МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Івано-Франківський національний технічний університет нафти і газу

Кафедра вищої математики

С.І. Гургула

ВИБРАНІ ПИТАННЯ ЗАГАЛЬНОЇ АЛГЕБРИ

Навчальний посібник

Івано-Франківськ

2006

МВ 02070855 – 1812 - 2006

С.І. Гургула Вибрані питання загальної алгебри. Навчальний посібник. – Івано-Франківськ: Факел, 2006. – 99 с.

Розглядаються алгебраїчні структури з однією і двома бінарними операціями – групи, кільця, поля. Приділено увагу також таким структурам як півкільця, тіла, алгебри, модулі. Детально вивчаються важливі для практичних застосувань приклади. Викладено також основні факти теорії многочленів. Міститься достатня кількість вправ для самостійного розв'язування.

Посібник розрахований на студентів спеціальності "Програмне забезпечення".

Рецензенти:
канд. фіз.-мат. наук, доцент кафедри алгебри та геометрії Прикарпатського Національного Університету ім. Василя Стефаника Собкович Р.І.,
канд. техн. наук, доцент кафедри програмного забезпечення ІФНТУНГ Процюк В.Р.

Зміст

1 Множини з алгебраїчними операціями

1.1 Бінарні операції

Нехай X – довільна множина. Ми будемо говорити, що на множині X задана *бінарна алгебраїчна операція* (або *закон композиції*), якщо всякій впорядкованій парі (a,b) елементів $a,b \in X$ ставиться у відповідність однозначно визначений елемент тієї ж множини X. Як правило, бінарну операцію позначають яким-небудь спеціальним символом: $*, \cdot, \circ, +, \times$ і т. д. Часто операціям дають спеціальні назви – додавання, множення, віднімання і т. д. Ми теж будемо дотримуватись цієї традиції, називаючи $a \cdot b$ (або просто ab) *добутком*, а $a+b$ - *сумою* елементів $a,b \in X$. Зрозуміло, що ці назви в більшості випадків умовні.

На одній і тій же множині може бути задано, взагалі кажучи, багато різних операцій. Бажаючи виділити одну з них, використовують позначення $(X,*)$ і кажуть, що операція $*$ визначає на X *алгебраїчну структуру,* або що $(X,*)$ - *алгебраїчна система*. Так, наприклад, на множині цілих чисел $\mathbb{Z}$ крім природних операцій + (додавання) і $\cdot$ (множення) легко вказати і багато "похідних" операцій: $m \circ n = mn - m + n$, $m * n = -m - n$ і т. д. Ми, таким чином, одержуємо різні алгебраїчні структури $(\mathbb{Z},+), (\mathbb{Z},\cdot), (\mathbb{Z},\circ), (\mathbb{Z},*)$.

Поряд з бінарними операціями являють собою інтерес більш загальні n-арні операції (унарні при $n=1$, тернарні при $n=3$ і т. д.). Зв'язані з ними алгебраїчні структури складають спеціальну теорію універсальних алгебр. Для математики принципову важливість має один із розділів теорії універсальних алгебр – алгебраїчні структури з бінарними операціями. Зрозуміло чому – адже на практиці ми маємо справу найчастіше якраз із бінарними операціями.

При конструюванні різних бінарних операцій на множині X відкривається необмежений простір для фантазії. Але задача вивчення довільних алгебраїчних структур занадто загальна, щоб являти собою реальну цінність. Тому цю задачу розглядають при різних природних обмеженнях. Зауважимо,

що множина з однією визначеною в ній бінарною операцією називається *групоїдом*.

1.2 Півгрупи і моноїди

Бінарна операція $*$ на множині X називається асоціативною, якщо

$$(a*b)*c = a*(b*c)$$

для всіх $a,b,c \in X$; вона називається *комутативною*, якщо

$$a*b = b*a$$

для всіх $a,b \in X$. Такі ж назви присвоюються відповідній алгебраїчній структурі $(X,*)$. Вимоги асоціативності і комутативності є незалежними.

Елемент $e \in X$ називається *одиничним* (або *нейтральним*) відносно розглядуваної бінарної операції $*$, якщо

$$e*a = a*e = a$$

для всіх $a \in X$. Якщо припустити, що в X є ще один одичний елемент e', то, як випливає з означення,

$$e' = e'*e = e,$$

тобто в алгебраїчній структурі може існувати не більше одного одиничного елемента.

Множина X із заданою на ній бінарною асоціативною операцією називається *півгрупою*. Півгрупу з одиничним (нейтральним) елементом називають *моноїдом* (або просто *півгрупою з одиницею*). Моноїд, основна операція якого є множення, будемо називати *мультиплікативним* і позначати $(M,\cdot,e)$. Моноїд відносно операції додавання називається *адитивним*. В адитивному моноїді нейтральний елемент називається нулем і позначається 0, а сам адитивний моноїд позначається $(M,+,0)$. Адитивний запис використовується, як правило, в комутативних моноїдах.

Підмножина S' півгрупи S з операцією $*$ називається *підпівгрупою*, якщо $a*b \in S'$ для всіх $a,b \in S'$. Тоді кажуть ще, що підмножина $S' \subset S$ замкнена відносно операції $*$.

Якщо $(M,*)$ - моноїд, а підмножина $M' \subset M$ не тільки замкнена відносно операції $*$, але містить ще і нейтральний елемент, то M' називається *підмоноїдом* в M.

