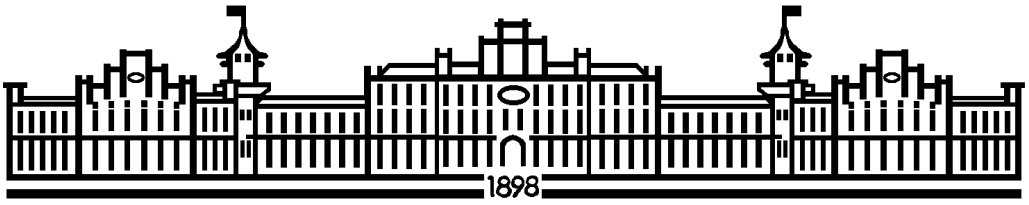


МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«Київський політехнічний інститут»

Т.В. Авдєєва В.М. Горбачук

ПРИКЛАДНА АЛГЕБРА

АЛГЕБРАЇЧНІ СТРУКТУРИ. МОРФІЗМИ. ОСНОВИ ТЕОРІЇ ЗОБРАЖЕНЬ ГРУП

Навчальний посібник

Київ
НТУУ «КПІ»
2015

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«Київський політехнічний інститут»

Т.В. Авдєєва В.М. Горбачук

ПРИКЛАДНА АЛГЕБРА

АЛГЕБРАЇЧНІ СТРУКТУРИ. МОРФІЗМИ. ОСНОВИ ТЕОРІЇ ЗОБРАЖЕНЬ ГРУП

Навчальний посібник

“Рекомендовано”
Методичною радою НТУУ “КПІ”

Київ
НТУУ «КПІ»
2015

УДК 512.8 (076)
512 (075.8)
ББК 22.14

Гриф надано методичною радою НТУУ «КПІ»
(протокол № 5 від 8червня 2015 р.)

Рецензенти: ***О.Г. Ганюшкін,*** канд. фіз.-мат. наук, доцент.,
Київський національний університет
Імені Тараса Шевченка

В*.В. Сергійчук**,* доктор фіз.-мат. наук,
провідний науковий співробітник
Інституту математики НАН України

Відповідальний
редактор: ***Н.О. Вірченко,*** д-р фіз.-мат. наук, проф.,
Національний технічний університет України
«Київський політехнічний інститут»

Прикладна алгебра. ***Алгебраїчні структури. Морфізми. Основи теорії зображень груп***. Навчальний посібник /Т.В. Авдєєва, В.М. Горбачук.- К.: НТУУ «КПІ», 2015. – 56 с. – Бібліогр.: с. 56. –100 пр.

В навчально-методичному посібнику викладено короткі теоретичні відомості з теорії груп, кілець і полів, даються приклади розв’язування задач з відповідних розділів. Наводяться варіанти індивідуальних завдань для самостійної роботи студентів.

Призначений для студентів фізико-математичного факультету НТУУ “ КПІ ”, може бути використаний також в інших університетах при вивчені курсу “ Прикладної алгебри”.

УДК 512.8 (076)
512 (075.8)
ББК 22.14

ЗМІСТ

Передмова

Посібник є методичним забезпеченням курсу прикладної алгебри, який, як відомо, є невід'ємною частиною фундаментальної підготовки для студентів спеціальності "Математика".

Даний посібник містить програму курсу, короткі теоретичні відомості та велику кількість прикладів, вправ і задач, необхідних для виконання типових розрахунків з цього курсу. Наводяться також наближені варіанти планових контрольних та самостійних робіт і перелік питань для колоквіумів.

Посібник розрахований на студентів фізико-математичного та інших факультетів для використання в навчальному процесі, пов'язаному з алгеброю.

ПРОГРАМА КУРСУ

4 семестр

Тема 1. Групи

Нормальні підгрупи, їх властивості, фактор групи, гомоморфізм груп, основні теореми про гомоморфізм, ізоморфізм груп, пряма сума та добуток груп, абелеві групи, скінчені абелеві групи, розклад скінченої абелевої групи.

Тема 2. Кільця

Кільця, основні властивості кілець, кільця з одиницею, дільники нуля, гомоморфізм кілець, ідеали кільця, кільця головних ідеалів, фактор-кільце, пряма сума кілець, мультиплікативна група кільця класів лишків.

Тема 3. Поля

Поля, поле класів лишків за простим модулем, властивості полів, підполе, класифікація полів, поле алгебраїчних чисел, розширення поля, прості розширення поля, алгебраїчні розширення полів, скінченні поля, гомоморфізм полів.

Тема 4. Елементи теорії зображень груп

Модулі, приклади модулів, властивості модулів, зображення групи, приклади зображень, характер зображення, представлення зображення через незвідні.

Розділ 1. АЛГЕБРАЇЧНІ СТРУКТУРИ

1.1. Фактор–група

Підгрупа H групи G називається **нормальною підгрупою**, або **нормальним дільником** цієї групи, якщо для довільного елемента g групи G виконується умова $gH = Hg$. Це означає, що для довільного елемента g групи G та елемента $h \in H$ можна знайти в підгрупі H таки елементи h_1 та h_2, що $hg = gh_1$ і $gh = h_2 g$. Зрозуміло, що умова $gH = Hg$ рівносильна умові $g^{-1}Hg = H$. Якщо підгрупа H нормальна в групи G, то записують $H \lhd G$. У довільної групі G одинична підгрупа E та сама група G є її нормальними підгрупами. Група G називається **простою**, якщо вона немає жодної іншої нормальної підгрупи крім G та E. Зауважимо, що проста група може мати нетривіальні підгрупи, але вони не повинні бути нормальними. Нехай $G-$група, $H-$ нормальна підгрупа групи G. Розглянемо розклад групи G на класи суміжності за підгрупою H. Оскільки H нормальна підгрупа групи G, то ліві суміжні класи групи G за підгрупою H будуть збігатися з правими суміжними класами, тому далі будемо говорити просто про суміжні класи групи G за підгрупою H. Множина цих класів суміжності позначається G/H.

На множині суміжних класів групи G за нормальною підгрупою H вводиться операція множення таким чином: $g_1H \cdot g_2H = g_1g_2H$. Якщо операція на G записується адитивно, то на множині суміжних класів групи G за нормальною підгрупою H визначається операція додавання таким чином: $(g_1 + H) + (g_2 + H) = (g_1 + g_2)H$. Множина суміжних класів G/H із так визначеною операцією множення (додавання) утворює групу, яка називається **фактор–групою** групи G за нормальною підгрупою H.

Приклад 1. Скласти таблицю Келі для фактор–групи U_{12}/U_4.

Розв'язання. Група U_{12} всіх коренів 12–го степеня з одиниці складається з елементів $1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots, \varepsilon_{11}$, де $\varepsilon_k = \cos\frac{2\pi}{12}k + i\sin\frac{2\pi}{12}k$.

Група U_4 всіх коренів 4–го степеня з одиниці складається з елементів $1, \varepsilon_3, \varepsilon_6, \varepsilon_9$.

Фактор–група U_{12}/U_4 складається з трьох класів суміжності:

$$U_4 = \{1, \varepsilon_3, \varepsilon_6, \varepsilon_9\},\ \varepsilon_1 U_4 = \{\varepsilon_1, \varepsilon_4, \varepsilon_7, \varepsilon_{10}\},\ \varepsilon_2 U_4 = \{\varepsilon_2, \varepsilon_5, \varepsilon_8, \varepsilon_{11}\},$$

а таблиця Келі має вигляд

·	U_4	$\varepsilon_1 U_4$	$\varepsilon_2 U_4$
U_4	U_4	$\varepsilon_1 U_4$	$\varepsilon_2 U_4$
$\varepsilon_1 U_4$	$\varepsilon_1 U_4$	$\varepsilon_2 U_4$	U_4
$\varepsilon_2 U_4$	$\varepsilon_2 U_4$	U_4	$\varepsilon_1 U_4$

Приклад 2. Скласти таблицю Келі для фактор–групи $Z/5Z$.

Оскільки $5Z = \{5k : k \in Z\}$, то фактор–група $Z/5Z$ складається з 5 класів суміжності:

$$\bar{0} = 5Z,\ \bar{1} = 1 + 5Z,\ \bar{2} = 2 + 5Z,\ \bar{3} = 3 + 5Z,\ \bar{4} = 4 + 5Z.$$

Таблиця Келі має вигляд

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

Кожна фактор–група абелевої групи також є абелевою, кожна фактор–група циклічної групи також є циклічною.

Завдання 1. Скласти таблицю Келі для фактор–групи:

1) $3Z/15Z$.
2) $4Z/12Z$.
3) $4Z/20Z$.
4) $12Z/48Z$.
5) A_4/K_4.
6) $2Z/12Z$.
7) $5Z/25Z$.
8) U_{12}/U_3.
9) U_{55}/U_{11}.
10) $3Z/18Z$.
11) $11Z/55Z$.
12) S_3/A_3.
13) $4Z/16Z$.
14) $5Z/30Z$.
15) $3Z/12Z$.
16) U_{48}/U_{12}.
17) $D_4/\{0^\circ,180^\circ\}$.
18) $12Z/60Z$.
19) U_{20}/U_4.
20) $15Z/75Z$.
21) $Q_8/\{\pm 1\}$.
22) $4Z/24Z$.
23) U_{25}/U_5.
24) $6Z/30Z$.
25) $7Z/35Z$.
26) U_{30}/U_6.
27) $6Z/36Z$.
28) U_{15}/U_3.
29) $7Z/42Z$.
30) U_{18}/U_3.

1.2. Гомоморфізм груп

Нагадаємо, що відображення f групи $(G,*)$ в групу $(G',\circ)$ називається гомоморфним відображенням або гомоморфізмом групи G в групу G', якщо для довільних елементів $a,b \in G$ виконується умова $f(a*b) = f(a) \circ f(b)$.

Приклад 1.

1. Відображення $f(n) = (-1)^n$ є гомоморфізмом адитивної групи цілих чисел Z в групу за множенням $M = \{-1,1\}$.

2. Занумеруємо вершини правильного трикутника. Тоді підстановкам $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ природно відповідають повороти трикутника навколо центра на кути відповідно $0^\circ,120^\circ,240^\circ$, а підстановкам

$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$ – симетрії трикутника відносно осей, що проходять відповідно через вершини з номерами 1,2,3. Одержане відображення буде гомоморфізмом групи S_3 у групу симетрій правильного трикутника.

Властивості гомоморфізмів груп:

1. при всякому гомоморфізмі $f: G \to G'$ групи G в групу G' одиничний елемент групи G відображається в одиничний елемент групи G';
2. при гомоморфізмі $f: G \to G'$ довільна пара взаємно обернених елементів g і g^{-1} групи G відображається у пару взаємно обернених елементів g' і $(g')^{-1}$ елементів групи G';
3. образ $f(G)$ групи G при гомоморфізмі $f: G \to G'$ є підгрупою групи G'.

Приклад 2. Знайти всі гомоморфні відображення $Z_{25} \to Z_{70}$.

Нехай для гомоморфізму $\varphi: Z_{25} \to Z_{70}$, $\varphi(1) = k \in Z_{70}$. Цією умовою гомоморфізм φ визначається однозначно, бо для довільного $n \in Z_{25}$ маємо:

$$\varphi(n) = \varphi\left(\underbrace{1+1+\ldots 1}_{n}\right) = \varphi(1)+\varphi(1)+\ldots+\varphi(1) = \underbrace{k+k+\ldots+k}_{n} = nk.$$

Оскільки в групі Z_{25} $\underbrace{1+1+\ldots+1}_{25} = 0$, то в групі Z_{70} має бути $\underbrace{k+k+\ldots+k}_{25} = 25k = 0$, тобто $25k \vdots 70$, $5k \vdots 14$. Числа 14 і 5 взаємно прості, тому має бути $k \vdots 14$. Отже, k є одним з чисел $0,14,28,42,56$. Таким чином, маємо п’ять гомоморфних відображень $Z_{25} \to Z_{70}$:

$$\varphi(1) = 0,\ \varphi(1) = 14,\ \varphi(1) = 28,\ \varphi(1) = 42,\ \varphi(1) = 56.$$

Завдання 2. Знайти всі гомоморфні відображення групи Z_n в групу Z_m

1)	$Z_{15} \to Z_{25}$.	11)	$Z_{25} \to Z_{15}$.	21)	$Z_{55} \to Z_{65}$.
2)	$Z_{18} \to Z_{24}$.	12)	$Z_{24} \to Z_{42}$.	22)	$Z_{55} \to Z_{20}$.
3)	$Z_{15} \to Z_{10}$.	13)	$Z_{10} \to Z_{15}$.	23)	$Z_{12} \to Z_{28}$.
4)	$Z_{35} \to Z_{30}$.	14)	$Z_{36} \to Z_{20}$.	24)	$Z_{20} \to Z_{55}$.
5)	$Z_{42} \to Z_{36}$.	15)	$Z_{40} \to Z_{15}$.	25)	$Z_{44} \to Z_{32}$.
6)	$Z_{15} \to Z_{40}$.	16)	$Z_{30} \to Z_{35}$.	26)	$Z_{28} \to Z_{52}$.
7)	$Z_{20} \to Z_{35}$.	17)	$Z_{15} \to Z_{55}$.	27)	$Z_{42} \to Z_{24}$.
8)	$Z_{20} \to Z_{36}$.	18)	$Z_{30} \to Z_{65}$.	28)	$Z_{55} \to Z_{20}$.
9)	$Z_{42} \to Z_{30}$.	19)	$Z_{28} \to Z_{20}$.	29)	$Z_{65} \to Z_{30}$.
10)	$Z_{35} \to Z_{20}$.	20)	$Z_{32} \to Z_{44}$.	30)	$Z_{45} \to Z_{40}$.

1.3. Скінченні абелеві групи

Підгрупа H групи G називається нормальною підгрупою (або нормальним дільником) групи G, якщо для довільного елемента $g \in G$ виконується рівність $gH = Hg$. Факт, що H є нормальною підгрупою групи G, записують $H \lhd G$.

Приклад 1.

1. У симетричній групі S_n для будь–якої підстановки $g \in S_n$ кожен із класів суміжності gA_n і $A_n g$ збігається з множиною тих підстановок з S_n, які мають однакову парність із g. Тому знакозмінна група A_n буде нормальною підгрупою симетричної групи S_n.

2. У групі $GL_n(R)$ дійсних невироджених матриць порядку n розглянемо підгрупу унімодулярних матриць $H = \{A : \det A = 1\}$. Із теореми про визначник добутку двох матриць випливає, що кожен із класів суміжності AH і HA збігається з множиною тих матриць із $GL_n(R)$, визначник яких

дорівнює $\det A$. Тому підгрупа унімодулярних матриць є нормальною підгрупою групи дійсних невироджених матриць порядку n.

3. Довільна підгрупа абелевої групи буде нормальною підгрупою.
4. Оскільки циклічна група є абелевою, то довільна підгрупа циклічної групи буде нормальною підгрупою.

Група G називається **внутрішнім прямим добутком** (або просто **прямим добутком**) своїх підгруп $H_1,...,H_m$, якщо

1) всі підгрупи H_i нормальні в G;
2) довільний елемент g із групи G однозначно записується у вигляді добутку $g = h_1 \cdot h_2 \cdot \ldots \cdot h_m$, де $h_i \in H_i$.

