), існування і єдиність найбільшого спільного дільника та найменшого

спільного кратного для будь-якого набору поліномів. (Вказівка: розглянути ідеал, породжений всіма лінійними комбінаціями заданих поліномів; розглянути ідеал $(f_1)\cap\ldots\cap(f_n)$ – найменший ідеал, що містить ці поліноми).

6.10. Нехай R – евклідове кільце, що не містить оборотних елементів, крім ±1. Чи можна стверджувати, що R[X] – також евклідове кільце? Довести або навести контрприклад.

6.11. Використовуючи тотожності $(1+X)^n=\sum_{i=0}^{n}C_n^iX^i$,

$(1+X)^n(1+X)^m=(1+X)^{n+m}$, довести: $\sum_{i=0}^{k}C_m^iC_n^{k-i}=C_{m+n}^k$.

6.12. Повторення. Нехай G – деяка група, A, B – її нормальні підгрупи, причому $A\cap B=\{e\}$. Довести: $\forall a\in A,\forall b\in B: ab=ba$.

6.13. Нехай F – деяке поле, $f, g\in F[x]$. Довести: $(f)\subset(g)\Leftrightarrow g\mid f$.

6.14. Нехай F – деяке поле, $f(x),g(x)\in F[X]$, $\deg f>0,\deg g>0$, $(f,g)=1$. Довести:

$\exists a(x),b(x)\in F[x]:\deg a<\deg g,\quad \deg b<\deg f,\quad a(x)f(x)+b(x)g(x)=1$.

6.15. Нехай F – деяке поле, $f_1(x),\ldots,f_n(x)\in F[X]$, $f_i(x)=d(x)g_i(x)$, де $d(x)=(f_1(x),\ldots,f_n(x))$. Довести: $(g_1(x),\ldots,g_n(x))=1$.

6.16. Побудувати таблиці Келі додавання та множення для факторкільця $F[x]/(x^3+x^2+x)$. Чи буде задане факторкільце полем? Чому?

6.17. Позначимо [x+1] – клас лишків у факторкільці $F[x]/(x^4+1)$, що містить елемент x+1. Знайти класи лишків, що утворюють у цьому кільці ідеал ([x+1]).

6.18. Визначити, чи мають нижченаведені поліноми кратні корені:

a) $f(x)=x^4-5x^3+6x^2+4x-8\in Q[x]$;

b) $f(x)=x^6+x^5+x^4+x^3+1\in F_2[x]$?

6.19. Знайти такий поліном $f(x)$, що:

a) $f(0)=f(1)=f(4)=1,\quad f(2)=f(3)=3,\quad f\in F_5[x],\quad \deg f\le 4;$

b) $f(-1)=-1,\ f(0)=3,\quad f(1)=3,\ f(2)=5,\quad f\in Q[x],\quad \deg f\le 3.$

6.20. Нехай $K\subset F$, де F – деяке поле. Довести: K є підполем поля F тоді і тільки тоді, коли одночасно виконуються умови:

1) K містить не менше двох елементів;

2) $\forall a,b\in K$ виконується $a-b\in K$;

3) $\forall a,b\in K$, де $b\neq 0$, виконується $ab^{-1}\in K$.

6.21. Довести: $f(x)=x^4+x+1\in F_2[x]$ – незвідний. Побудувати таблиці додавання та множення у факторкільці $F_2[x]/f(x)$. Чи буде це факторкільце полем? Чому?

6.22. Нехай R – евклідове кільце, $a,b,c\in R$, a,c – прості, не асоційовані між собою. Довести: якщо a/b, c/b, то ac/b.