Наведемо деякі приклади півгруп і моноїдів.

1) Нехай Ω - довільна множина і $\mathbb{F}(\Omega)$ - множина всіх її підмножин. Оскільки для будь-яких підмножин A,B,C множини Ω виконуються рівності $A\cap(B\cap C)=(A\cap B)\cap C$ і $A\cup(B\cup C)=(A\cup B)\cup C$, то на $\mathbb{F}(\Omega)$ визначені дві природні асоціативні бінарні операції. Очевидно, що $\varnothing\cup A=A$ і $\Omega\cap A=A$. Ми маємо два комутативних моноїди $(\mathbb{F}(\Omega),\cap,\Omega)$ і $(\mathbb{F}(\Omega),\cup,\varnothing)$.

2) Нехай $M_n(\mathbb{R})$ - множина квадратних матриць n-го порядку з дійсними елементами. Тоді $(M_n(\mathbb{R}),+,0)$ - комутативний моноїд з нейтральним елементом – нульовою матрицею, а $(M_n(\mathbb{R}),\cdot,E)$ - некомутативний моноїд з нейтральним елементом – одиничною матрицею E.

3) Нехай $\mathbb{Z}$ - множина цілих чисел. Тоді $(\mathbb{Z},+,0)$ і $(\mathbb{Z},\cdot,1)$ - комутативні моноїди. Нехай $n\mathbb{Z}=\{nm \mid m\in\mathbb{Z}\}$ -множина цілих чисел, які діляться на n $(n>1)$. Очевидно $(n\mathbb{Z},+,0)$ - комутативний моноїд, який є підмоноїдом моноїда $(\mathbb{Z},+,0)$. А $(n\mathbb{Z},\cdot)$ - комутативна півгрупа без одиниці, яка є підпівгрупою в $(\mathbb{Z},\cdot)$.

1.3 Узагальнена асоціативність; степені

Нехай задана довільна алгебраїчна структура $(X,\cdot)$ з бінарною операцією $\cdot$, яку для простоти будемо опускати і писати ab (замість $a\cdot b$ і називати добутком). Нехай, далі, $a_1,a_2,...,a_n$ - впорядкована послідовність елементів із X . Не міняючи порядку, ми можемо багатьма різними способами складати добутки довжини n; наприклад, при $n=4$ одержуємо

$$(a_1a_2)(a_3a_4),\quad (a_1(a_2a_3))a_4,\quad ((a_1a_2)a_2)a_4\ ,$$

і т. д. Чи залежить результат від розставляння дужок? Виявляється, що в півгрупах (і моноїдах) розставляння дужок

є зайвим. Справедлива

Теорема 1.1. Якщо бінарна операція на X асоціативна, то результат її послідовного застосування до n елементів множини X не залежить від розставляння дужок.

Доведення проведемо методом математичної індукції. При $n=1,2$ доводити нічого, при $n=3$ твердження співпадає з означенням асоціативності. Тому припустимо, що $n>3$ і для числа елементів меншого n справедливість твердження встановлена. За цим припущенням кожен добуток, що складається з меншого ніж n числа множників, однозначно визначений. Доведемо, що тоді це твердження правильне і для n. Для цього доведемо, що для будь-якого натурального $k<n-1$ справедлива рівність

$$\left(a_1a_2\ldots a_k\right)\left(a_{k+1}a_{k+2}\ldots a_n\right)=\left(a_1a_2\ldots a_{k+1}\right)\left(a_{k+2}a_{k+3}\ldots a_n\right) \quad (1.1)$$

Справді, добутки $a_1a_2\ldots a_k$ і $a_{k+2}a_{k+3}\ldots a_n$ однозначно визначені. Нехай $a_1a_2\ldots a_k=b$, $a_{k+2}a_{k+3}\ldots a_n=c$, тоді $\left(a_1a_2\ldots a_k\right)\left(a_{k+1}a_{k+2}\ldots a_n\right)=b\left(a_{k+1}c\right)$,

$\left(a_1a_2\ldots a_{k+1}\right)\left(a_{k+2}a_{k+3}\ldots a_n\right)=\left(ba_{k+1}\right)c$. Але, в силу асоціативності $b\left(a_{k+1}c\right)=\left(ba_{k+1}\right)c$, і тим самим рівність (1.1) доведена.

З рівності (1.1) випливає, що для будь-яких натуральних k і l, менших n, має місце рівність

$$\left(a_1a_2\ldots a_k\right)\left(a_{k+1}a_{k+2}\ldots a_n\right)=\left(a_1a_2\ldots a_l\right)\left(a_{l+1}a_{l+2}\ldots a_n\right). \quad (1.2)$$

Справді, припустимо, що $l>k$, нехай $l=k+s$. Тоді, використовуючи рівність (1.1), одержуємо

$$\left(a_1a_2\ldots a_k\right)\left(a_{k+1}a_{k+2}\ldots .a_n\right)=\left(a_1a_2\ldots a_{k+1}\right)\left(a_{k+2}a_{k+3}\ldots a_n\right)=$$

$$=\left(a_1a_2\ldots a_{k+2}\right)\left(a_{k+3}a_{k+4}\ldots a_n\right)=\ldots=$$

$$=\left(a_1a_2\ldots a_{k+s-1}\right)\left(a_{k+s}a_{k+s+1}\ldots a_n\right)=\left(a_1a_2\ldots a_l\right)\left(a_{l+1}a_{l+2}\ldots a_n\right),$$

отже, рівність (1.2) доведено.