Із однозначності розкладу $g = h_1 \cdot h_2 \cdot \ldots \cdot h_m$ випливає, що будь–які дві з підгруп $H_1,...,H_m$ перетинаються лише по одиниці e групи G.

Якщо група G є прямим добутком підгруп H_i, то кажуть також, що G **розкладається у прямий добуток** підгруп H_i, і записують $G = H_1 \times H_2 \times \ldots \times H_m$ або $G = \prod_{i=1}^{m} H_i$. Розклад, в якому всі множники є власними підгрупами, називається нетривіальним. Група, яка не має нетривіальних розкладів, називається **нерозкладною**.

Якщо дія в групі G записується адитивно, то говорять про **пряму суму підгруп** H_i. Записують $G = H_1 \oplus H_2 \oplus \ldots \oplus H_m$.

Приклад 2.

1. Група Z_{79} є нерозкладною, оскільки 79 просте число.
2. Група S_3 є нерозкладною, бо вона має лише одну власну нормальну підгрупу A_3.
3. Із правила додавання комплексних чисел, записаних в алгебраїчної формі:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2) i,$$

випливає, що адитивна група C комплексних чисел розкладається в пряму суму двох підгруп, кожна з яких ізоморфна адитивній групі R дійсних чисел.

Група порядку $p^n > 1$, де p – просте число, називається **примарною** групою.

Твердження 1. Кожна примарна циклічна група нерозкладна.

Твердження 2. Циклічна група C_n порядку $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$, де $p_1, p_2, \ldots, p_m$ різні прості числа, розкладається в прямий добуток m циклічних груп, що мають відповідно порядки $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, … , $p_m^{\alpha_m}$. Тобто $C_n \cong C_{p_1^{\alpha_1}} \times C_{p_2^{\alpha_2}} \times \ldots \times C_{p_m^{\alpha_m}}$

Приклад 3.

a) $Z_{170} = Z_{2 \cdot 5 \cdot 17} \cong Z_2 \oplus Z_5 \oplus Z_{17}$.

b) $Z_{125} = Z_{5^3}$ - нерозкладна.

c) $Z_{76500} = Z_{4 \cdot 9 \cdot 125 \cdot 17} \cong Z_4 \oplus Z_9 \oplus Z_{125} \oplus Z_{17}$.

d) $Z_{1080} = Z_{8 \cdot 27 \cdot 5} \cong Z_8 \oplus Z_{27} \oplus Z_5$.

e) $Z_{14112} = Z_{32 \cdot 9 \cdot 49} \cong Z_{32} \oplus Z_9 \oplus Z_{49}$.

Основна теорема про скінченні абелеві групи:

Кожна скінченна абелева група G розкладається в прямий добуток примарних циклічних груп. Цей розклад є однозначним із точністю до порядку слідування множників.

Якщо абелева група записується адитивно, то говорять про пряму суму примарних циклічних груп і про однозначність із точністю до порядку слідування доданків.

Приклад 4. Знайти з точністю до ізоморфізму всі абелеві групи порядку 720.

Знайдемо всі можливі розклади числа 720 у добуток степенів простих чисел:

$720 = 2\cdot 2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 5 = 4\cdot 2\cdot 2\cdot 3\cdot 3\cdot 5 = 4\cdot 4\cdot 3\cdot 3\cdot 5 = 2^3\cdot 2\cdot 3\cdot 3\cdot 5 = 2^4\cdot 3\cdot 3\cdot 5 =$
$= 2\cdot 2\cdot 2\cdot 2\cdot 9\cdot 5 = 4\cdot 2\cdot 2\cdot 9\cdot 5 = 4\cdot 4\cdot 9\cdot 5 = 2^3\cdot 2\cdot 9\cdot 5 = 2^4\cdot 9\cdot 5.$

Тому з точністю до ізоморфізму всі абелеві групи порядку 720 вичерпуються списком:

$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_5$, $Z_4 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_5$,

$Z_4 \oplus Z_4 \oplus Z_3 \oplus Z_3 \oplus Z_5$, $Z_8 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_5$, $Z_{16} \oplus Z_3 \oplus Z_3 \oplus Z_5$,

$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_9 \oplus Z_5$, $Z_4 \oplus Z_2 \oplus Z_2 \oplus Z_9 \oplus Z_5$, $Z_4 \oplus Z_4 \oplus Z_9 \oplus Z_5$,

$Z_8 \oplus Z_2 \oplus Z_9 \oplus Z_5$, $Z_{16} \oplus Z_9 \oplus Z_5$.

Приклад 5. З'ясувати, які з наступних груп ізоморфні?

a) $Z_{144} \oplus Z_{720}$.

b) $Z_{12} \oplus Z_{72} \oplus Z_{120}$.

c) $Z_{144^2} \oplus Z_5$.

d) $Z_9 \oplus Z_9 \oplus Z_{16} \oplus Z_{80}$.

e) $Z_{16} \oplus Z_{80} \oplus Z_{81}$.

f) $Z_{27} \oplus Z_{15} \oplus Z_{256}$.

g) $Z_{135} \oplus Z_{768}$.

Знайдемо розклад кожної групи в пряму суму примарних підгруп:

a) $Z_{144} \oplus Z_{720} \cong Z_{16} \oplus Z_9 \oplus Z_{16} \oplus Z_9 \oplus Z_5$.

b) $Z_{12} \oplus Z_{72} \oplus Z_{120} \cong Z_8 \oplus Z_3 \oplus Z_5 \oplus Z_4 \oplus Z_3 \oplus Z_8 \oplus Z_9$.

c) $Z_{144^2} \oplus Z_5 \cong Z_{2^8} \oplus Z_{81} \oplus Z_5$.

d) $Z_9 \oplus Z_9 \oplus Z_{16} \oplus Z_{80} \cong Z_{16} \oplus Z_5 \oplus Z_{16} \oplus Z_9 \oplus Z_9$.

e) $Z_{16} \oplus Z_{80} \oplus Z_{81} \cong Z_{16} \oplus Z_{16} \oplus Z_5 \oplus Z_{81}$.

f) $Z_{27} \oplus Z_{15} \oplus Z_{256} \cong Z_{27} \oplus Z_3 \oplus Z_5 \oplus Z_{256}$.

g) $Z_{135} \oplus Z_{768} \cong Z_5 \oplus Z_{27} \oplus Z_3 \oplus Z_{256}$.

Порівнюючи праві частини (з точністю до порядку слідування доданків), отримуємо: $a) \cong d)$, $f) \cong g)$, всі інші групи попарно неізоморфні.

Завдання 3. Використовуючи основну теорему про скінченні абелеві групи, знайти, з точністю до ізоморфізму, всі абелеві групи порядку:

1)	784.	7)	1080.	13)	144.	19)	504.	25)	1100.
2)	1960.	8)	1512.	14)	1620.	20)	400.	26)	4900.
3)	675.	9)	600.	15)	2268.	21)	392.	27)	1625.
4)	1370.	10)	1400.	16)	6125.	22)	11025.	28)	1375.
5)	4725.	11)	200.	17)	720.	23)	500.	29)	650.
6)	216.	12)	324.	18)	360.	24)	1500.	30)	1300.

Завдання 4. З'ясувати, які з наступних груп ізоморфні між собою?

1) $Z_{44} \oplus Z_{22} \oplus Z_5 \oplus Z_{51}$, $Z_{220} \oplus Z_{34} \oplus Z_{33}$, $Z_{120} \oplus Z_{121} \oplus Z_{17}$.

2) $Z_8 \oplus Z_{19} \oplus Z_{55}$, $Z_5 \oplus Z_{38} \oplus Z_{44}$, $Z_{40} \oplus Z_{209}$.

3) $Z_9 \oplus Z_{11} \oplus Z_{11} \oplus Z_{25}$, $Z_3 \oplus Z_{45} \oplus Z_{121}$, $Z_{99} \oplus Z_{275}$.

4) $Z_{24} \oplus Z_{25} \oplus Z_{26}$, $Z_8 \oplus Z_{13} \oplus Z_{150}$, $Z_{20} \oplus Z_{52} \oplus Z_{60}$.

5) $Z_{10} \oplus Z_{11} \oplus Z_{12}$, $Z_4 \oplus Z_{15} \oplus Z_{22}$, $Z_{24} \oplus Z_{55}$.

6) $Z_3 \oplus Z_{14} \oplus Z_{24} \oplus Z_{125}$, $Z_{144} \oplus Z_{875}$, $Z_8 \oplus Z_{42} \oplus Z_{375}$.

7) $Z_4 \oplus Z_5 \oplus Z_9$, $Z_2 \oplus Z_6 \oplus Z_{15}$, $Z_9 \oplus Z_{20}$.

8) $Z_{10} \oplus Z_{48}$, $Z_{16} \oplus Z_{30}$, $Z_{20} \oplus Z_{24}$.

9) $Z_{48} \oplus Z_{49} \oplus Z_{50}$, $Z_{16} \oplus Z_{150} \oplus Z_{491}$, $Z_{98} \oplus Z_{1200}$.

10) $Z_{14} \oplus Z_{15} \oplus Z_{16}$, $Z_2 \oplus Z_{21} \oplus Z_{80}$, $Z_{80} \oplus Z_{81}$.

11) $Z_4 \oplus Z_9 \oplus Z_{25}$, $Z_3 \oplus Z_{15} \oplus Z_{20}$, $Z_{25} \oplus Z_{36}$.

12) $Z_2 \oplus Z_5 \oplus Z_{18}$, $Z_9 \oplus Z_9 \oplus Z_{10}$, $Z_{12} \oplus Z_{15}$.

13) $Z_6 \oplus Z_{17} \oplus Z_{18}$, $Z_2 \oplus Z_{17} \oplus Z_{144}$, $Z_4 \oplus Z_{34} \oplus Z_{36}$.

14) $Z_{16} \oplus Z_{25} \oplus Z_{27}$, $Z_9 \oplus Z_{30} \oplus Z_{40}$, $Z_{27} \oplus Z_{400}$.

15) $Z_5 \oplus Z_6 \oplus Z_{49}$, $Z_3 \oplus Z_5 \oplus Z_{96}$, $Z_{14} \oplus Z_{105}$.

16) $Z_2 \oplus Z_5 \oplus Z_7 \oplus Z_9$, $Z_3 \oplus Z_{14} \oplus Z_{15}$, $Z_{18} \oplus Z_{35}$.

17) $Z_{26} \oplus Z_{27} \oplus Z_{28}$, $Z_{13} \oplus Z_{28} \oplus Z_{54}$, $Z_{13} \oplus Z_{24} \oplus Z_{63}$.

18) $Z_4 \oplus Z_6 \oplus Z_{10}$, $Z_2 \oplus Z_6 \oplus Z_{20}$, $Z_8 \oplus Z_{30}$.

19) $Z_5 \oplus Z_{12} \oplus Z_{21}$, $Z_3 \oplus Z_{15} \oplus Z_{28}$, $Z_{20} \oplus Z_{63}$.

20) $Z_5 \oplus Z_6 \oplus Z_{12}$, $Z_2 \oplus Z_{12} \oplus Z_{15}$, $Z_{10} \oplus Z_{36}$.

21) $Z_{11} \oplus Z_{13} \oplus Z_{35} \oplus Z_{113}$, $Z_{35} \oplus Z_{55} \oplus Z_{791}$, $Z_{14} \oplus Z_{339}$.

22) $Z_2 \oplus Z_3 \oplus Z_4 \oplus Z_{30}$, $Z_2 \oplus Z_{15} \oplus Z_{24}$, $Z_{18} \oplus Z_{40}$.

23) $Z_5 \oplus Z_{15} \oplus Z_{40}$, $Z_8 \oplus Z_9 \oplus Z_{125}$, $Z_{25} \oplus Z_{120}$.

24) $Z_3 \oplus Z_4 \oplus Z_{15}$, $Z_{12} \oplus Z_{15}$, $Z_3 \oplus Z_{64}$.

25) $Z_5 \oplus Z_{15} \oplus Z_{512}$, $Z_{10} \oplus Z_{30} \oplus Z_{128}$, $Z_{25} \oplus Z_{1536}$.

26) $Z_5 \oplus Z_{24} \oplus Z_{42}$, $Z_6 \oplus Z_{15} \oplus Z_{56}$, $Z_{48} \oplus Z_{105}$.

27) $Z_2 \oplus Z_{18} \oplus Z_{40}$, $Z_5 \oplus Z_9 \oplus Z_{32}$, $Z_{24} \oplus Z_{60}$.

28) $Z_5 \oplus Z_6 \oplus Z_7 \oplus Z_{11}$, $Z_7 \oplus Z_{15} \oplus Z_{22}$, $Z_8 \oplus Z_{35}$.

29) $Z_3 \oplus Z_7 \oplus Z_{11} \oplus Z_{25}$, $Z_5 \oplus Z_{33} \oplus Z_{35}$, $Z_{33} \oplus Z_{175}$.

30) $Z_{11} \oplus Z_{135} \oplus Z_{147}$, $Z_{49} \oplus Z_{55} \oplus Z_{81}$, $Z_{297} \oplus Z_{735}$.

1.4. Фактор–група вільної абелевої групи

Вільною абелевою групою рангу n називається група $\underbrace{Z \oplus Z \oplus \ldots \oplus Z}_{n \text{ доданків}}$.

Нехай $G = Z \oplus Z \oplus \ldots \oplus Z$ – вільна абелева група рангу n, H – підгрупа групи G, $y_1 = (a_{11}, a_{12}, \ldots, a_{1n})$, $y_2 = (a_{21}, a_{22}, \ldots, a_{2n})$, … , $y_k = (a_{k1}, a_{k2}, \ldots, a_{kn})$ – система твірних підгрупи H. Щоб розкласти

фактор–групу G/H у пряму суму циклічних груп, виписують спочатку цілочисельну матрицю

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{k1} & a_{k2} & \dots & a_{kn} \end{pmatrix}.$$

Далі зводять цю матрицю до діагонального вигляду. З рядками або стовпчиками можна робити такі перетворення:

1) рядки (стовпчики) можна переставляти місцями;
2) до рядка (стовпчика) можна додавати інший рядок (стовпчик) помножений

на довільне **ціле** число;

3) можна міняти знак всіх елементів одного рядка (стовпчика) на протилежний.