ГЛОСАРІЙ

автоморфізм 32	automorphism
— внутрішній 38	— inner automorphism
— груп 32	— of groups
— кілець 53	— of rings
алгебраїчна система 17	algebraic system
відображення 13	map, mapping, imaging
— бієктивне 13	— bijective
— ін'єктивне 13	— injective
— сюр'єктивне 13	— surjective
генератор групи 23	group generator
гомоморфізм 32	homomorphism
— груп 32	— of groups
— кілець 53	— of rings
група 18	group
— абелева 18	— abelian
— адитивна 45	— additive
— лишків 19	— residue
— мультиплікативна 48	— multiplicative
— нескінченна 21	— infinite
— скінченна 21	— finite
— циклічна 22	— cyclic
дільник 60	divisor
— власний 64	— proper
— нетривіальний 64	— non-trivial
— нуля 46	— of zero, zero divisor
— одиниці 47	— of unity
— тривіальний 64	— trivial
елемент	element
— асоційований (з якимось елементом) 60	— associate, associated
— обернений (до якогось елемента) 18	— inverse (for some element)
— оборотний 60	— invertible

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Глухов М. М.* Алгебра : учебник в 2-х томах / *М. М. Глухов, В. П. Елизаров, А. А. Нечаев.* – М. : Гелиос АРВ, 2003. – Т. I. 336 с., Т. II. 416 с.

2. *Ван-дер-Варден Б. Л.* Алгебра / *Б. Л. Ван-дер-Варден.* – М. : Наука, 1975. – 649 с.

3. *Коблиц Н.* Курс теории чисел и криптографии. / Н. Коблиц – М. : Научное изд-во ТВП, 2001. – 254 с.

4. *Лидл Р.* Конечные поля: в 2-х томах / *Р. Лидл, Г. Нидеррайтер.* – М. : Мир, 1988. – Т. 1. – 430 с.

5. *Кострикин А. И.* Введение в алгебру / *А. И. Кострикин.* – М.: Наука, 1977. – 496 с.

6. *Мальцев А. И.* Алгебраические системы / *А. И. Мальцев.* – М. : Наука, 1970. – 392 с.

7. *Биркгоф Г., Барти Т.* Современная прикладная алгебра / *Г. Биркгоф, Т. Барти.* – М. : Мир, 1976. – 400 с.

8. *Ленг С.* Алгебра / *С. Ленг.* – М. : Мир, 1968. – 572 с.

9. *Курош А. Г.* Общая алгебра / *А. Г. Курош.* – М. : Физматлит, 1970. – 162 с.

10. *Ковальчук Л. В.* К вопросу о триномах, делящихся на заданный примитивный полином над GF_2 / *Л. В. Ковальчук* // Сборник научных трудов "Защита информации". – 2005. – Вып. 12. – С. 117–126.

11. *Ковальчук Л. В.* Псевдонеприводимые полиномы. Вероятностное тестирование неприводимости / *Л. В. Ковальчук* // Кибернетика и системный анализ. – 2004. – № 4. – С. 168–176.

12. *Яремчук Ю. Є.* Алгебраїчні моделі асиметричних криптографічних систем / *Ю. Є. Яремчук* // Захист інформації. – 2014. – Том 16, № 1. – С. 68–80.

13. *Яремчук Ю. Є.* Рекурентні послідовності як основа криптографічних методів / *Ю. Є. Яремчук* // Наукові записки Українського науково-дослідного інституту зв'язку. – 2012. – № 4(24). – С. 21–25.

Навчальне видання

Ковальчук Людмила Василівна
Яремчук Юрій Євгенович

ПРИКЛАДНА АЛГЕБРА
Частина 1. Основи абстрактної алгебри

Навчальний посібник

Редактор В. Дружиніна

Оригінал-макет підготовлено Ю. Є. Яремчуком

Підписано до друку 19.03.2015 р.
Формат 29,7×42¼. Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк. 6,3.
Наклад 75 пр. Зам. № 2015-037.

Вінницький національний технічний університет,
навчально-методичний відділ ВНТУ.
21021, м. Вінниця, Хмельницьке шосе, 95.
ВНТУ, к. 2201.
Тел. (0432) 59-87-36.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.

Віддруковано у Вінницькому національному технічному університеті
в комп'ютерному інформаційно-видавничому центрі.
21021, м. Вінниця, Хмельницьке шосе, 95.
ВНТУ, ГНК, к. 114.
Тел. (0432) 59-87-38.
Свідоцтво суб'єкта видавничої справи
серія ДК № 3516 від 01.07.2009 р.