Припустимо, що в системі елементів $a_1,a_2,\ldots,a_n$ двома будь-якими способами розставлено дужки, які вказують, в якому порядку треба виконувати множення. Але при першому розставлянні дужок останнім кроком буде множення деякого добутку $a_1a_2\ldots a_k$ на добуток $a_{k+1}a_{k+2}\ldots a_n$ $\left(1\le k\le n-1\right)$.

При другому розставлянні дужок останнім кроком буде множення деякого добутку $a_1a_2...a_l$ на добуток $a_{l+1}a_{l+2}...a_n \quad (1 \le l \le n-1)$. Але в силу рівності (1.2) ці добутки рівні. Тобто, в обох випадках маємо той самий результат. Терему доведено.

Таким чином, при обчисленні добутку $a_1a_2...a_n$ елементів моноїда дужки зайві. Потрібно тільки слідкувати за порядком співмножників, та і то тільки в тому випадку, коли вони не всі перестановочні між собою. Зокрема, якщо $a_1 = a_2 = ... = a_n = a$, добуток $a \cdot a \cdot ... \cdot a$ позначають a^n і називають n-м *степенем елемента* a. Наслідком теореми 1.1 є співвідношення

$$a^m \cdot a^n = a^{m+n}, \qquad \left(a^m\right)^n = a^{mn}, \qquad m,n \in \mathbb{N}. \qquad (1.3)$$

В моноїді $(M,\cdot,e)$ для всякого $a \in M$ покладають ще $a^0 = e$.

В моноїді $(M,+,0)$ степеням відповідають *кратні* $na = a + a + ... + a$ елемента a. Співвідношення (1.3) тоді запишуться так:

$$ma + na = (m+n)a, \qquad n(ma) = (nm)a, \qquad m,n \in \mathbb{N}.$$

Зауважимо, що якщо a і b перестановочні: $ab = ba$, то

$$(ab)^n = a^n b^n, \qquad n = 0,1,2,... \qquad (1.4)$$

Зокрема, так буде завжди в комутативному моноїді. Рівність (1.4) доводиться індукцією по n:

$$(ab)^n = (ab)^{n-1}(ab) = \left(a^{n-1}b^{n-1}\right)(ab) = \left(a^{n-1}b^{n-1}a\right)b =$$
$$= \left(a^{n-1}ab^{n-1}\right)b = \left(a^{n-1}a\right)\left(b^{n-1}b\right) = a^n b^n.$$

Більш загально, якщо $a_i a_j = a_j a_i$, $1 \le i, j \le m$, то

$$\left(a_1a_2...a_m\right)^n = a_1^n a_2^n ... a_m^n.$$

Аналогічно в адитивному моноїді:

$$n(a+b) = na + nb \quad (\text{якщо } a+b = b+a), \qquad n = 0,1,2,...,$$

$$n\left(a_1 + a_2 + ... + a_m\right) = na_1 + na_2 + ... + na_m$$

(якщо $a_i + a_j = a_j + a_i$, $1 \le i, j \le m$), $\qquad n = 0,1,2,...$.

1.4 Оборотні елементи

Елемент a моноїда $(M,\cdot,e)$ називається *оборотним*, якщо знайдеться елемент $b\in M$ такий, що

$$ab=ba=e$$

(ясно, що елемент b теж буде оборотним). Якщо припустити, що для оборотного елемента a існує ще один елемент b' такий, що $ab'=b'a=e$, то

$$b'=eb'=(ba)b'=b(ab')=be=b.$$

Це дає підстави говорити просто про *обернений елемент* a^{-1} до (оборотного) елемента a:

$$aa^{-1}=a^{-1}a=e.$$

Зрозуміло, що $\left(a^{-1}\right)^{-1}=a$.

Доведемо, що якщо a і b - оборотні елементи, то їх добуток теж оборотний, причому $(ab)^{-1}=b^{-1}a^{-1}$. Справді,

$$(ab)\left(b^{-1}a^{-1}\right)=a\left(bb^{-1}\right)a^{-1}=aea^{-1}=aa^{-1}=e,$$

$$\left(b^{-1}a^{-1}\right)(ab)=b^{-1}\left(a^{-1}a\right)b=b^{-1}eb=b^{-1}b=e.$$

Враховуючи, що нейтральний елемент теж оборотний, очевидно $e^{-1}=e$, можна твердити, що множина всіх оборотних елементів моноїда $(M,\cdot,e)$ замкнена відносно операції $\cdot$ і утворює підмоноїд в M.

Вправи

1. Довести, що

$$M_n^0(\mathbb{R})=\left\{A=(a_{ij})\in M_n(\mathbb{R})\,\middle|\,\sum_{j=1}^{n}a_{ij}=0,\ \ i=1,2,...,n\right\}$$ -

півгрупа із звичайною операцією множення матриць. Чи є $\left(M_n^0(\mathbb{R}),\cdot\right)$ моноїдом?

2. Нехай M - мультиплікативний моноїд. Виберемо в ньому довільний елемент t і введемо нову операцію $*$: $x*y=xty$. Довести, що $(M,*)$ - півгрупа і що оборотність

елемента t в M - необхідна і достатня умова , при виконанні якої $(M,*)$ - моноїд з нейтральним елементом t^{-1}.