Нехай цілочисельна матриця вказаними перетвореннями зведена до діагонального вигляду

$$\begin{pmatrix} \alpha_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha_m & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

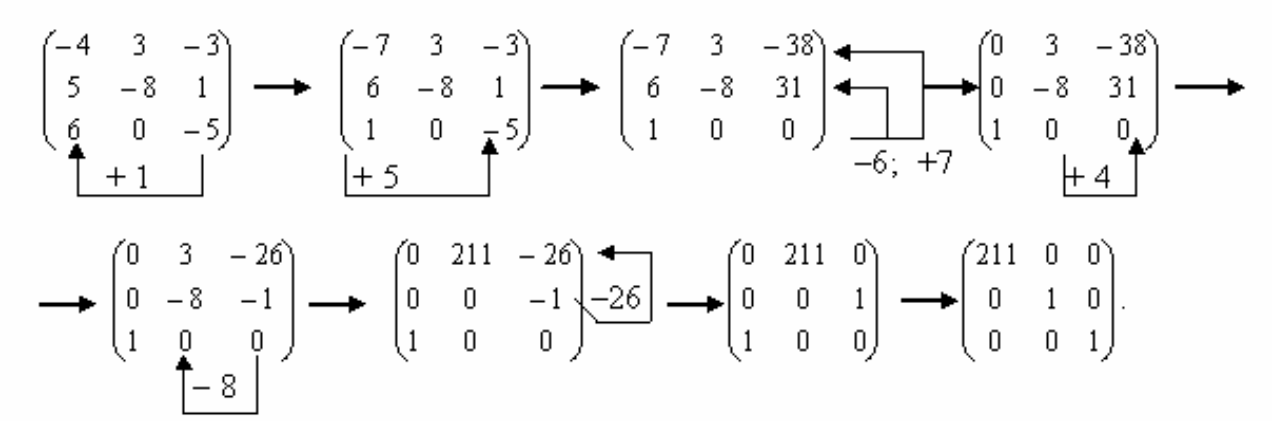
Тоді розклад фактор–групи G/H у пряму суму циклічних груп буде мати такий вигляд:

$$G/H \cong Z_{\alpha_1} \oplus Z_{\alpha_2} \oplus \dots \oplus Z_{\alpha_m} \oplus \underbrace{Z \oplus Z \oplus \dots \oplus Z}_{n-m}.$$

Зауваження. Якщо для якогось i $\alpha_i = 1$, то $Z_{\alpha_i} \cong 0$, а нульовий доданок можна опустити.

Приклад 1. Розкласти в пряму суму циклічних груп фактор–групу A/B, де $A-$ вільна абелева група рангу 3, а підгрупа B породжується елементами $y_1 = -4x_1 + 3x_2 - 3x_3$, $y_2 = 5x_1 - 8x_2 + x_3$, $y_3 = 6x_1 - 5x_3$, де $x_1 = (1,0,0)$, $x_2 = (0,1,0)$, $x_3 = (0,0,1)$.

Випишемо цілочисельну матрицю коефіцієнтів $\begin{pmatrix} -4 & 3 & -3 \\ 5 & -8 & 1 \\ 6 & 0 & -5 \end{pmatrix}$. Зведемо її до діагонального вигляду (тобто ненульові елементи можуть стояти лише на головній діагоналі).

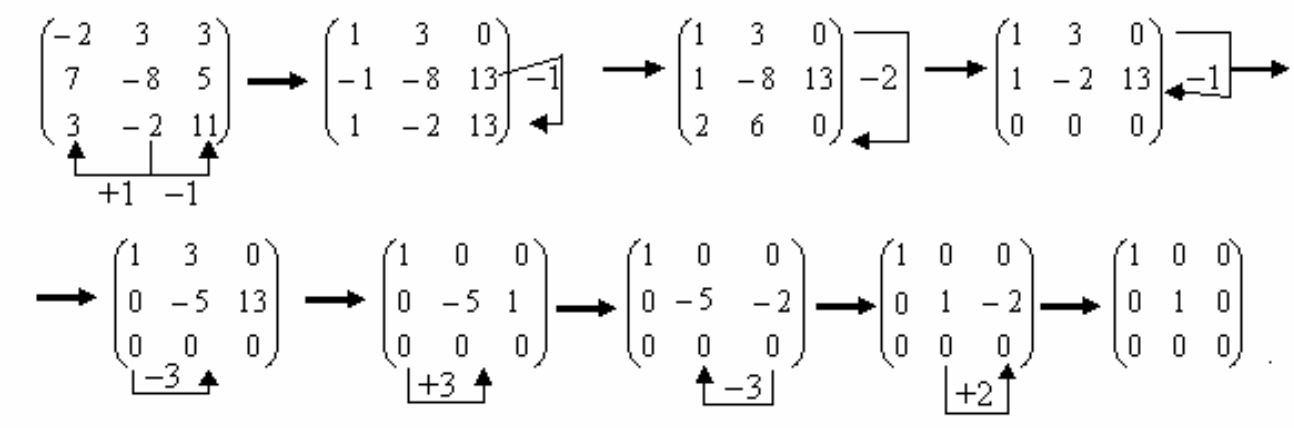


Останнім перетворенням буде перестановка стовпчиків. Отже, шуканий розклад фактор–групи має вигляд:

$$A/B = Z/\langle 211\rangle \oplus Z/\langle 1\rangle \oplus Z/\langle 1\rangle \cong Z_{211} \oplus 0 \oplus 0 \cong Z_{211}.$$

Приклад 2. Розкласти в пряму суму циклічних груп фактор–групу A/B, де $A-$ вільна абелева група рангу 3, а підгрупа B породжується елементами $y_1 = -2x_1 + 3x_2 + 3x_3$, $y_2 = 7x_1 - 8x_2 + 5x_3$, $y_3 = 2y_1 + y_2$, де $x_1 = (1,0,0)$, $x_2 = (0,1,0)$, $x_3 = (0,0,1)$.

Знову зведемо цілочисельну матрицю коефіцієнтів до діагонального вигляду:



Отже, $A/B = Z/\langle 1\rangle \oplus Z/\langle 1\rangle \oplus Z/\langle 0\rangle \cong 0 \oplus 0 \oplus Z \cong Z$.

Завдання 5. Розкласти в пряму суму циклічних груп фактор – групу A/B, де A – вільна абелева група рангу 3, а підгрупа B породжується елементами y_1, y_2, y_3,

де $x_1 = (1,0,0)$, $x_2 = (0,1,0)$, $x_3 = (0,0,1)$

1. $y_1 = 7x_1 + 2x_2 + 3x_3,\ y_2 = 2x_1 + 8x_2 + 9x_3,\ y_3 = 5x_1 + 4x_2 - 3x_3$.
2. $y_1 = 5x_1 - 5x_2 + 2x_3,\ y_2 = 11x_1 + 8x_2 - 5x_3,\ y_3 = 7x_1 + 5x_2 + 8x_3$.
3. $y_1 = -4x_1 + 5x_2 - x_3,\ y_2 = 8x_1 + 9x_2 + x_3,\ y_3 = 4x_1 + 6x_2 - 2x_3$.
4. $y_1 = 5x_1 + 5x_2 + 4x_3,\ y_2 = -7x_1 + 6x_2 + 9x_3,\ y_3 = 5x_1 + 4x_2 - 4x_3$.
5. $y_1 = 5x_1 - 5x_2 + 3x_3,\ y_2 = 5x_1 + 6x_2 - 5x_3,\ y_3 = 8x_1 + 7x_2 + 9x_3$.
6. $y_1 = 6x_1 + 5x_2 + 7_3,\ y_2 = 8x_1 + 7x_2 + 2x_3,\ y_3 = 6x_1 + 5x_2 - x_3$.
7. $y_1 = 2x_1 + 6x_2 - 2x_3,\ y_2 = -2x_1 + 8x_2 + 4x_3,\ y_3 = 4x_1 + 11x_2 - 4x_3$.
8. $y_1 = 4x_1 + 7x_2 + 3x_3,\ y_2 = 2x_1 - 3x_2 + 2x_3,\ y_3 = 6x_1 + 10x_2 - 5x_3$.
9. $y_1 = 2x_1 + 3x_2 + 4x_3,\ y_2 = -5x_1 + 3x_2 + 6x_3,\ y_3 = 2x_1 - 6x_2 + 9x_3$.
10. $y_1 = 3x_1 + 2x_2 + 7x_3,\ y_2 = 9x_1 + 8x_2 + 21x_3,\ y_3 = 3x_1 - 4x_2 + 5x_3$.
11. $y_1 = 5x_1 + 3x_2 + 5x_3,\ y_2 = 6x_1 + 5x_2 + 5x_3,\ y_3 = 7x_1 + 9x_2 + 8x_3$.

12. $y_1 = 8x_1 + 11x_2 + 7x_3,\ y_2 = 6x_1 + 11x_2 + 5x_3,\ y_3 = 6x_1 + 7x_2 + 5x_3.$

13. $y_1 = 2x_1 + 3x_2 - 3x_3,\ y_2 = 3x_1 + 8x_2 - 2x_3,\ y_3 = 5x_1 - 4x_2 + 3x_3.$

14. $y_1 = x_1 - 2x_2 + 3x_3,\ y_2 = 2x_1 + 8x_2 + 9x_3,\ y_3 = 5x_1 + 4x_2 - 3x_3.$

15. $y_1 = 3x_1 - 2x_2 - 3x_3,\ y_2 = x_1 + 4x_2 + 3x_3,\ y_3 = 2x_1 + 4x_2 - 3x_3.$

16. $y_1 = 6x_1 + x_2 + 2x_3,\ y_2 = 5x_1 - 8x_2,\ y_3 = 5x_1 + 4x_2 - 3x_3.$

17. $y_1 = 7x_1 + 2x_2 + 3x_3,\ y_2 = 21x_1 + 6x_2 + 9x_3,\ y_3 = 5x_1 - 4x_2 + 3x_3.$

18. $y_1 = 5x_1 - 3x_2 + 3x_3,\ y_2 = 8x_1 + 8x_2 + 9x_3,\ y_3 = 5x_1 - 4x_2 - 3x_3.$

19. $y_1 = x_1 + 2x_2 + x_3,\ y_2 = 2x_1 + 8x_2 + x_3,\ y_3 = 3x_1 + 4x_2 + x_3.$

20. $y_1 = 5x_1 - x_2 + 2x_3,\ y_2 = 8x_1 + 9x_2 + x_3,\ y_3 = 3x_1 - 4x_2 + 9x_3.$

21. $y_1 = 10x_1 - 8x_2 + 6x_3,\ y_2 = 2x_1 + 3x_2 + 6x_3,\ y_3 = 5x_1 - 4x_2 + 3x_3.$

22. $y_1 = x_1 + 4x_2 + x_3,\ y_2 = 3x_1 + 8x_2 + x_3,\ y_3 = 5x_1 + 3x_2 + 3x_3.$

23. $y_1 = 3x_1 + 2x_2 + 5x_3,\ y_2 = 11x_1 + 7x_2 - 4x_3,\ y_3 = 5x_1 + 5x_2 + 3x_3.$

24. $y_1 = -2x_1 - 3x_2 + x_3,\ y_2 = 9x_1 - 8x_2 + 9x_3,\ y_3 = 2x_1 + 3x_2 - 3x_3.$

25. $y_1 = 2x_1 - x_2 + 4x_3,\ y_2 = 10x_1 + 3x_2 + x_3,\ y_3 = 5x_1 - 5x_2 + x_3.$

26. $y_1 = 23x_1 + 2x_2 + 7x_3,\ y_2 = 7x_1 + 3x_2 + x_3,\ y_3 = 3x_1 - 3x_2 + 5x_3.$

27. $y_1 = 12x_1 + 8x_2 + 9x_3,\ y_2 = 21x_1 + 9x_2 + 7x_3,\ y_3 = x_1 - 4x_2 + 13x_3.$

28. $y_1 = 7x_1 + 11x_2 + 2x_3,\ y_2 = 13x_1 + 8x_2 + 3x_3,\ y_3 = 6x_1 - 2x_2 + 5x_3.$

29. $y_1 = 9x_1 + 12x_2 - 6x_3,\ y_2 = x_1 + x_2 + 5x_3,\ y_3 = 2x_1 - 3x_2 + 4x_3.$

30. $y_1 = x_1 + 3x_2 - 5x_3,\ y_2 = 2y_1,\ y_3 = -3y_1.$

Завдання 6

1. Знайти всі ізоморфізми між групами $(Z_{12}, +)$ і $(Z_{13}^*, \cdot)$.
2. Нехай в абелевій групі G є елементи порядків 30 і 45. Довести, що в групі G є елемент порядку 90.
3. Нехай G - скінченно породжена абелева група, H – підгрупа групи G. Довести, що H – скінченно породжена.

4. Довести, що скінченна підгрупа мультиплікативної групи P^* поля P є циклічною.
5. Нехай G - скінченна абелева група. Довести, що G циклічна тоді й лише тоді, коли кожна примарна компонента групи G є циклічною.
6. Знайти комутант групи кватерніонів Q_8.
7. Нехай G – група, H_1, H_2 – нормальні підгрупи групи G, $H_1 \cap H_2 = e$. Довести, що $xy = yx$ для довільних елементів $x \in H_1$, $y \in H_2$.
8. Знайти всі ізоморфізми між групами $(Z_{10}, +)$ і $(Z_{11}^*, \cdot)$.
9. Нехай G, G' – групи, φ – гомоморфне відображення G в G', за яким $a \to a'$. Довести, що порядок елемента a ділиться на порядок елемента a'.
10. Нехай в абелевій групі G є елементи порядків 35 і 42. Довести, що в групі G є елемент порядку 210.
11. Довести, що в групі Q/Z кожен елемент має скінченний порядок.
12. Довести, що кожна група порядку p^2, де p – просте число, є комутативною.
13. Нехай в абелевій групі G є елементи порядків 30 і 70. Довести, що в групі G є елемент порядку 210.
14. Чи може група G містити більше ніж одну підгрупу індексу 2?
15. Нехай A, B – скінченні абелеві групи, $A \oplus A \cong B \oplus B$. Довести, що $A \cong B$.
16. Нехай G – скінчено породжена абелева група. Довести, що довільний гомоморфізм групи G на себе є автоморфізмом.
17. Нехай A, B, C – скінченні абелеві групи, $A \oplus C \cong B \oplus C$. Довести, що $A \cong B$.
18. Нехай G, G_1 – групи, φ – гомоморфне відображення G на G_1. Довести, що порядок групи G ділиться на порядок групи G_1.
19. Довести, що комутант G' групи G є нормальною підгрупою групи G.

20. Довести, що в групі Q/Z для кожного натурального n існує єдина підгрупа порядку n.
21. Довести, що в групі C^* кожна скінченна підгрупа є циклічною.
22. Знайти всі ізоморфізми між групами $(Z_4,+)$ і $(Z_5^*,\cdot)$.
23. Довести, що в мультиплікативній групі P^* поля P для кожного натурального n існує не більше одної підгрупи порядку n.
24. Нехай $G-$ група, $G'-$ комутант групи G. Довести, що фактор–група G/G' комутативна.
25. Нехай в абелевій групі G є елементи порядків 20 і 25. Довести, що в групі G є елемент порядку 100.
26. Знайти комутант групи D_4.
27. Знайти всі ізоморфізми між групами $(Z_6,+)$ і $(Z_7^*,\cdot)$.
28. Нехай $A-$ скінченна абелева група, порядок якої вільний від квадратів (тобто не ділиться на квадрат жодного цілого числа, більшого за 1). Довести, що група A циклічна.
29. Нехай в абелевій групі G є елементи порядків 20 і 15. Довести, що в групі G є елемент порядку 60.
30. Знайти комутант групи A_4.

1.5. Гомоморфізми кілець

Відображення $f: K \to K'$ кільця K в кільце K' будемо називати **гомоморфізмом,** якщо для довільних двох елементів $a,b \in K$ виконуються дві умови: $f(a+b) = f(a) + f(b)$, $f(a \cdot b) = f(a) \cdot f(b)$.

Приклад 1. З'ясувати, чи буде відображення $f: k \to 2k$ кільця $12Z$ в кільце $24Z$ гомоморфізмом.

Маємо $f(12) = 2 \cdot 12 = 24$ і $f(144) = 2 \cdot 144 = 288$. З іншого боку, $144 = 12 \cdot 12$. Але $f(144) = 288 \neq 24 \cdot 24 = f(12) \cdot f(12)$. Отже, відображення не є гомоморфізмом.