3. Довести, що множина $\mathbb{Z}$ з операцією $\circ$: $m \circ n = m + n + mn = (1+m)(1+n) - 1$ є комутативним моноїдом. Що є в $(\mathbb{Z},\circ)$ нейтральним елементом? Знайти в $(\mathbb{Z},\circ)$ всі оборотні елементи.

4. Довести, що як вироджені, так і невироджені матриці утворюють підпівгрупи півгрупи матриць відносно множення. Причому невироджені матриці утворюють навіть підмоноїд в моноїді $(M_n(\mathbb{R}),\cdot,E)$.

5. Розглянемо наступні операції на множинах

	Множина	Операція
1	Квадратні матриці порядку n	$A \circ B = AB + BA$
2	Квадратні матриці порядку n	$A \circ B = AB - BA$
3	Вектори простору	Векторний добуток
4	Додатні цілі числа	$m \circ n = m^n$
5	Невід'ємні цілі числа	$m \circ n = \min(m, n)$
6	Довільна	$x \circ y = x$

Які з цих операцій асоціативні чи комутативні? В яких випадках існують нейтральний елемент і обернені елементи?

6. На множині дійсних чисел визначимо операцію $x \circ y = 0$ для будь-яких x, y. Довести, що це півгрупа. Знайти всі її підпівгрупи.

7. На множині чотирьохвимірних рядків визначимо операцію

$$(a,b,c,d) \circ (s,t,u,v) = (a,b,u,v).$$

Довести, що це півгрупа і що всі її елементи є ідемпотентами (елемент f півгрупи називається *ідемпотентом*, якщо $f^2 = f$).

8. Довести, що множина всіх ідемпотентів комутативної півгрупи з одиницею є підпівгрупою.

9. Нехай $(M,\cdot,e)$ - моноїд. Довести, що якщо для якогось елемента a цього моноїда знайдеться елемент e_a, який задовольняє одній з умов $a\cdot e_a = a$ або $e_a \cdot a = a$, то обов'язково $e_a = e$.

10. Нехай $(M,\cdot,e)$ - моноїд. Довести, що якщо для якогось елемента a цього моноїда знайдеться елемент a', який задовольняє одній з умов $a'\cdot a = e$ або $a\cdot a' = e$, то обов'язково $a' = a^{-1}$.

11. Довести, що якщо $a_1, a_2, ..., a_n$ - оборотні елементи, то їх добуток теж оборотний, причому

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

2 Групи

2.1 Означення і приклади

Моноїд, всі елементи якого оборотні, називається *групою*. Іншими словами, множина G з визначеною на ній бінарною операцією (нехай вона зараз називається множенням) називається групою, якщо виконані умови:

1) операція є асоціативною: для будь-яких $a,b,c \in G$

$$a(bc) = (ab)c;$$

2) в множині G існує *одиничний* (*нейтральний*) елемент e такий, що для всякого $a \in G$

$$ae = ea = a;$$

3) для будь-якого $a \in G$ існує *обернений* елемент $a^{-1} \in G$ такий, що

$$aa^{-1} = a^{-1}a = e.$$

Умови 1), 2), 3) називаються аксіомами групи.

Далі ми будемо притримуватись в-основному наведеної вище "мультиплікативної" термінології. Але термін "множення" не потрібно розуміти буквально. Мова іде про будь-яку операцію, яка задовольняє даним аксіомам. Зокрема, в ряді випадків зручніше називати операцію додаванням і відповідно переформулювати аксіоми групи, користуючись "адитивною" термінологією:

1) додавання асоціативне: для будь-яких $a,b,c \in G$

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

2) існує *нульовий* елемент 0 такий, що для всякого $a \in G$

$$0 + a = a + 0 = a;$$

3) для всякого $a \in G$ існує *протилежний* елемент $-a$ такий, що

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

Операція, визначена в групі, називається *груповою операцією* або *груповим законом*.

Якщо групова операція є комутативною, то група називається *комутативною* або *абелевою*.

Група називається *скінченною*, якщо вона складається із скінченного числа елементів; в противному випадку група називається *нескінченною*. Число елементів скінченної групи називається її *порядком*.

Наведемо кілька прикладів груп.

1) Множина всіх цілих чисел відносно операції додавання – *адитивна група* всіх цілих чисел.
2) Множина всіх відмінних від нуля дійсних чисел – *мультиплікативна група* дійсних чисел.
3) Множина всіх векторів простору відносно операції додавання векторів.
4) Множина всіх невироджених матриць заданого порядку з дійсними елементами відносно операції множення матриць.
5) Множина всіх многочленів з дійсними коефіцієнтами відносно операції додавання многочленів.

Все це приклади нескінченних груп. Що ж стосується скінченних груп, то, якщо число елементів в такій групі невелике, множення в ній задається часто за допомогою *таблиці множення* (або *таблиці Келі*), в першому рядку і в першому стовпчику якої виписуються всі елементи групи, починаючи з одиничного, а потім на перетині рядка, де стоїть елемент a_i і стовпчика, де стоїть елемент a_j, записується елемент, який дорівнює добутку $a_i a_j$. Для прикладу розглянемо т. зв. *групу обертань* правильного трикутника.

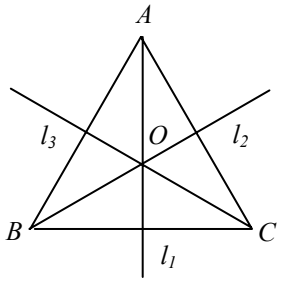

Рисунок 2.1

Таблиця 2.1

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Нехай A, B, C - вершини рівностороннього трикутника ABC (рис. 2.1). Повернемо трикутник навколо його центра O на $120°$ проти руху годинникової стрілки. Тоді вершина A перейде у вершину B, B в C і C в A. Таким чином, трикутним суміститься із своїм початковим положенням

(якщо не враховувати назви вершин), тобто поворот на $120°$ навколо точки O є перетворенням, яке переводить трикутник в себе. Позначимо це перетворення через a. Його можна записати у виді $a = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$, де у верхньому рядку записані всі вершини трикутника, а нижній рядок показує, куди кожна з них переходить. Поворот на $240°$ в тому ж напрямі навколо точки O теж є перетворенням, яке переводить трикутник в себе. Позначимо його b, тоді $b = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$. Є ще один поворот, який переводить трикутник в себе – це поворот на $0°$. Позначимо це перетворення через e, тоді $e = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$.

Нехай g_1 і g_2 - довільні перетворення трикутника. Тоді під $g_1 \cdot g_2$ (чи просто $g_1 g_2$) ми будемо розуміти перетворення g_3, яке одержиться, якщо спочатку виконати перетворення g_2, а потім перетворення g_1; g_3 будемо називати добутком або композицією перетворень g_2 і g_1. Можна скласти таблицю множення для обертань правильного трикутника, розглянутих вище (табл. 2.1). Неважко бачити, що обертання правильного трикутника утворюють комутативну групу. Справді, асоціативність і комутативність операції очевидна, роль нейтрального елемента виконує e; крім того, $a^{-1} = b, \quad b^{-1} = a$.

Всяке перетворення деякої фігури в себе, яке зберігає віддалі між всіма її точками називається *симетрією* даної фігури. Розглянуті вище обертання рівностороннього трикутника є, очевидно, його симетріями. Крім обертань, у рівностороннього трикутника є ще три симетрії, а саме, дзеркальні відображення відносно осей l_1, l_2 і l_3 (рис. 2.1). Ці перетворення позначимо відповідно c, d, f, так що

$c = \begin{pmatrix} A\ B\ C \\ A\ C\ B \end{pmatrix}$, $d = \begin{pmatrix} A\ B\ C \\ C\ B\ A \end{pmatrix}$, $f = \begin{pmatrix} A\ B\ C \\ B\ A\ C \end{pmatrix}$. Причому при розгляді композиції перетворень вважатимемо, що осі не зв'язані жорстко з фігурою і не перетворюються разом з нею. Пропонуємо самостійно скласти таблицю множення для всіх симетрій правильного трикутника і переконатись, що вони утворюють некомутативну групу.

2.2 Групи підстановок

Важливими прикладами скінченних груп є т. зв. *групи підстановок*.

Підстановкою n-го степеня називається взаємно-однозначне відображення множини натуральних чисел $\{1,2,...,n\}$ на себе, тобто таке відображення, при якому кожному числу від 1 до n відповідає якесь із цих чисел і двом різним числам завжди відповідають два різних числа. Всяка підстановка n-го степеня може бути записана у виді

$$\pi = \begin{pmatrix} 1\ 2\ ...\ n \\ i_1\ i_2\ ...\ i_n \end{pmatrix}, \qquad (2.1)$$

де $i_1, i_2, ..., i_n$ - якимось чином переставлені символи $1,2,...,n$. При цьому кажуть, що підстановка π переводить 1 в i_1, 2 в i_2 і т. д., n переводить в i_n, що записується ще так: $\pi(k) = i_k$, $k = 1,2,...,n$. Різні підстановки відрізняються одна від одної розташуванням символів в нижньому рядку, тому кількість підстановок n-го степеня дорівнює кількості перестановок із n елементів, тобто дорівнює $n!$ Підстановка

$$e = \begin{pmatrix} 1\ 2\ ...\ n \\ 1\ 2\ ...\ n \end{pmatrix},$$

яка залишає всі символи на місці, називається одиничною, або тотожною.

Підстановки множаться у відповідності до загального правила композиції відображень: $(\sigma\tau)(k) = \sigma(\tau(k))$. Наприклад, для підстановок

$$\sigma = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$$

маємо

$$\sigma\tau = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix}\begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix}.$$

В той же час

$$\tau\sigma = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}\begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,4\,1 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,1\,4 \end{pmatrix},$$

так що $\sigma\tau \neq \tau\sigma$.

Неважко переконатись, що множина всіх підстановок n-го степеня утворює групу відносно введеної вище операції множення. Справді, множення підстановок асоціативне:

$$\big(\sigma(\tau\pi)\big)(k) = \sigma\big((\tau\pi)(k)\big) = \sigma\big(\tau(\pi(k))\big),$$

$$\big((\sigma\tau)\pi\big)(k) = (\sigma\tau)\big(\pi(k)\big) = \sigma\big(\tau(\pi(k))\big)$$

для будь-якого $k = 1,2,...,n$. Тобто $\sigma(\tau\pi) = (\sigma\tau)\pi$ для будь-яких підстановок σ, τ, π. Роль нейтрального елемента виконує тотожна підстановка e. Оберненою до підстановки π, такої, що $\pi(k) = i_k$, $k = 1,2,...,n$, буде підстановка π^{-1}, така, що $\pi^{-1}(i_k) = k$, $k = 1,2,...,n$. Група підстановок n-го степеня називається *симетричною групою n-го степеня* і позначається S_n. При $n \geq 3$ група S_n некомутативна.