Приклад 2. Знайти всі гомоморфізми кілець 1) $f : 6Z \to 3Z$,

2) $f : 6Z \to 6Z$.

1. Нехай $f(6) = 3k$. Довільний елемент кільця $6Z$ має вигляд $6n$, де $n \in Z$, тому має бути

$$f(6n) = f(\underbrace{6 + 6 + \ldots + 6}_{n}) = \underbrace{f(6) + f(6) + \ldots + f(6)}_{n} = 3kn.$$

З'ясуємо, яким може бути k. Розглянемо елемент $36 \in 6Z$. Позаяк $36 = 6 \cdot 6$, то

$$f(36) = f(6 \cdot 6) = f(6) \cdot f(6) = 3k \cdot 3k = 3^2 k^2.$$

З іншого боку, $f(36) = f(\underbrace{6 + \ldots + 6}_{6}) = \underbrace{f(6) + \ldots + f(6)}_{6} = 6 \cdot 3k$.

Якщо f гомоморфізм, то має бути $9k^2 = 18k$, $9k(k-2) = 0$, звідки випливає, що $k = 0$ або $k = 2$. Таким чином, маємо два відображення: $f_1(6n) = 0$ і $f_2(6n) = 6n$. Легко перевірити, що кожне з них є гомоморфізмом.

2. Нехай $f(6) = 6k$. Довільний елемент кільця $6Z$ має вигляд $6n$, де $n \in Z$, тому має бути

$$f(6n) = f(\underbrace{6 + 6 + \ldots + 6}_{n}) = \underbrace{f(6) + f(6) + \ldots + f(6)}_{n} = 6kn.$$

Як і в попередньому випадку, з'ясуємо, яким може бути k. Розглянемо елемент $36 \in 6Z$. Оскільки, $36 = 6 \cdot 6$, то

$$f(36) = f(6 \cdot 6) = f(6) \cdot f(6) = 6k \cdot 6k = 6^2 k^2.$$

З іншого боку, $f(36) = f(\underbrace{6 + \ldots + 6}_{6}) = \underbrace{f(6) + \ldots + f(6)}_{6} = 6 \cdot 6k$.

Якщо f гомоморфізм, то має бути $36k^2 = 36k$, $36k(k-1) = 0$, звідки випливає, що $k = 0$, або $k = 1$. Таким чином, маємо два відображення: $f_1(6n) = 0$ і $f_2(6n) = 6n$, ці відображення гомоморфні.

Завдання 7. Знайти всі гомоморфізми кілець :

1) $f : Z \to 3Z$.
2) $f : 5Z \to 7Z$.
3) $f : 10Z \to 5Z$.
4) $f : 4Z \to 3Z$.
5) $f : 5Z \to 2Z$.
6) $f : 6Z \to 9Z$.
7) $f : Z \to 2Z$.
8) $f : 5Z \to 3Z$.
9) $f : 12Z \to 6Z$.
10) $f : 3Z \to 4Z$.
11) $f : 5Z \to 10Z$.
12) $f : 2Z \to 8Z$.
13) $f : 7Z \to 6Z$.
14) $f : 2Z \to 4Z$.
15) $f : 6Z \to 5Z$.
16) $f : 3Z \to 6Z$.
17) $f : 9Z \to 6Z$.
18) $f : 7Z \to 5Z$.
19) $f : 2Z \to Z$.
20) $f : 6Z \to 12Z$.
21) $f : 3Z \to 2Z$.
22) $f : 10Z \to 15Z$.
23) $f : 2Z \to 6Z$.
24) $f : 3Z \to Z$.
25) $f : 6Z \to 2Z$.
26) $f : 2Z \to 5Z$.
27) $f : 2Z \to 12Z$.
28) $f : 2Z \to 7Z$.
29) $f : 3Z \to 12Z$.
30) $f : 2Z \to 3Z$.

1.6. Ідеал кільця. Модулі

Непорожня підмножина J кільця K називається **ідеалом** цього кільця, якщо:

1) J є підгрупою адитивної групи кільця K;
2) для довільних $a \in J$ і $x \in K$ кожен із елементів ax і xa належить J.

У кожному кільці є два тривіальні ідеали: саме кільце K (одиничний ідеал) та ідеал, що складається з одного елемента 0 (нульовий ідеал).

Ідеал комутативного кільця K, який складається з елементів вигляду $xa + na$, де елемент $a \in K -$ фіксований, а елементи $x \in K$ і $n \in N -$ довільні, називається **головним ідеалом** , що породжується елементом a, і позначається (a).

Приклад 1. Вказати всі ідеали кільця Z_{70}.

Оскільки адитивна група кільця Z_{70} циклічна і $70 = 2 \cdot 5 \cdot 7$, то можна виписати список усіх підгруп адитивної групи : $\langle 1 \rangle = Z_{70}$, $\langle 2 \rangle$, $\langle 5 \rangle$, $\langle 7 \rangle$, $\langle 10 \rangle$, $\langle 14 \rangle$, $\langle 35 \rangle$, $\langle 0 \rangle$. Легко перевіряється, що кожна з цих підгруп задовольняє також другій умові означення, отже, є ідеалом. Зауважимо, що всі ці ідеали є головними.

Приклад 2. Знайти всі ідеали кільця Z_{120} і з'ясувати, чи утворюють ідеал необоротні елементи цього кільця?

Оскільки $120 = 2^3 \cdot 3 \cdot 5$, то ідеали

$(\bar{0})$, Z_{120}, (60), (40), (30), (24), (20), (15), (12), (10), (8), (6), (4), (5), (2), (3).

Необоротні елементи: 0, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, … ідеал не утворюють, оскільки множина необоротних елементів M не є підгрупою адитивної групи: $2 + 5 = 7 \notin M$.

Приклад 3. Чи утворюють ідеал необоротні елементи кільця 1) Z_{64};

2) Z_{173}.

1. Оскільки $n = 64 = 2^6$, то необоротними елементами будуть всі парні числа:

0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, …, 62.

Оскільки сума парних чисел і довільне кратне парного числа знову є парними числами, то необоротні елементи утворюють ідеал.

2. Число 173 – просте, тому в Z_{173} буде лише один необоротний елемент – 0. Очевидно, що він утворює нульовий ідеал.

Завдання 8. Чи утворюють ідеал необоротні елементи кільця Z_n? Знайти всі ідеали кільця Z_m

1)	$n=169; m=30$.	11)	$n=625; m=70$.	21)	$n=128; m=44$.
2)	$n=225; m=50$.	12)	$n=100; m=25$.	22)	$n=385; m=125$.
3)	$n=168; m=35$.	13)	$n=145; m=75$.	23)	$n=140; m=48$.
4)	$n=191; m=32$.	14)	$n=156; m=144$.	24)	$n=125; m=81$.
5)	$n=264; m=45$.	15)	$n=224; m=169$.	25)	$n=243; m=75$.
6)	$n=512; m=24$.	16)	$n=369; m=27$.	26)	$n=196; m=130$.
7)	$n=192; m=42$.	17)	$n=144; m=40$.	27)	$n=124; m=128$.
8)	$n=160; m=20$.	18)	$n=121; m=49$.	28)	$n=200; m=343$.
9)	$n=125; m=28$.	19)	$n=145; m=38$.	29)	$n=159; m=54$.
10)	$n=105; m=63$.	20)	$n=164; m=36$.	30)	$n=158; m=121$.

1.7. Фактор–кільце

Нехай K – кільце, J – ідеал цього кільця. Оскільки J є підгрупою адитивної абелевої групи K, то розглянемо фактор–групу $K/J = \{0+J, a+J, b+J, ...\}$ адитивної абелевої групи за нормальним дільником J. У групі K/J визначимо також множення за правилом:

$$(a+J)\cdot(b+J) = (ab)+J .$$

Тоді адитивна фактор–група K/J перетворюється в кільце, яке називають **фактор–кільцем** кільця K за ідеалом J і також позначають K/J.

Приклад 1. Фактор–кільце K/K є нульовим ідеалом, а фактор–кільце $K/(0)$ ізоморфне кільцю K.

Приклад 2. Скласти таблички додавання і множення для фактор–кільця $Z/_{5Z} = \{0+5Z, 1+5Z, 2+5Z, 3+5Z, 4+5Z\}$.

Введемо позначення:

$$\bar{0} = 0+5Z,\ \bar{1} = 1+5Z,\ \bar{2} = 2+5Z,\ \bar{3} = 3+5Z,\ \bar{4} = 4+5Z.$$

Тоді таблиці Келі відносно додавання і відносно множення будуть мати такий вигляд:

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

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Зауважимо, що це кільце буде полем, оскільки воно комутативне і для кожного ненульового елемента існує обернений.

Приклад 3. Скласти таблички додавання і множення для фактор–кільця $Z_2[x]/(x^2+1)$.

Зауважимо, що многочлен x^2+1 є розкладним над $Z_2[x]$: $x^2+1=(x+1)^2$. Знайдемо класи лишків. При діленні на многочлен другого степеня в остачі може бути лише многочлен степеня, меншого за 2, тобто вигляду $ax+b$, де $a,b \in Z_2$. Введемо позначення: $J=(x^2+1)$. Тоді фактор–кільце буде містити таки 4 елементи: $\bar{0} = J$, $\bar{1} = 1+J$, $\bar{x} = x+J$, $\overline{x+1} = x+1+J$.

Таблиці Келі відносно додавання і відносно множення будуть мати такий вигляд:

$+$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\bar{1}$	$\overline{x+1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\overline{x+1}$	$\bar{0}$

Зауважимо, що це фактор–кільце не є полем (є дільники нуля).

Приклад 4. З'ясувати, чи ізоморфні фактор–кільця $Z_3[x]/(x^2+1)$, $Z_2[x]/(x^2+1)$ і $Z_3[x]/(x^2+2)$.

Зауважимо, що многочлен x^2+1 є незвідним над $Z_3[x]$, але є розкладним над $Z_2[x]$: $x^2+1=(x+1)^2$. Многочлен x^2+2 є звідним над $Z_3[x]$: $x^2+2=(x+1)(x+2)$. Таким чином, фактор–кільце $Z_3[x]/(x^2+1)$ є полем, а фактор-кільце $Z_3[x]/(x^2+2)$ не утворює поле. Отже ці фактор-кільця неізоморфні. Фактор–кільце $Z_2[x]/(x^2+1)$ не може бути ізоморфне жодному з двох інших оскільки воно має порядок 4, а інші фактор-кільця містять по 9 елементів.

Нехай K – асоціативне кільце з одиницею 1 та V – деяка адитивна абелева група. Розглянемо відображення декартового добутку $K\times V$ в групу V. Образ пари (x,u) при цьому відображенні будемо позначати xu. Якщо при відображені для всіх елементів $x,y\in K$ та довільних $u,v\in V$ виконуються умови:

(M1) $x(u+v)=xu+xv$,

(M2) $(x+y)v=xv+yv$,

(M3) $(xy)v=x(yv)$,

(M4) $1\cdot v=v$

то група V називається **лівим K-модулем**, або **лівим модулем над кільцем** K.

Зауважимо, що символ "+" у лівій та правій частинах умови (М2) має різний сенс, а саме: зліва – це сума елементів кільця K, а справа – сума елементів групи V.

Аналогічно визначається правий K-модуль, коли елементи групи множаться на елементи кільця справа. Модуль M, який одночасно є правим та лівим K-модулем, називають **двостороннім**, або **K-модулем**.

Зауважимо, що довільну абелеву групу A можна розглядати як модуль над кільцем цілих чисел Z. Справді, для довільного цілого числа $n \in Z$ та довільного елемента групи $u \in V$ добутки nu та un можна визначити як кратні елемента u: $nu = u + u + ... + u = un$.

Легко перевіряється, що довільний ідеал J кільця K є лівим (правим) модулем над кільцем K, а лінійний простір L над полем P є модулем над полем P.

Якщо M – лівий K-модуль, то для довільних елементів $a, b \in M$ та довільних $r, s \in K$ мають місце наступні рівності:

$$r0 = 0a = 0,\ (-r)a = r(-a) = -ra,\ (r-s)a = ra - sa,\ r(a-b) = ra - rb.$$

Підмножина H лівого модуля M над кільцем K називається підмодулем, якщо $H < M$ та H є лівим K-модулем. Перетин довільної множини підмодулів модуля M також є підмодулем.

Завдання 9. Скласти таблички додавання і множення для фактор–кільця K/J. З'ясувати, чи буде це кільце полем?

1) $K = Z_2[x],\ J = (x^2 + x + 1)$.

2) $K = Z_3[x],\ J = (x^2 + 1)$.

3) $K = Z_2[x],\ J = (x^2 + x)$.

4) $K = Z_2[x],\ J = (x^3 + 1)$.

16) $K = Z_3[x],\ J = (x^2 + x + 1)$.

17) $K = Z_3[x],\ J = (x^2 + x)$.

18) $K = Z_3[x],\ J = (2x^2)$.

19) $K = Z_3[x],\ J = (x^2 + 2x + 1)$.

5) $K = Z_2[x],\ J = (x^2)$.

6) $K = Z_2[x],\ J = (x^3 + x^2 + x + 1)$.

7) $K = Z_3[x],\ J = (2x^2 + 2x)$.

8) $K = Z_2[x],\ J = (x^3 + x^2 + x)$.

9) $K = Z_3[x],\ J = (x^2 + 2)$.

10) $K = Z_2[x],\ J = (x^3 + x^2 + 1)$.

11) $K = Z_3[x],\ J = (x^2)$.

12) $K = Z_2[x],\ J = (x^2 + x + 1)$.

13) $K = Z_3[x],\ J = (2x^2 + x + 2)$

14) $K = Z_3[x],\ J = (2x^2 + 2x + 1)$.

15) $K = Z_3[x],\ J = (x^2 + 2x)$.

20) $K = Z_3[x],\ J = (x^2 + x + 2)$.

21) $K = Z_3[x],\ J = (2x^2 + x + 1)$.

22) $K = Z_3[x],\ J = (2x^2 + 2x + 2)$.

23) $K = Z_3[x],\ J = (x^2 + 2x + 2)$.

24) $K = Z_2[x],\ J = (x^3 + x + 1)$.

25) $K = Z_2[x],\ J = (x^3 + x^2)$.

26) $K = Z_3[x],\ J = (2x^2 + 2)$.

27) $K = Z_2[x],\ J = (x^3)$.

28) $K = Z_3[x],\ J = (2x^2 + 1)$.

29) $K = Z_3[x],\ J = (2x^2 + x + 1)$.

30) $K = Z_2[x],\ J = (x^2 + 1)$.

Завдання 10

1. Довести, що при гомоморфізмі образ комутативного кільця є комутативним кільцем.
2. Нехай J – ідеал кільця K. Довести, що коли J містить оборотний елемент, то $J = K$.
3. З'ясувати, чи ізоморфні фактор–кільця $Z[x]/(x^2 - 2)$ і $Z[x]/(x^2 - 3)$?
4. Довести, що кільце цілих чисел Z не містить мінімальних ідеалів.
5. Нехай I, J – максимальні ліві ідеали кільця R. Довести, що $I = J$ або $I + J = R$.
6. Нехай R – комутативне кільце з одиницею. Довести, що коли R не має інших ідеалів, крім одиничного та нульового, то R є полем.
7. Для яких a, b, c фактор–кільце $Z_2[x]/(x^3 + ax^2 + bx + c)$ є полем?
8. Довести, що кільця Z_{mn} і $Z_m \oplus Z_n$ ізоморфні тоді й лише тоді, коли числа m та n взаємно прості.

9. Нехай R – комутативне кільце з одиницею, J – ідеал кільця R. Довести, що фактор–кільце R/J є полем тоді й лише тоді, коли J – максимальний ідеал кільця R.
10. Нехай F – поле, $a \in F$. Довести, що $F[x]/(x-a) \cong F$.
11. Довести, що фактор–кільце $Z[i]/(2)$ не є полем.
12. Довести, що для довільного цілого $n>1$ фактор–кільце $Z[x]/(n)$ є ізоморфним кільцю $Z_n[x]$.
13. З'ясувати, чи ізоморфні фактор–кільця $Z_3[x]/(x^3+1)$ і $Z_3[x]/(x^3+2x^2+x+1)$.
14. Нехай R – кільце з одиницею, J – ідеал кільця R. Довести, що фактор–кільце R/J також має одиницю.
15. Нехай R – кільце з одиницею e, J_1, J_2 – двосторонні ідеали кільця R. Нехай $R = J_1 \oplus J_2$, $e = e_1 + e_2$, $e_1 \in J_1$, $e_2 \in J_2$. Довести, що e_1, e_2 – одиниці кілець J_1, J_2.
16. Довести, що фактор–кільце $Z[i]/(3)$ є полем з дев'яти елементів.
17. Для яких a, b фактор–кільця $Z_2[x]/(x^2+ax+b)$ ізоморфні між собою?
18. Довести, що кільце лишків Z_n, де $n = p_1 p_2 \dots p_m$, де $p_1, p_2, \dots, p_m$ – різні прості числа, є прямою сумою полів.
19. Довести, що для кожного кільця R існує таке кільце з одиницею R', що R є ізоморфним підкільцю кільця R'.
20. Довести, що кожен многочлен з коефіцієнтами з поля P має корінь у деякому розширенні $L \supset P$.
21. Для яких a, b фактор–кільце $Z_3[x]/(x^2+ax+b)$ є полем?

22. Нехай P – поле, R – кільце. Довести, що довільний гомоморфізм поля в кільце є або нульовим, або ізоморфним відображенням на деяке підполе поля кільця R.
23. Нехай P – поле. Довести, що для довільного многочлена з кільця $P[x]$ існує поле розкладу цього многочлена.
24. Нехай R – поле дійсних чисел. Довести, що $R[x]/(x^2+1) \cong C$.
25. Для яких a, b фактор–кільце $Z_2[x]/(x^2+ax+b)$ є полем?
26. Нехай R – поле дійсних чисел. Довести, що $R[x]/(x^2+x+1) \cong C$.
27. З'ясувати, чи ізоморфні фактор–кільця $Z_3[x]/(x^3+1)$ і $Z_3[x]/(x^3+x+1)$.
28. Довести, що довільне скінченне розширення скінченного поля є сепарабельним.
29. Довести, що кількість елементів скінченного поля є степенем простого числа.
30. З'ясувати, чи ізоморфні кільця $Z_3[x]/(x^2+x)$ і Z_9.

1.8. Мінімальний многочлен алгебраїчного елемента

Нагадаємо, що многочлен $f(x) \in P[x]$ степеня $n \geq 1$ називається незвідним над полем P, якщо його не можна розкласти в добуток многочленів степеня меншого за n. У противному разі многочлен $f(x)$ називається звідним над полем P. Якщо многочлен є звідним над полем P, то він звідний над будь–яким розширенням $\overline{P}$ поля P. Для кожного многочлена $f(x) \in P[x]$ степеня $n \geq 1$ існує розширення $\overline{P}$ поля P, в якому $f(x)$ має хоча б один корінь. Многочлен $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ з кільця $P[x]$ називається **нормованим**, або **унітарним**, якщо його старший коефіцієнт a_0 дорівнює одиниці.

Нехай T – кільце, R – підкільце кільця T. Елемент $t \in T$ **називається алгебраїчним елементом над** R, якщо існує такий многочлен $f(x) \in R[x]$, що $f(t) = 0$. Елемент $t \in T$ називається **трансцендентним елементом над** R, якщо такого многочлена не існує. Якщо кільце T збігається з полем комплексних чисел, а підкільце R – з полем раціональних чисел (тобто $R = Q$, $T = C$), то кажуть просто про **алгебраїчні і трансцендентні числа**.

Далі будемо розглядати лише многочлени з раціональними коефіцієнтами.

Приклад 1. Кожне раціональне число a є алгебраїчним числом, бо воно є коренем многочлена $f(x) = x - a$ з раціональними коефіцієнтами; кожне число вигляду $\sqrt[n]{a}$, де $n \in N$, $a \in Q$, також алгебраїчне, бо воно є коренем многочлена $f(x) = x^n - a$; числа i та $\sqrt{2} + \sqrt{3}$ є коренями відповідно многочленів $x^2 + 1$ та $x^4 - 10x^2 + 1$, тому вони також є алгебраїчними. Доведено, що кожне з чисел π, e, $\lg 2$, $2^{\sqrt{2}}$ є трансцендентним числом (зауважимо, що доведення трансцендентності якогось числа завжди є дуже важкою задачею).

Зауважимо, що множина всіх алгебраїчних чисел зліченна, а множина всіх трансцендентних чисел незліченна.

Многочлен $f(x)$ з раціональними коефіцієнтами, коренем якого є алгебраїчне число α, називається **анулюючим** многочленом числа α. Множина всіх анулюючих многочленів числа α є ідеалом в кільці многочленів з раціональними коефіцієнтами. Многочлен $f(x)$ називається **мінімальним многочленом для алгебраїчного числа** α, якщо він є незвідним над полем Q, анулюючим та нормованим. Мінімальний многочлен для алгебраїчного числа α позначається $m_\alpha(x)$. Степінь

мінімального многочлена $m_\alpha(x)$ числа α називається **степенем алгебраїчного числа α.**

Приклад 2. Многочлен $f(x)=x^5-11$ є мінімальним для елемента $\alpha=\sqrt[5]{11}$, оскільки він нормований, незвідний (за критерієм Айзенштайна для $p=11$) та анулюючий для цього числа. Многочлен

$$f(x)=x^6-6x^5+15x^4-24x^3+27x^2-18x+6$$

є мінімальним многочленом для елемента $\alpha=1+\sqrt[3]{2-\sqrt{3}}$: він є нормованим, незвідним (за критерієм Айзенштайна для $p=3$) та анулюючим для цього числа.

Мінімальний многочлен для алгебраїчного числа єдиний – це забезпечується умовами нормованості та незвідності многочлена.

Многочлен $f(x)\in Q[x]$ називається **сепарабельним,** якщо над полем C він має лише прості корені. Многочлен $f(x)=x^3-6x^2+12x-8$ сепарабельний, а многочлен $f(x)=x^2-10x+25=(x-5)^2$ не є сепарабельним.

Многочлен $f(x)\in Z[x]$ називається **примітивним**, якщо найбільший спільний дільник його коефіцієнтів дорівнює 1. Добуток двох примітивних многочленів є примітивним многочленом.

Приклад 3. Многочлен $f(x)=5x^6-10x^5+4x^4-9x+15$ є примітивним, а многочлен $f(x)=6x^6-10x^5+4x^4-24x+18$ не є примітивним.

Приклад 4. Знайти мінімальний многочлен для елемента $\alpha=\sqrt{2}+\sqrt{5}$.

Піднесемо ліву та праву частини до квадрата: $\alpha^2=2+2\sqrt{10}+5$, $\alpha^2-7=2\sqrt{10}$. Ще раз піднесемо ліву та праву частини до квадрата: $\alpha^4-14\alpha^2+49=40$. Многочлен $f(x)=x^4-14x^2+9$ є анулюючим і

нормованим. Пересвідчимося, що він є незвідним. Зауважимо, що над полем R цей многочлен має розклад:

$$x^4 - 14x^2 + 9 = \left(x - \sqrt{2} - \sqrt{5}\right)\left(x - \sqrt{2} + \sqrt{5}\right)\left(x + \sqrt{2} - \sqrt{5}\right)\left(x + \sqrt{2} + \sqrt{5}\right), \quad (*)$$

в якому жоден із лінійних множників не належить кільцю $Q[x]$. Тому над полем Q многочлен $f(x)$ може розкластися лише в добуток двох многочленів степеня 2. Але, групуючи множники розкладу $(*)$ по 2, ми все одно не одержимо многочленів із раціональними коефіцієнтами. Отже, многочлен $f(x) = x^4 - 14x^2 + 9$ є мінімальним.

Приклад 5. Знайти мінімальний многочлен для елемента $\alpha = \sqrt[5]{3 + \sqrt{3}}$.

Піднесемо ліву та праву частини до п'ятого степеня :

$$\alpha^5 = 3 + \sqrt{3} \text{ або } \alpha^5 - 3 = \sqrt{3}.$$

Піднесемо ліву та праву частини останньої рівності до квадрата: $\alpha^{10} - 6\alpha^5 + 9 = 3$, отже, $f(x) = x^{10} - 6x^5 + 6$. Анулюючий многочлен $f(x) = x^{10} - 6x^5 + 6$ є нормованим і незвідним за критерієм Айзенштайна для $p = 2$. Отже, многочлен $f(x) = x^{10} - 6x^5 + 6$ є мінімальним.

Завдання 11. Знайти мінімальний многочлен для елемента α

1) $\alpha = \sqrt{3} + \sqrt{11}$.	11) $\alpha = \sqrt{8} - \sqrt{3}$.	21) $\alpha = \sqrt{3} + 4i$.
2) $\alpha = \sqrt{7} - \sqrt{5}$.	12) $\alpha = \sqrt{7} + \sqrt{21}$.	22) $\alpha = \sqrt{14} - \sqrt{23}$.
3) $\alpha = \sqrt{3} - \sqrt{13}$.	13) $\alpha = 2\sqrt[4]{3} + 1$.	23) $\alpha = \sqrt{2} - 3\sqrt{11}$.
4) $\alpha = \sqrt{3} + i$.	14) $\alpha = \sqrt{3} + \sqrt{31}$.	24) $\alpha = 3\sqrt{3} + i$.
5) $\alpha = \sqrt{11} - \sqrt{17}$.	15) $\alpha = \sqrt{3} - \sqrt{15}$.	25) $\alpha = \sqrt{7} + \sqrt{8}$.
6) $\alpha = \sqrt{6} + \sqrt{19}$.	16) $\alpha = \sqrt{5} + \sqrt{12}$.	26) $\alpha = 2\sqrt{3} - i$.
7) $\alpha = \sqrt{5} + \sqrt{17}$.	17) $\alpha = \sqrt{3} - \sqrt{14}$.	27) $\alpha = \sqrt{3} + 2\sqrt{5}$.
8) $\alpha = 2\sqrt{3} - \sqrt{7}$.	18) $\alpha = \sqrt{10} + \sqrt{11}$.	28) $\alpha = 1 - \sqrt[4]{4}$.

9) $\alpha = i + \sqrt{11}$.	19) $\alpha = \sqrt{6} + \sqrt{7}$.	29) $\alpha = \sqrt{14} - \sqrt{11}$.
10) $\alpha = 3i - \sqrt{11}$.	20) $\alpha = \sqrt{3} - \sqrt{7}$.	30) $\alpha = \sqrt{7} + \sqrt{6}$.

1.9. Розширення поля

Якщо P є підполем поля $\overline{P}$, то поле $\overline{P}$ називають **розширенням поля P.**

Приклад 1. Поле $Q(\sqrt{5}) = \{ a + b\sqrt{5} : a,b \in Q \}$ є розширенням поля раціональних чисел. Поле комплексних чисел є розширенням поля дійсних чисел.

Нехай поле $\overline{P}$ є розширенням поля P і $A \subseteq \overline{P}$. Найменше підполе поля $\overline{P}$, яке містить поле P і множину A, позначають $P(A)$ і називають приєднанням до поля P елементів множини A. Якщо множина A складається лише з одного елемента a, то поле $P(a)$, називають простим розширенням поля P, а a – примітивним елементом цього розширення. Якщо елемент a є алгебраїчним елементом, то говорять про просте алгебраїчне розширення, якщо a є трансцендентним елементом, то говорять про просте трансцендентне розширення поля P. Будова простого трансцендентного розширення поля P характеризується наступним твердженням.

Твердження 1. Кожне просте трансцендентне розширення поля $P(\alpha)$ ізоморфне полю $P(x)$ раціональних дробів від змінної x із коефіцієнтами з поля P.

Приклад 2. Оскільки число π є трансцендентним числом, то

$$Q(\pi) = \left\{ \frac{f(\pi)}{g(\pi)} : f(x), g(x) \in Q[x], \quad g(x) \neq 0 \right\}.$$

Нехай $F-$ числове поле, $z \in F, \sqrt{z} \notin F$. Тоді просте квадратичне розширення поля F буде складатися з елементів вигляду $a+b\sqrt{z},\ a,b \in F$.

Твердження 2. Якщо α є алгебраїчним елементом над полем P степеня n, то поле $P(\alpha)$ складається з усіх елементів вигляду $\gamma = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$, де $a_i \in P$.

Зокрема, якщо $p-$ просте число, то просте розширення $Q\left(\sqrt[n]{p}\right)$ поля Q буде складатися з елементів вигляду

$$a_0 + a_1\sqrt[n]{p} + a_2\sqrt[n]{p^2} + a_3\sqrt[n]{p^3} + \ldots + a_{n-1}\sqrt[n]{p^{n-1}},\ a_i \in Q.$$

Приклад 3.

$$Q\left(\sqrt[6]{3}\right) = \left\{ a_0 + a_1\sqrt[6]{3} + a_2\sqrt[6]{3^2} + a_3\sqrt[6]{3^3} + a_4\sqrt[6]{3^4} + a_5\sqrt[6]{3^5} : a_0, \ldots, a_5 \in Q \right\}.$$

Якщо поле $\overline{P}$ є розширенням поля P, то $\overline{P}$ можна розглядати як векторний простір над полем P. Якщо цей простір є скінченновимірним, то розширення $\overline{P} \supseteq P$ називають **скінченним**, у противному випадку $\overline{P}$ називають **нескінченним розширенням** поля P. Розмірність $\dim_P \overline{P}$ векторного простору $\overline{P}$ над полем P позначають символом $\left[\overline{P} : P\right]$ і називають **степенем розширення** $\overline{P}$ над P.

Твердження 3. Якщо $\alpha-$ алгебраїчний елемент, то степінь $\left[P(\alpha) : P\right]$ розширення $P(\alpha) \supset P$ дорівнює степеню елемента α.

Приклад 4. Просте алгебраїчне розширення $P(\alpha)$ є скінченим розширенням поля P, оскільки степінь алгебраїчного елемента завжди скінченний. Просте трансцендентне розширення $P(\alpha)$ є нескінченим розширенням поля P.

Твердження 4. Нехай $F \supset P$, а $T \supset F$. Розширення $T \supset P$ буде скінченним тоді й лише тоді, коли буде скінченним кожне з розширень $T \supset F$ і $F \supset P$. Якщо вони скінченні, то $[T:P]=[T:F]\cdot[F:P]$.