Нехай задана деяка перестановка чисел $1,2,...,n$. Кажуть, що в даній перестановці числа i і j складають *інверсію,* якщо $i > j$, але i стоїть в цій перестановці раніше j. Перестановка називається *парною*, якщо її символи складають парне число інверсій, і *непарною* – в противному випадку.

Підстановка (2.1) називається *парною*, якщо парною є перестановка , яка стоїть в її нижньому рядку, в противному випадку підстановка називається *непарною*. Тотожна підстановка, очевидно, є парною, оскільки кількість інверсій в перестановці, що стоїть в її нижньому рядку, дорівнює нулю.

Якщо в деякій перестановці поміняти місцями два символи (не обов'язково сусідні), а всі решта символи залишити на місці, то одержимо нову перестановку. Таке перетворення перестановки називається *транспозицією*. Очевидним є те, що від будь-якої перестановки можна перейти до будь-якої іншої за допомогою декількох транспозицій.

Доведемо, що транспозиція міняє парність перестановки. Справді, нехай транспонуються символи k і l. Якщо ці символи стоять поруч, тобто перестановка має вид $\ldots k\, l \ldots$, де крапками замінено ті символи, які не зачіпаються транспозицією, то твердження очевидне. Нехай тепер між символами, які транспонуються розташовані s символів, тобто перестановка має вид

$$\ldots k\, i_1\, i_2 \ldots i_s\, l \ldots . \qquad (2.2)$$

Очевидно, транспозицію елементів k і l можна одержати в результаті послідовного виконання $2s+1$ транспозиції сусідніх елементів. Отже, ми непарну кількість разів міняли парність перестановки, тому перестановка (2.2) і перестановка

$$\ldots l\, i_1\, i_2 \ldots i_s\, k \ldots \qquad (2.3)$$

мають протилежні парності.

Розглянемо тепер підстановки спеціального виду, які одержуються із тотожної підстановки e за допомогою однієї транспозиції в її нижньому рядку. Ці підстановки, очевидно, непарні; вони називаються *транспозиціями* і мають вид

$$\begin{pmatrix} \ldots k \ldots l \ldots \\ \ldots l \ldots k \ldots \end{pmatrix}, \qquad (2.4)$$

де крапками замінено символи, які залишаються на місці. Позначимо цю транспозицію $(k\ l)$. Якщо довільну підстановку

$$\begin{pmatrix} 1 \ldots k \ldots l \ldots n \\ i_1 \ldots i_k \ldots i_l \ldots i_n \end{pmatrix}$$

помножити справа на підстановку (2.4), тобто на транспозицію $(k\ l)$, то це зведеться до транспозиції символів i_k і i_l в нижньому рядку цієї підстановки. Оскільки всі перестановки можна одержати із однієї з них, наприклад із

$1\,2\ldots n$ послідовним виконанням транспозицій, то всяка підстановка може бути одержана із тотожної підстановки шляхом послідовного виконання декількох транспозицій в її нижньому рядку, тобто шляхом послідовного множення на підстановки виду (2.4). Можна твердити (опустивши множник e), що всяка підстановка представляється у виді добутку транспозицій. Причому всяку підстановку можна розкласти в добуток транспозицій багатьма різними способами. Наприклад

$$\begin{pmatrix}1\,2\,3\,4\,5\\2\,5\,4\,3\,1\end{pmatrix}=(1\,2)(2\,5)(3\,4)=(1\,5)(1\,2)(3\,4)=$$
$$=(2\,4)(1\,3)(1\,4)(3\,5)(2\,3).$$

При всіх розкладах підстановки в добуток транспозицій парність числа цих транспозицій буде одна і та ж, причому вона співпадатиме з парністю самої підстановки. Справді, твердження буде доведене, якщо ми доведемо, що добуток будь-яких k транспозицій є підстановка, парність якої співпадає з парністю числа k. При k=1 це вірно, оскільки транспозиція є непарна підстановка. Нехай твердження доведено для випадку k-1 множників. Тоді його справедливість для k множників випливає з того, що числа k-1 і k мають протилежні парності, а множення підстановки (в даному випадку – добутку k-1 співмножників) на транспозицію рівносильне виконанню цієї транспозиції в нижньому рядку підстановки, тобто міняє її парність.

Звідси безпосередньо випливає, що добуток двох підстановок однакової парності є парна, а добуток двох підстановок різної парності є непарна підстановка. Справді, представлення $\sigma\tau$ у виді добутку транспозицій ми одержимо, записавши відповідні розклади для σ і τ один за другим. Зрозуміло, що кількість співмножників, які при цьому одержуються дорівнює сумі кількостей співмножників, які є в розкладах σ і τ. Тоді легко бачити, що підстановки σ і σ^{-1} мають однакову парність, бо їх добуток є підстановка парна.

Якщо розглянути множину тільки парних підстановок n-го степеня, то із сказаного вище випливає, що вони утворюють групу відносно множення; порядок цієї групи дорівнює $n!/2$.

Ця група називається *знакозмінною групою n-го степеня*. Легко перевірити, що вона некомутативна при $n \geq 4$, хоча буде комутативною при $n = 3$.

Вправи

1. Довести, що аксіоми 1)-3) групи еквівалентні умовам:

1) операція є асоціативною;

2) для будь-яких двох елементів $a, b \in G$ існує рівно один такий елемент $x \in G$, що $ax = b$ і рівно один такий елемент $y \in G$, що $ya = b$.

2. Довести, що якщо $ab = ac$, а також, якщо $ba = ca$, то $b = c$.

3. Довести, що множина всіх парних цілих чисел утворює групу відносно операції додавання.

4. Довести, що множина всіх відмінних від нуля раціональних чисел утворює групу відносно операції множення.

5. Скласти таблицю множення для обертань квадрата. Переконатись, що одержана комутативна група.

6. Знайти всі симетрії квадрата і скласти для них таблицю множення. Чи комутативна одержана група?

7. Нехай $ABCD$ - ромб, який не є квадратом. Знайти всі його симетрії і скласти для них таблицю множення. Чи комутативна одержана група?

8. Нехай $ABCD$ - прямокутник, який не є квадратом. Знайти всі його симетрії і скласти для них таблицю множення. Чи комутативна одержана група?

9. Нехай $a \cdot a = e$ для будь-якого елемента a групи G. Довести, що група G комутативна.

10. Скласти таблицю множення для груп S_2 і S_3.

11. Визначити парність підстановок $\begin{pmatrix} 1\,2\,3\,4\,5 \\ 2\,5\,4\,1\,3 \end{pmatrix}$, $\begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 3\,5\,4\,1\,2\,6 \end{pmatrix}$. Розкласти їх в добуток транспозицій.

12. Які підстановки є оберненими до транспозицій?

13. Чи утворює групу множина непарних підстановок n-го степеня?

14. Транспозиції $(1\ 2), (2\ 3), ..., (n-1\ n)$ називаються елементарними. Довести, що довільну транспозицію можна представити у виді добутку елементарних.

15. Нехай $A, B \in M_n(\mathbb{R})$ і $(AB)^m = E$ для деякого цілого числа m. Чи вірно, що $(BA)^m = E$?

3 Підгрупи, циклічні групи, суміжні класи

3.1 Підгрупи

Підмножина $H \subset G$ групи G називається *підгрупою* цієї групи, якщо вона сама є групою відносно операції, визначеної в групі G.

Так, наприклад, адитивна група парних цілих чисел є підгрупою адитивної групи всіх цілих чисел, яка, в свою чергу, сама є підгрупою адитивної групи раціональних чисел. Мультиплікативна група додатних дійсних чисел є підгрупою мультиплікативної групи всіх відмінних від нуля дійсних чисел.

У всякій групі G підмножина, яка складається з одиничного елемента групи e є підгрупою, яка називається *одиничною підгрупою* групи G. Сама група G теж є своєю підгрупою. Будемо говорити, що підгрупа $H \subset G$ - *власна*, якщо $H \neq e$ і $H \neq G$.

Легко довести таке твердження: Якщо H_1 і H_2 - підгрупи групи G, то і їх перетин $H_1 \bigcap H_2$ теж буде підгрупою групи G.

Дійсно, якщо $a,b \in H_1 \bigcap H_2$, то $a,b \in H_1$, а тому $ab, a^{-1} \in H_1$ (див. вправу 2). За тими ж міркуваннями $ab,\ a^{-1} \in H_2$. А, значить, $ab,\ a^{-1} \in H_1 \bigcap H_2$. Одержаний результат справедливий, як легко бачити, для будь-якого сімейства підгруп, скінченного чи нескінченного.

3.2 Степені з будь-якими цілими показниками

Ми вже визначили a^n, якщо n - натуральне число. Від'ємні степені елемента a можна визначити або як елементи групи G, обернені до додатних степенів цього елемента, або як добуток співмножників, рівних елементу a^{-1}. В дійсності ці означення співпадають, тобто

$$\left(a^n\right)^{-1} = \left(a^{-1}\right)^n, \quad n > 0.$$

Справді, розглянемо добуток

$$a^n\left(a^{-1}\right)^n = \underbrace{a...aa}_{n}\underbrace{a^{-1}a^{-1}...a^{-1}}_{n} = \underbrace{a...a}_{n-1}\underbrace{a^{-1}...a^{-1}}_{n-1} = ...= aa^{-1} = e\ ,$$

тому $\left(a^n\right)^{-1} = \left(a^{-1}\right)^n$. Елемент, який дорівнює як лівій, так і правій частині останньої рівності позначимо через a^{-n}, тобто

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

Домовимося, нарешті, що $a^0 = e$.

Легко перевірити (рекомендуємо це зробити самостійно), що в будь-якій групі для степенів будь-якого елемента a при будь-яких показниках m і n, додатних, від'ємних чи нульових, виконані рівності

$$a^m \cdot a^n = a^n \cdot a^m = a^{m+n}, \tag{3.1}$$

$$\left(a^m\right)^n = a^{mn}. \tag{3.2}$$

3.3 Циклічні групи

Позначимо через $\langle a\rangle$ підмножину групи G, яка складається із всіх степенів елемента a. Неважко бачити, що $\langle a\rangle$ є підгрупою групи G (переконатись самостійно). Ця підгрупа називається *циклічною підгрупою групи* G, *породженою елементом* a. Як видно з рівності (3.1) вона завжди комутативна, навіть якщо група G і некомутативна.