Якщо $A=\{a_1,a_2,\ldots,a_n\}$, де $n>1$ і всі елементи $a_1,a_2,\ldots,a_n$ алгебраїчні над P, то розширення $P(A)=P(a_1,a_2,\ldots,a_n)$ називається складним алгебраїчним розширенням. Складне алгебраїчне розширення завжди скінченне.

Завдання 12. Описати вигляд елементів простого алгебраїчного розширення, утвореного приєднанням до поля Q елемент α

1) $\alpha=\sqrt[3]{53}$.
2) $\alpha=\sqrt[4]{47}$.
3) $\alpha=\sqrt[5]{23}$.
4) $\alpha=\sqrt[3]{17}$.
5) $\alpha=\sqrt[5]{11}$.
6) $\alpha=\sqrt[4]{19}$.
7) $\alpha=\sqrt[5]{5}$.
8) $\alpha=\sqrt[3]{11}$.
9) $\alpha=\sqrt[5]{13}$.
10) $\alpha=\sqrt[4]{17}$.
11) $\alpha=\sqrt[4]{29}$.
12) $\alpha=\sqrt[5]{17}$.
13) $\alpha=\sqrt[4]{23}$.
14) $\alpha=\sqrt[4]{53}$.
15) $\alpha=\sqrt[3]{13}$.
16) $\alpha=\sqrt[6]{5}$.
17) $\alpha=\sqrt[3]{23}$.
18) $\alpha=\sqrt[6]{2}$.
19) $\alpha=\sqrt[4]{37}$.
20) $\alpha=\sqrt[5]{19}$.
21) $\alpha=\sqrt[3]{31}$.
22) $\alpha=\sqrt[5]{7}$.
23) $\alpha=\sqrt[5]{37}$.
24) $\alpha=\sqrt[5]{41}$.
25) $\alpha=\sqrt[4]{59}$.
26) $\alpha=\sqrt[5]{31}$.
27) $\alpha=\sqrt[4]{49}$.
28) $\alpha=\sqrt[3]{41}$.
29) $\alpha=\sqrt[3]{37}$.
30) $\alpha=\sqrt[4]{5}$.

1.10. Поле розкладу многочлена

Нехай P – поле, $f(x)$ – многочлен степеня $n\geq 1$ із кільця $P[x]$. Найменше розширення $F \supset P$ поля P, над яким многочлен $f(x)$ розкладається в добуток лінійних множників,

$$f(x)=c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n), c\in P, \alpha_i \in F,$$

називається **полем розкладу многочлена** $f(x)$ і позначається $F = P(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Не виключено, що поле розкладу многочлена $f(x)$ збігається з полем P.

Приклад 1. Знайти степінь поля розкладу многочлена $x^2 - 3$ над Q.

Розкладемо многочлен $x^2 - 3$ на лінійні множники: $x^2 - 3 = \left(x + \sqrt{3}\right)\left(x - \sqrt{3}\right)$. Отже, полем розкладу є $Q\left(\sqrt{3}\right)$, тому степінь поля розкладу $\left[Q\left(\sqrt{3}\right) : Q\right] = 2$.

Приклад 2. Знайти степінь поля розкладу многочлена $x^3 - 2$ над Q.

Одним із коренів многочлена $x^3 - 2$ є число $\sqrt[3]{2}$. Тому для поля P розкладу многочлена $x^3 - 2$ маємо $P \supset Q\left(\sqrt[3]{2}\right) \supset Q$. За твердженням 3 попереднього параграфа $\left[Q\left(\sqrt[3]{2}\right) : Q\right] = 3$. Крім того, над полем $Q\left(\sqrt[3]{2}\right)$

$$x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}\right).$$

Зауважимо, що поле $Q\left(\sqrt[3]{2}\right) = \left\{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in Q\right\}$ містить лише дійсні числа, а многочлен $x^2 + \sqrt[3]{2}x + \sqrt[2]{4}$ дійсних коренів не має. Щоб одержати поле P, потрібно до $Q\left(\sqrt[3]{2}\right)$ приєднати один із коренів многочлена $x^2 + \sqrt[3]{2}x + \sqrt[2]{4}$. Отже, $\left[P : Q\left(\sqrt[3]{2}\right)\right] = 2$ і $\left[P : Q\right] = \left[P : Q\left(\sqrt[3]{2}\right)\right] \cdot \left[Q\left(\sqrt[3]{2}\right) : Q\right] = 2 \cdot 3 = 6$.

Приклад 3. Знайти степінь поля розкладу многочлена $x^8 + 1$ над Q.

З'ясуємо спочатку питання про звідність цього многочлена. Припустимо, що він звідний, тоді його можна подати у вигляді $x^8 + 1 = f(x) \cdot g(x)$, і звідним буде також многочлен

$$(y+1)^8 + 1 = f(y+1) \cdot g(y+1) = y^8 + 8y^7 + 28y^6 + 56y^5 + 70y^4 + 56y^3 + 28y^2 + 8 + 2$$

Але останній многочлен незвідний над полем Q за критерієм Айзенштайна для простого $p = 2$. Отже, наше припущення було

помилковим, тобто многочлен x^8+1 незвідний над Q. Поле P розкладу многочлена x^8+1 буде містити всі його корені многочлена

$$\varepsilon_k = \cos\frac{\pi(1+2k)}{8} + i\sin\frac{\pi(1+2k)}{8}, \quad k = 0,1,2,\ldots,7.$$

Очевидно, що $P \supseteq Q(\varepsilon_0)$. Оскільки $\varepsilon_0 -$ корінь незвідного многочлена x^8+1, то $[Q(\varepsilon_0):Q]=8$. З іншого боку, з рівностей $\varepsilon_k = \varepsilon_0^{2k+1}$, $k=1,2,\ldots,7$ випливає, що всі корені многочлена x^8+1 містяться в $Q(\varepsilon_0)$, тобто многочлен x^8+1 розкладається над $Q(\varepsilon_0)$ на лінійні множники. Отже, $P = Q(\varepsilon_0)$ і $[P:Q]=8$.

Приклад 4. Знайти степінь поля розкладу многочлена x^4-9 над Q. Оскільки $x^4-9=(x^2-3)(x^2+3)=(x-\sqrt{3})(x+\sqrt{3})(x-i\sqrt{3})(x+i\sqrt{3})$, то поле P розкладу многочлена x^4-9 збігається з полем $Q(\sqrt{3},i)$. Маємо ланцюжок розширень: $Q \subset Q(\sqrt{3}) \subset Q(\sqrt{3},i)$, тому степінь поля розкладу многочлена x^4-9 над $Q[x]$ дорівнює $[Q(\sqrt{3},i):Q]=[Q(\sqrt{3},i):Q(\sqrt{3})]\cdot[Q(\sqrt{3}):Q]=2\cdot 2=4$.

Приклад 5. Знайти степінь поля розкладу многочлена x^4-11 над Q. Зауважимо, що над полем раціональних чисел цей многочлен є незвідним за критерієм Айзенштайна. Оскільки $x^4-11=(x-\sqrt[4]{11})(x+\sqrt[4]{11})(x-i\sqrt[4]{11})(x+i\sqrt[4]{11})$, то поле P розкладу многочлена x^4-11 збігається з полем $Q(\sqrt[4]{11},i)$. Степінь поля розкладу многочлена x^4-11 над $Q[x]$ дорівнює

1. $[Q(\sqrt[4]{11},i):Q]=[Q(\sqrt[4]{11},i):Q(\sqrt[4]{11})]\cdot[Q(\sqrt[4]{11}):Q]=2\cdot 4=8$ $\varphi(\sqrt{3})=\sqrt{3}$, $\varphi(i)=i$ тоді

$$\varphi(a_1+a_2\sqrt{3}+a_3 i+a_4 i\sqrt{3}) = a_1+a_2\sqrt{3}+a_3 i+a_4 i\sqrt{3}.$$

Завдання 13. Знайти степінь поля розкладу многочлена

$$f(x) \in Q[x]$$

1) $f(x) = x^6 - 2$.
2) $f(x) = x^4 - 15$.
3) $f(x) = x^6 + 36$.
4) $f(x) = x^5 - 12$.
5) $f(x) = x^6 - 8$.
6) $f(x) = x^4 + 10$.
7) $f(x) = x^5 - 10$.
8) $f(x) = x^4 + 25$.
9) $f(x) = x^6 - 9$.
10) $f(x) = x^4 - 23$.
11) $f(x) = x^3 + 17$.
12) $f(x) = x^5 - 18$.
13) $f(x) = x^3 - 9$.
14) $f(x) = x^5 + 21$.
15) $f(x) = x^5 - 3$.
16) $f(x) = x^5 - 15$.
17) $f(x) = x^5 + 7$.
18) $f(x) = x^5 - 29$.
19) $f(x) = x^3 - 33$.
20) $f(x) = x^3 + 25$.
21) $f(x) = x^4 - 20$.
22) $f(x) = x^6 - 121$.
23) $f(x) = x^4 + 3$.
24) $f(x) = x^5 - 25$.
25) $f(x) = x^4 - 27$.
26) $f(x) = x^4 + 8$.
27) $f(x) = x^3 - 49$.
28) $f(x) = x^4 + 12$.
29) $f(x) = x^6 - 27$.
30) $f(x) = x^5 - 16$.

1.11. Автоморфізми поля

Автоморфізм поля P – це ізоморфізм поля P на себе. Множина всіх автоморфізмів поля P утворює групу відносно композиції автоморфізмів. Вона називається групою автоморфізмів поля P і позначається $AutP$.

Нехай поле F є розширенням поля P. Автоморфізм φ поля F називається автоморфізмом розширення $F \supset P$, якщо для всіх $x \in P$ $\varphi(x) = x$ (тобто всі елементи поля P є нерухомими точками автоморфізму φ). Група всіх автоморфізмів розширення $F \supset P$ позначається $Aut(F : P)$. Якщо P – просте поле, то $Aut(F : P) = AutF$, бо просте поле при будь-якому автоморфізмі лишається нерухомим.

Твердження 1. Для скінченного розширення $F \supset P$ $|Aut(F : P)| \le [F : P]$.

Приклад 1. Знайти всі автоморфізми поля $Q\left(\sqrt[3]{17}\right)$.

Кожний елемент поля можна записати у вигляді $a+b\sqrt[3]{17}+c\sqrt[3]{17^2}$, де $a,b,c\in Q$. Q – просте поле, тому при автоморфізмах елементи з Q будуть лишатися нерухомими. Нехай $\varphi\in AutQ\left(\sqrt[3]{17}\right)$. Оскільки $\left(\sqrt[3]{17}\right)^3=17$, то $\varphi\left(\sqrt[3]{17}\right)^3=17$, тобто $\varphi\left(\sqrt[3]{17}\right)$ є коренем многочлена x^3-17. Але всі елементи поля $Q\left(\sqrt[3]{17}\right)$ є дійсними числами, а многочлен x^3-17 має лише один дійсний корінь – число $\sqrt[3]{17}$. Тому має бути $\varphi\left(\sqrt[3]{17}\right)=\sqrt[3]{17}$ і $\varphi\left(a+b\sqrt[3]{17}+c\sqrt[3]{17^2}\right)=\varphi(a)+\varphi(b)\varphi\left(\sqrt[3]{17}\right)+\varphi(c)\varphi(\sqrt[3]{17^2})=a+b\sqrt[3]{17}+c\sqrt[3]{17^2}$. Отже, маємо лише тотожній автоморфізм.

Приклад 2. Знайти всі автоморфізми поля $Q\left(\sqrt{3},i\right)$.

Кожний елемент поля можна записати у вигляді $a_1+a_2\sqrt{3}+a_3i+a_4i\sqrt{3}$, де $a_i\in Q$. Елементи з поля Q при автоморфізмі залишаються нерухомими. Для елемента $\sqrt{3}$ мінімальним многочленом є многочлен x^2-3. Поле $Q\left(\sqrt{3},i\right)$ містить два дійсних кореня мінімального многочлена, а саме $\sqrt{3}$ і $-\sqrt{3}$. Для елемента i мінімальним многочленом є многочлен x^2+1. Поле $Q\left(\sqrt{3},i\right)$ містить обидва комплексних кореня цього мінімального многочлена, а саме i та $-i$. Нехай $\varphi\in AutQ\left(\sqrt{3},i\right)$. Тоді

$$\varphi\left(a_1+a_2\sqrt{3}+a_3i+a_4i\sqrt{3}\right)=\varphi(a_1)+\varphi\left(a_2\sqrt{3}\right)+\varphi(a_3i)+\varphi\left(a_4i\sqrt{3}\right)=$$
$$=a_1+a_2\varphi\left(\sqrt{3}\right)+a_3\varphi(i)+a_4\varphi(i)\cdot\varphi\left(\sqrt{3}\right).$$

Можливі таки варіанти:

2. $\varphi\left(\sqrt{3}\right)=\sqrt{3}$, $\varphi(i)=i$, тоді
$$\varphi\left(a_1+a_2\sqrt{3}+a_3i+a_4i\sqrt{3}\right)=a_1+a_2\sqrt{3}+a_3i+a_4i\sqrt{3}.$$
3. $\varphi\left(\sqrt{3}\right)=-\sqrt{3}$, $\varphi(i)=i$, тоді

$$\varphi\left(a_1 + a_2\sqrt{3} + a_3 i + a_4 i\sqrt{3}\right) = a_1 - a_2\sqrt{3} + a_3 i - a_4 i\sqrt{3}.$$

4. $\varphi\left(\sqrt{3}\right) = \sqrt{3}$, $\varphi(i) = -i$, тоді

$$\varphi\left(a_1 + a_2\sqrt{3} + a_3 i + a_4 i\sqrt{3}\right) = a_1 + a_2\sqrt{3} - a_3 i - a_4 i\sqrt{3}.$$

5. $\varphi\left(\sqrt{3}\right) = -\sqrt{3}$, $\varphi(i) = -i$, тоді

$$\varphi\left(a_1 + a_2\sqrt{3} + a_3 i + a_4 i\sqrt{3}\right) = a_1 - a_2\sqrt{3} - a_3 i + a_4 i\sqrt{3}.$$

Можна перевірити, що кожне з цих відображень справді є автоморфізмом.

Зауважимо, що поле $Q\left(\sqrt[4]{p}\right)$, де p – просте число, буде мати два автоморфізми. Кожний елемент поля $Q\left(\sqrt[4]{p}\right)$ можна записати у вигляді $a_1 + a_2\sqrt[4]{p} + a_3\sqrt[4]{p^2} + a_4\sqrt[4]{p^3}$, де $a_i \in Q$. Елементи з поля Q при автоморфізмі залишаються нерухомими (поле Q просте). Для елемента $\sqrt[4]{p}$ мінімальним многочленом є многочлен $x^4 - p$. Поле $Q\left(\sqrt[4]{p}\right)$ містить два дійсних кореня мінімального многочлена, а саме $\sqrt[4]{p}$ і $-\sqrt[4]{p}$. Нехай $\varphi \in AutQ\left(\sqrt[4]{p}\right)$. Тоді

$$\varphi\left(a_1 + a_2\sqrt[4]{p} + a_3\sqrt[4]{p^2} + a_4\sqrt[4]{p^3}\right) = \varphi(a_1) + \varphi\left(a_2\sqrt[4]{p}\right) + \varphi\left(a_3\sqrt[4]{p^2}\right) + \varphi\left(a_4\sqrt[4]{p^3}\right) =$$
$$= a_1 + a_2\varphi\left(\sqrt[4]{p}\right) + a_3\varphi\left(\sqrt[4]{p^2}\right) + a_4\varphi\left(\sqrt[4]{p^3}\right).$$

Можливі таки варіанти:

6. $\varphi\left(\sqrt[4]{p}\right) = \sqrt[4]{p}$, тоді

$$\varphi\left(a_1 + a_2\sqrt[4]{p} + a_3\sqrt[4]{p^2} + a_4\sqrt[4]{p^3}\right) = a_1 + a_2\sqrt[4]{p} + a_3\sqrt[4]{p^2} + a_4\sqrt[4]{p}$$

7. $\varphi\left(\sqrt[4]{p}\right) = -\sqrt[4]{p}$, тоді

$$\varphi\left(a_1 + a_2\sqrt[4]{p} + a_3\sqrt[4]{p^2} + a_4\sqrt[4]{p^3}\right) = a_1 - a_2\sqrt[4]{p} + a_3\sqrt[4]{p^2} - a_4\sqrt[4]{p}.$$

Легко перевірити, що кожне з цих відображень справді є автоморфізмом.

Завдання 14. Знайти всі автоморфізми поля :

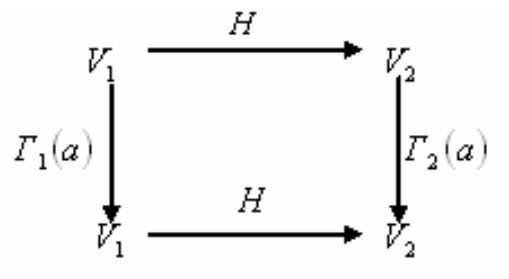
1) $Q\left(\sqrt[4]{5}\right)$.
2) $Q\left(\sqrt{17},\sqrt{2}\right)$.
3) $Q\left(\sqrt{7},i\right)$.
4) $Q\left(\sqrt[4]{7}\right)$.
5) $Q\left(\sqrt{2},\sqrt{3}\right)$.
6) $Q\left(\sqrt{12}\right)$.
7) $Q\left(\sqrt{21}\right)$.
8) $Q\left(\sqrt{18}\right)$.
9) $Q\left(\sqrt{14}\right)$.
10) $Q\left(\sqrt{41},i\right)$.
11) $Q\left(\sqrt[3]{11}\right)$.
12) $Q\left(\sqrt{22}\right)$.
13) $Q\left(\sqrt{2},\sqrt{19}\right)$.
14) $Q\left(\sqrt{6}\right)$.
15) $Q\left(\sqrt{7},i\right)$.
16) $Q\left(\sqrt[4]{3}\right)$.
17) $Q\left(\sqrt[3]{5}\right)$.
18) $Q\left(\sqrt{13},\sqrt{3}\right)$.
19) $Q\left(\sqrt{3},\sqrt{11}\right)$.
20) $Q\left(\sqrt[3]{7}\right)$.
21) $Q\left(\sqrt[4]{2}\right)$.
22) $Q\left(\sqrt{29},i\right)$.
23) $Q\left(\sqrt[3]{2}\right)$.
24) $Q\left(\sqrt{24}\right)$.
25) $Q\left(\sqrt{19},\sqrt{2}\right)$.
26) $Q\left(\sqrt{5},\sqrt{11}\right)$.
27) $Q\left(\sqrt[3]{3}\right)$.
28) $Q\left(\sqrt{11},i\right)$.
29) $Q\left(\sqrt{10}\right)$.
30) $Q\left(\sqrt{20}\right)$.

Розділ 2. Основи теорії зображень груп

2.1. Зображення груп

Гомоморфне відображення Γ групи G в групу $GL(V)$ невироджених лінійних операторів, що діють в векторному (комплексному) просторі V, називається **лінійним (комплексним) зображенням групи** G. Розмірність простору V називається розмірністю або, частіше, **степенем зображення**. Одиничне зображення групи G – це одновимірне зображення $\Gamma : G \to C^*$, при якому кожному $a \in G$ ставиться у відповідність число 1, тобто $\Gamma(a) = 1$, $\forall a \in G$.

Зображення $\Gamma_1 : G \to GL(V_1)$ і $\Gamma_2 : G \to GL(V_2)$ називаються **ізоморфними** (еквівалентними, подібними), якщо існує таке ізоморфне відображення H простору V_1 на простір V_2, що $H\Gamma_1(a) = \Gamma_2(a)H$ для всіх $a \in G$, тобто для кожного $a \in G$ має бути комутативною діаграма



Зображення $\Gamma : G \to GL(V)$ називається звідним, якщо в V існує нетривіальний (відмінний від V та від нульового підпростору) підпростір V_1, інваріантний відносно G (тобто інваріантний відносно всіх перетворень $\Gamma(a)$, де $a \in G$). Якщо такого підпростору не існує, то зображення Γ називається **незвідним**. Одновимірне зображення завжди незвідне.

Якщо W інваріантний підпростір для зображення $\Gamma : G \to GL(V)$, то ми можемо розглянути індуковане зображення $\widetilde{\Gamma} : G \to GL(W)$, обмеживши кожний оператор $\Gamma(a) : V \to V$ на підпростір W. Кажуть, що зображення $\Gamma : G \to GL(V)$ є прямою сумою зображень $\Gamma_1 : G \to GL(V_1)$ і $\Gamma_2 : G \to GL(V_2)$ (і записують $\Gamma = \Gamma_1 \oplus \Gamma_2$), якщо простір V розпадається в пряму суму $V = V_1 \oplus V_2$ інваріантних
відносно Γ підпросторів V_1 і V_2, а індуковані зображення
$\widetilde{\Gamma}_1 : G \to GL(V_1)$ і $\widetilde{\Gamma}_2 : G \to GL(V_2)$ збігаються відповідно з Γ_1 і Γ_2.

Твердження 1. Довільне комплексне зображення скінченної групи або незвідне, або є прямою сумою незвідних зображень.

Твердження 2. Нехай $G-$ група порядку n і $\Gamma_1, \Gamma_2, \ldots, \Gamma_k -$ всі попарно неізоморфні незвідні комплексні зображення групи G степенів $n_1, n_2, \ldots, n_k$ відповідно. Тоді k дорівнює кількості класів спряжених елементів групи G, кожне з чисел $n_1, n_2, \ldots, n_k$ є дільником числа n, хоча б одне з чисел $n_1, n_2, \ldots, n_k$ дорівнює 1 і $n_1^2 + n_2^2 + \ldots + n_k^2 = n$.

Для симетричної групи S_n степеня $n \geq 3$ та знакозмінної групи A_n степеня $n > 3$ завжди існує незвідне зображення степеня $n-1$.

Якщо група G абелева, то кількість класів спряжених елементів дорівнює порядку групи, тому всі незвідні зображення абелевої групи одновимірні і кількість таких зображень дорівнює порядку групи. Оскільки циклічна група комутативна, то всі її незвідні зображення одновимірні.

Нагадаємо, що порядок групи D_n симетрій правильного $n-$ кутника дорівнює $2n$, а кількість класів спряжених елементів у групі D_n дорівнює $\frac{n+3}{2}$ при непарному n, і $\frac{n}{2}+3$ при парному n.

Приклад 1. Знайти кількість нееквівалентних незвідних лінійних зображень групи A_5 та вказати їх розмірності.

Порядок групи A_5 дорівнює $\frac{5!}{2}=60$, кількість класів спряжених елементів дорівнює 5. Ця група має незвідне зображення степеня 4 та одновимірне зображення. Отже, $n_1^2+n_2^2+n_3^2+4^2+1=60$, звідси маємо $n_1^2+n_2^2+n_3^2=43$. Легко пересвідчитись, що останнє рівняння має лише один (із точністю до порядку доданків) розв'язок у натуральних числах: $n_1=n_2=3,\ n_3=5$. Отже, група A_5 має одне одновимірне, два тривимірних, одне чотиривимірне та одне п'ятивимірне незвідні зображення.

Приклад 2. Знайти кількість нееквівалентних незвідних лінійних зображень групи $G=D_6\times C_2$ та вказати їх розмірності.

Порядок групи D_6 дорівнює 12, кількість класів спряжених елементів $\frac{6}{2}+3=6$; порядок групи C_2 – дорівнює 2, кількість класів спряжених елементів також дорівнює 2. Порядок групи $G=D_6\times C_2$ дорівнює $12\cdot 2=24$, кількість класів спряжених елементів дорівнює $6\cdot 2=12$. Маємо: $24=n_1^2+n_2^2+\ldots+n_{11}^2+1$. Або $23=n_1^2+n_2^2+\ldots+n_{11}^2$.

Нехай $n_1 \geq n_2 \geq n_3 \geq \ldots \geq n_{11}$. Зрозуміло, що $n_1 < 4$ (бо інакше $7 = n_2^2 + n_3^2 + \ldots + n_{11}^2$ при $n_i \neq 0$). Нехай $n_1 = 3$, тоді $14 = n_2^2 + n_3^2 + \ldots + n_{11}^2$. Очевидно, що $n_2 \leq 2$, але серед чисел n_i не всі дорівнюють 1. Нехай одновимірних зображень буде k. Тоді $k + (10 - k) \cdot 4 = 14$, але рівняння $26 = 3k$ в натуральних числах розв'язку немає. Отже, випадок $n_1 = 3$ неможливий.

Нехай $n_1 = 2$, тоді $19 = n_2^2 + n_3^2 + \ldots + n_{11}^2$, де не всі $n_i = 1$. Нехай одновимірних зображень буде k, тоді $k + (10 - k) \cdot 4 = 19$, $21 = 3k$, тобто $k = 7$.

Отже, група $G = D_6 \times C_2$ має 8 одновимірних і 4 двовимірних незвідних зображень.

Завдання 15. Знайти кількість нееквівалентних незвідних лінійних зображень групи G та вказати їх розмірності

1) $G = D_8$.
2) $G = S_3$.
3) $G = D_3 \times C_2$.
4) $G = A_4$.
5) $G = D_3 \times C_4$.
6) $G = D_4$.
7) $G = D_4 \times C_2$.
8) $G = Q_8$.
9) $G = A_4 \times C_2$.
10) $G = D_{12}$.
11) $G = S_4$.
12) $G = Q_8 \times C_2$.
13) $G = D_3$.
14) $G = D_3 \times C_3$.
15) $G = Z_8$.
16) $G = S_3 \times C_2$.
17) $G = D_9$.
18) $G = S_3 \times C_2 \times C_2$.
19) $G = D_6$.
20) $G = Q_8 \times C_3$.
21) $G = S_3 \times C_4$.
22) $G = S_3 \times C_3$.
23) $G = D_5 \times C_2$
24) $G = D_4 \times C_3$.
25) $G = D_3 \times C_2 \times C_2$.
26) $G = D_{10}$.
27) $G = GL_2(Z_2) \times C_2$.
28) $G = GL_2(Z_2) \times C_4$.
29) $G = D_{11}$.
30) $G = GL_2(Z_2) \times C_3$.

Додаток 1. Питання колоквіуму

4 семестр

1. Бінарні операції, асоціативність, комутативність та дистрибутивність бінарних операцій, основні властивості бінарних операцій.
2. Означення групи, приклади груп.
3. Властивості груп. Довести:
4. a) рівність $a^m \cdot a^n = a^{m+n}$;
5. b) що кожне з рівнянь $ax = b$, $ya = b$ має єдиний розв'язок;
6. c) що з $ab = ac$ випливає $b = c$.
7. Підгрупи та їх властивості. Критерії того, що підмножина групи є підгрупою.
8. Циклічна група; приклади циклічних груп. Теорема про будову підгруп циклічної групи.
9. Ізоморфізм груп; показати, що відношення ізоморфізму є відношенням еквівалентності.
10. Довести, що при ізоморфізмі нейтральний елемент переходить в нейтральний елемент, а обернений елемент – в обернений.
11. Теорема, що коли множина з бінарною операцією ізоморфна групі, то вона є групою.
12. Теорема: кожна нескінченна циклічна група ізоморфна адитивній групі цілих чисел, кожна скінченна група порядку n ізоморфна групі поворотів правильного n - кутника.
13. Розклад групи за підгрупою.
14. Теорема Лагранжа та наслідки з неї.
15. Кільця, приклади кілець, кільце лишків.
16. Основні властивості кілець, кільце з одиницею, дільники одиниці.
17. Дільники нуля. Область цілісності. Приклади областей цілісності.
18. Підкільце. Критерій того, що підмножина кільця є підкільцем.
19. Ізоморфізм кілець, властивості ізоморфних кілець.

20. Поле, властивості полів. Поле лишків Z_p. Довести, що поле не містить дільників нуля.
21. Характеристика поля, її властивості. Довести, що в полі характеристики p $(a+b)^p = a^p + +b^p$.
22. Підполе, розширення поля, ізоморфізм полів.
23. Ділення з остачею в кільці Z, єдиність розкладу в добуток простих чисел.
24. Означення нормальної підгрупи; спряжений елемент; необхідна і достатня умова нормальності підгрупи; перетин нормальних підгруп групи G.
25. Фактор–група за нормальною підгрупою та її властивості.
26. Основна теорема про гомоморфізм груп.
27. Теорема про фактор–групи за нормальною підгрупою і підгрупи даної групи.
28. Теорема про ізоморфізм груп.
29. Підгрупа, породжена підмножиною групи; структура цієї підгрупи.
30. Прямі добутки груп. Довести, що прямий добуток груп є групою.
31. Необхідна і достатня умова розкладності групи в прямий добуток двох своїх підгруп.
32. Пряма сума абелевих груп.
33. Теорема про нерозкладність у прямий добуток примарних циклічних груп.
34. Довести, що коли $n = st$, де $(s,t) = 1$, то циклічна група порядку n розкладається в пряму суму циклічних груп порядків s і t.
35. Довести, що коли циклічна група має порядок $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_k}$, то вона розкладається в пряму суму циклічних груп порядків $p_1^{k_1}, p_2^{k_2}, \dots, p_m^{k_k}$.
36. Довести, що в скінченній абелевій групі існують елементи, порядки яких є степенями простих чисел.

37. Довести, що скінченна абелева група розкладається в пряму суму примарних циклічних підгруп.
38. Довести, що коли порядок кожного елемента є степенем даного простого числа, то і порядок групи також є степенем цього простого числа.
39. Кожна скінченна абелева p–група розкладається в пряму суму примарних циклічних підгруп.
40. Теорема про єдиність розкладу скінченної абелевої групи в пряму суму примарних підгруп.
41. Основна теорема про скінченні абелеві групи.
42. Ідеал кільця, головний ідеал, приклади кілець головних ідеалів.
43. Операції над ідеалами.
44. Фактор–кільце за ідеалом.
45. Гомоморфізм кілець, образ нульового та оберненого елемента при гомоморфізмі
46. Основна теорема про гомоморфізм кілець.
47. Прямі суми кілець.
48. Допоміжна лема про попарно взаємно прості числа.
49. Теорема про розклад групи Z_n.
50. Теорема про мультиплікативну групу кільця Z_n^*.
51. Довести, що коли елементи a і b переставні, їх порядки s та t взаємно прості, то елемент ab породжує циклічну підгрупу порядку st.
52. Довести, що коли p–непарне просте число, то при будь–якому m група $Z_{p^m}^*$ циклічна.
53. Теорема: Z_2^* і Z_4^* – циклічні групи порядків 1 і 2 відповідно; при $m \geq 3$ група $Z_{2^m}^*$ є прямим добутком групи порядку 2^{m-2} і циклічної групи порядку 2. Наслідок.

Додаток 2. Варіанти контрольних та самостійних робіт

Самостійна робота (4 семестр).

Варіант 1

1. Знайти всі орбіти та всі стаціонарні підгрупи для групи $G = \langle g \rangle$:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 10 & 5 & 9 & 1 & 2 & 3 & 8 & 4 & 6 \end{pmatrix}.$$

2. Скласти таблицю Келі для фактор–групи : *a*) $4Z/24Z$; *b*) U_{40}/U_8 .
3. Розкласти в пряму суму груп Z_{2160} .
4. Використовуючи основну теорему про скінченні абелеві групи, знайти, з точністю до ізоморфізму, всі абелеві групи порядку 40 .
5. Чи ізоморфні абелеви групи: $Z_6 \oplus Z_{48} \oplus Z_{343}$,

$$Z_2 \oplus Z_{14} \oplus Z_{36} \oplus Z_{98}, \ Z_3 \oplus Z_{48} \oplus Z_{686} .$$

6. Чи утворюють ідеал необоротні елементи кільця Z_{243} . Знайти всі ідеали кільця Z_{84} .

Варіант 2

1. Знайти всі орбіти та всі стаціонарні підгрупи для групи $G = \langle g \rangle$:

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 1 & 5 & 3 & 8 & 9 & 10 & 7 & 6 \end{pmatrix}.$$

2. Скласти таблицю Келі для фактор–групи : *a*) $6Z/30Z$; *b*) U_{40}/U_8 .
3. Розкласти в пряму суму груп Z_{28224} .
4. Використовуючи основну теорему про скінченні абелеві групи, знайти, з точністю до ізоморфізму, всі абелеві групи порядку 54 .
5. Чи ізоморфні абелеви групи: $Z_{17} \oplus Z_{121} \oplus Z_{143}$,

$$Z_{13} \oplus Z_{17} \oplus Z_{1331}, \ Z_{13} \oplus Z_{121} \oplus Z_{187} .$$

6. Чи утворюють ідеал необоротні елементи кільця Z_{135} . Знайти всі ідеали кільця Z_{198} .

Контрольна робота (4 семестр)

Варіант 1

1. Довести, що в групі Q/Z кожен елемент має скінченний порядок.
2. Розкласти в пряму суму циклічних груп фактор – групу A/B, де A – вільна абелева група рангу 3, а підгрупа B породжується елементами y_1, y_2, y_3, де $x_1 = (1,0,0)$, $x_2 = (0,1,0)$, $x_3 = (0,0,1)$

   $y_1 = 5x_1 + 5x_2 + 4x_3$, $y_2 = -7x_1 + 6x_2 + 9x_3$, $y_3 = 5x_1 + 4x_2 - 4x_3$.
3. Чи ізоморфні абелеві групи

   $Z_7 \oplus Z_{32} \oplus Z_{81}$, $Z_4 \oplus Z_{56} \oplus Z_{81}$, $Z_8 \oplus Z_{28} \oplus Z_{81}$.
4. Знайти всі гомоморфізми кілець $f : 4Z \to 3Z$.
5. Знайти мінімальний многочлен для елемента $\alpha = 2\sqrt[4]{3} + 1$.

Варіант 2

1. Нехай в абелевій групі G є елементи порядків 35 і 42. Довести, що в групі G є елемент порядку 210.
2. Знайти всі гомоморфні відображення групи $Z_{28} \to Z_7$.
3. Чи ізоморфні абелеві групи $Z_{33} \oplus Z_{54}$, $Z_{27} \oplus Z_{22} \oplus Z_3$, $Z_{22} \oplus Z_{81}$.
4. Знайти всі автоморфізми поля $Q(\sqrt[3]{5})$.
5. Знайти степінь поля розкладу многочлена $f(x) = x^4 + 25 \in Q[x]$.

Додаток 3. Цікаві задачі

1. Доведіть, що довільна скінченна підгрупа H групи C^* є циклічною.
2. Нехай p, q – прості числа та $p < q$. Доведіть, що кожна група порядку pq містить підгрупу порядку p (порядку q).
3. Доведіть, що для кожного натурального числа n фактор–група Q/Z містить єдину підгрупу порядку n.
4. Доведіть, що всі скінченні підгрупи фактор–групи Q/Z – циклічні.
5. Доведіть, що кожна некомутативна група порядку 8 ізоморфна або групі D_4, або групі кватерніонів Q_8.
6. Доведіть, що кожна група порядку p^4 містить абелеву підгрупу порядку p^3.
7. Доведіть, що група A_5 не містить підгруп порядків 15, 20 і 30.
8. Знайдіть кількість силовських p – підгруп у групі S_{2p}.
9. Знайти примітивний елемент поля $Q\left(\sqrt{p}, \sqrt{q}\right)$, де p, q – прості числа.
10. Знайти розмірність поля розкладу многочлена $x^p - 2$ над полем Q, p – просте.
11. Довести, якщо для скінченних нормальних підгруп $K, H \lhd G$ виконується рівність: $|HK| \cdot |H \cap K| = |H| \cdot |K|$.
12. Нехай $K_1, K_2 \lhd G$ такі, що $K_1 \cap K_2 = E$. Чи ізоморфна група G деякій підгрупі декартового добутку $\left(G/K_1\right) \times \left(G/K_2\right)$.
13. Довести: якщо F є розширенням простого поля P простого степеня, то воно не має власних підполів окрім P.
14. Довести, що коли елемент x кільця $\Re$ є нільпотентним, то елемент $(1 - x)$ є оборотним *(елемент a кільця $\Re$ називається нільпотентним, якщо для деякого натурального числа n маємо $a^n = 0$)*.
15. Довести, що Z_m містить нільпотентні елементи тоді й лише тоді, коли m ділиться на квадрат натурального числа більшого за 1.
16. Довести: кожне п'яти елементне кільце або ізоморфне Z_5, або є кільцем з нульовим множенням.
17. Нехай $K \lhd G = A \times B$. Доведіть, що або K абелева група, або один з перетинів $K \cap A$, $K \cap B$ є нетривіальним.
18. Доведіть, що фактор кільце $Z[i]/(3)$ є полем з 9 елементів.
19. З'ясувати, чи буде полем фактор–кільце $Z_5[x]/\left(x^2 + 4x + 1\right)$.

Додаток 4. Умовні позначення

$НСД(a,b)$ – найбільший спільний дільник чисел a та b;

$НСК(a,b)$ – найменше спільне кратне чисел a та b;

A^T – матриця, транспонована до матриці A;

$|A|$ – потужність множини A;

$|a|$ – порядок елемента a;

$\langle a,b,...,c \rangle$ – група породжена елементами $a,b,...,c$;

$A \subseteq B$ – A є підмножиною B;

$A \subset B$ – A є власною підмножиною B (тобто $A \subseteq B$ і $A \neq B$);

A_n – знакозмінна група всіх парних підстановок степеня n;

C – множина, або адитивна група, або поле комплексних чисел;

C^* – мультиплікативна група поля комплексних чисел;

C_n – група за множенням усіх комплексних коренів степеня n з 1 або група поворотів правильного n-кутника;

$C(a)$ – клас спряженості елемента a;

D_n – група симетрій правильного n-кутника;

E_n – одинична матриця порядку n (матриця порядку n, в якій на головній діагоналі стоять одиниці, а решта елементів – нулі);

$GL_n(P)$ – повна лінійна група степеня n – група за множенням усіх невироджених матриць порядку n з коефіцієнтами з поля P;

$GL_n(Z)$ – група за множенням усіх невироджених цілочисельних матриць порядку n, обернені до яких також є цілочисельними;

G/H – фактор-група групи G за нормальною підгрупою H;

$H \lhd G$ – H є нормальною підгрупою H;

K_4 – четверна група Кляйна – група підстановок $\{e,(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\}$;

$M_{n\times m}(P)$ – адитивна група матриць розміру $n \times m$ з коефіцієнтами з поля P;

$M_n(P)$ – адитивна група квадратних матриць порядку n з коефіцієнтами з поля P;

N_0 – множина цілих невід'ємних чисел;

$P[x]$ – кільце многочленів від x з коефіцієнтами з поля P;

$P_n[x]$ – множина всіх многочленів від x степеня не більшого ніж n з коефіцієнтами з поля P;

$P_n[x_1,...,x_k]$ – множина всіх многочленів степеня не більшого ніж n від змінних $x_1,...,x_k$ з коефіцієнтами з поля P;

Q_8 – група кватерніонів;

Q^+ – мультиплікативна група всіх додатних раціональних чисел;

Q^* – мультиплікативна група поля раціональних чисел;

R^+ – мультиплікативна група всіх додатних дійсних чисел;

R^* – мультиплікативна група поля дійсних чисел;

$SL_n(P)$ – спеціальна лінійна група степеня n – підгрупа матриць із $GL_n(P)$, визначник яких дорівнює 1;

S_n – симетрична група всіх підстановок степеня n;

$T_n(P)$ – група за множенням усіх невироджених верхніх трикутних матриць порядку n з коефіцієнтами з поля P;

U_n – група комплексних коренів степеня n з 1;

Z_n – множина, або адитивна група, або кільце класів лишків за модулем натурального числа n;

Z_n^* – мультиплікативна група оборотних класів лишків за модулем числа n;

$\tau(n)$ – кількість всіх натуральних дільників числа n;

$S(n)$ – сума всіх кількість всіх натуральних дільників числа n;

$\varphi(n)$ – функція Ойлера – кількість натуральних чисел менших за n та взаємно простих з ним.

Додаток 5. Таблиця простих чисел для $n \le 4861$

2	233	547	877	1229	1597	1993	2371	2749	3187	3583	4003	4421
3	239	557	881	1231	1601	1997	2377	2753	3191	3593	4007	4423
5	241	563	883	1237	1607	1999	2381	2767	3203	3607	4013	4441
7	251	569	887	1249	1609	2003	2383	2777	3209	3613	4019	4447
11	257	571	907	1259	1613	2011	2389	2789	3217	3617	4021	4457
13	263	577	911	1277	1619	2017	2393	2791	3221	3623	4027	4463
17	269	587	919	1279	1621	2027	2399	2797	3229	3631	4049	4481
19	271	593	929	1283	1627	2029	2411	2801	3251	3637	4051	4483
23	277	599	937	1289	1637	2039	2417	2803	3253	3643	3307	4493
29	281	601	941	1291	1657	2053	2423	2819	3257	3659	4057	4507
31	283	607	947	1297	1663	2063	2437	2833	3259	3671	4073	4513
37	293	613	953	1301	1667	2069	2441	2837	3271	3673	4079	4517
41	307	617	967	1303	1669	2081	2447	2843	3299	3677	4091	4519
43	311	619	971	1307	1693	2083	2459	2851	3301	3691	4093	4523
47	313	631	977	1319	1697	2087	2467	2857	3313	3697	4099	4547
53	317	641	983	1321	1699	2089	2473	2861	3319	3701	4111	4549
59	331	643	991	1327	1709	2099	2477	2879	3323	3709	4127	4561
61	337	647	997	1361	1721	2111	2503	2887	3329	3719	4129	4567
67	347	653	1009	1367	1723	2113	2521	2897	3331	3727	4133	4583
71	349	659	1013	1373	1733	2129	2531	2903	3343	3733	4139	4591
73	353	661	1019	1381	1741	2131	2539	2909	3347	3739	4153	4597
79	359	673	1021	1399	1747	2137	2543	2917	3359	3761	4157	4621
83	367	677	1031	1409	1753	2141	2549	2927	3361	3767	4159	4637
89	373	683	1033	1423	1759	2143	2551	2939	3371	3769	4177	4639
97	379	691	1039	1427	1777	2153	2557	2953	3373	3779	4201	4643
101	383	701	1049	1429	1783	2161	2579	2957	3389	3793	4211	4649
103	389	709	1051	1433	1787	2179	2591	2963	3391	3797	4217	4651
107	397	719	1061	1439	1789	2203	2593	2969	3407	3803	4219	4657
109	401	727	1063	1447	1801	2207	2609	2971	3413	3821	4229	4663
113	409	733	1069	1451	1811	2213	2617	2999	3433	3823	4231	4673
127	419	739	1087	1453	1823	2221	2621	3001	3449	3833	4241	4679
131	421	743	1091	1459	1831	2237	2633	3011	3457	3847	4243	4691
137	431	751	1093	1471	1847	2239	2647	3019	3461	3851	4253	4703
139	433	757	1097	1481	1861	2243	2657	3023	3463	3853	4259	4721
149	439	761	1103	1483	1867	2251	2659	3037	3467	3863	4261	4723
151	443	769	1109	1487	1871	2267	2663	3041	3469	3877	4271	4451
157	449	773	1117	1489	1873	2269	2671	3049	3491	3881	4273	4729
163	457	787	1123	1493	1877	2273	2677	3061	3499	3889	4283	4733
167	461	797	1129	1499	1879	2281	2683	3067	3511	3907	4289	4751
173	463	809	1151	1511	1889	2287	2687	3079	3517	3911	4297	4759
179	467	811	1153	1523	1901	2293	2689	3083	3527	3917	4327	4783
181	479	821	1163	1531	1907	2297	2693	3089	3529	3919	4337	4787
191	487	823	1171	1543	1913	2309	2699	3109	3533	3923	4339	4789
193	491	827	1181	1549	1931	2311	2707	3119	3539	3929	4349	4793
197	499	829	1187	1553	1933	2333	2711	3121	3541	3931	4357	4799
199	503	839	1193	1559	1949	2339	2713	3137	3547	3943	4363	4801
211	509	853	1201	1567	1951	2341	2719	3163	3557	3947	4373	4813
223	521	857	1213	1571	1973	2347	2729	3167	3559	3967	4391	4817
227	523	859	1217	1579	1979	2351	2731	3169	3571	3989	4397	4831
229	541	863	1223	1583	1987	2357	2741	3181	3581	4001	4409	4861

Основна література

1. Завало С.Т., Костарчук В.Н., Хацет Б.І . Алгебра і теорія чисел. В 2–х ч. –К.: Вища шк., 1974, 1977, 1980.
2. Завало С.Т. Курс алгебри. К.: Вища шк., 1985.
3. Курош А.Г. Курс высшей алгебры. М., Наука, 1971.
4. Ван дер Варден Б.Л. Алгебра. – М.: Наука, 1976.
5. Калужнин Л.А. Введение в общую алгебру. – М.: Наука, 1973.
6. Кострикин А.И. Введение в алгебру. – М.: Наука, 1977.
7. Скорняков Л.А. Элементы алгебры. – М.: Наука, 1965.
8. Фаддеев Д.К. Лекции по алгебре. – М.: Наука, 1984.
9. Фаддеев Д.К., Соминский И.С. Сборник задач по высшей алгебре. М.: Наука, 1977.
10. Проскуряков И.В. Сборник задач по линейной алгебре. – М.: Наука, 1965.