Якщо всі степені елемента a різні, то елемент a називається *елементом нескінченного порядку*. Нехай серед степенів елемента a є рівні: $a^m = a^n$ при $m \neq n$. Це завжди має місце в скінченних групах, але може статись і в нескінченній групі. Якщо $m > n$, то $a^{m-n} = e$, тобто існують додатні степені елемента a, рівні одиничному елементу. Нехай q - найменший додатний показник, для якого $a^q = e$.

В цьому випадку кажуть, що a - *елемент скінченного порядку* q. Зрозуміло, що в скінченній групі всі елементи мають скінченний порядок.

Якщо елемент a має скінченний порядок q, то всі елементи

$$e, a, a^2, ..., a^{q-1}, \tag{3.3}$$

як легко бачити, будуть різними. Всякий інший степінь елемента a, додатний чи від'ємний, дорівнює одному з елементів (3.3). Тобто можна сказати, що

$$\langle a \rangle = \left\{ e, a, a^2, ..., a^{q-1} \right\}.$$

Справді, будь-яке ціле число k можна подати у виді

$$k = lq + r, \quad 0 \le r \le q - 1,$$

тоді

$$a^k = a^{lq+r} = a^{lq} \cdot a^r = \left(a^q \right)^l \cdot a^r = e^l \cdot a^r = a^r.$$

Зокрема, якщо $a^k = e$, то $a^r = e$, тобто $r = 0$, значить $k = lq$.

Зауважимо, що всяка група містить один-єдиний елемент першого порядку – це буде одиничний елемент e. Циклічна підгрупа $\langle e \rangle$ співпадає з одиничною підгрупою.

Група G називається *циклічною групою*, якщо вона складається із степенів одного із своїх елементів a, тобто співпадає із однією із своїх циклічних підгруп $\langle a \rangle$. Елемент a при цьому називається *твірним елементом* групи G. Всяка циклічна група, очевидно, абелева.

Наприклад, адитивна група цілих чисел є нескінченна циклічна група з твірним елементом 1 (або –1). Прикладом скінченної циклічної групи порядку n може служити мультиплікативна група коренів n-го степеня із 1. Як відомо, всі ці корені є степенями одного з них.

3.4 Суміжні класи за підгрупою; теорема Лагранжа

Нехай M і N - підмножини групи G. Під *добутком* MN цих *підмножин* ми будемо розуміти сукупність тих елементів групи G, які хоча б одним способом можна представити у виді добутку деякого елемента із M на деякий елемент із N. Із асоціативності групової операції випливає асоціативність множення підмножин групи:

$$\left(MN\right)P = M\left(NP\right).$$

Одна із підмножин може складатись лише із одного елемента a. В цьому випадку ми одержуємо добуток aN елемента a на підмножину N, або добуток Ma підмножини M на елемент a.

Нехай H - підгрупа групи G і g - будь-який елемент групи G. *Лівим суміжним класом* групи G за підгрупою H, породженим елементом g, називається добуток gH, тобто сукупність елементів виду gh, де h пробігає всі елементи підгрупи H. Зрозуміло, що сам елемент g міститься в суміжному класі gH, оскільки $g = ge$, а $e \in H$.

Всякий лівий суміжний клас породжується будь-яким із своїх елементів, тобто якщо $g_1 \in gH$, то

$$gH = g_1H. \qquad (3.4)$$

Дійсно, g_1 можна представити у виді $g_1 = ga$, $a \in H$. Тоді для будь-яких елементів a' і a'' із H матимемо $g_1a' = \left(ga\right)a' = g\left(aa'\right)$, $ga'' = \left(g_1a^{-1}\right)a'' = g_1\left(a^{-1}a''\right)$, чим і доводиться рівність (3.4).

Звідси випливає, що два будь-яких лівих суміжних класи групи G за підгрупою H або співпадають, або не мають ні одного спільного елемента. Дійсно, якщо припустити, що два класи g_1H і g_2H мають спільний елемент g_3, то

$$g_1H = g_3H = g_2H\ .$$

Отже, група G розкладається на ліві суміжні класи за підгрупою H, що не перетинаються. Цей розклад називається *лівостороннім розбиттям групи* G *за підгрупою* H. Зауважимо, що одним із суміжних класів є сама підгрупа H, цей суміжний клас породжується, наприклад, елементом e. Очевидно, це єдиний суміжний клас, який є підгрупою; ніякий інший суміжний клас підгрупою не є.

Зрозуміло, що називаючи *правим суміжним класом* групи G за підгрупою H, породженим елементом g, добуток Hg, ми аналогічно одержали б *правостороннє розбиття групи* G *за підгрупою* H. Для абелевої групи, зрозуміло, її лівостороннє і правостороннє розбиття за всякою підгрупою будуть співпадати, тобто можна говорити просто про *розклад групи за підгрупою*.

Так, наприклад, розклад адитивної групи цілих чисел за підгрупою чисел, кратних натуральному числу k, складається із k різних суміжних класів, які породжуються відповідно числами $0,1,2,...,k-1$. При цьому в класі, породженому числом l, $0 \le l \le k-1$, зібрані всі ті числа, які при діленні на k дають остачу l.

Ще один приклад. В симетричній групі третього степеня S_3 позначимо

$$e = \begin{pmatrix} 1\,2\,3 \\ 1\,2\,3 \end{pmatrix},\quad \pi_1 = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix},\quad \pi_2 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix},$$

$$\pi_3 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix},\ \pi_4 = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix},\ \pi_5 = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}$$

і візьмемо підгрупу H, яка складається із елементів e і π_5. Тоді при лівосторонньому розкладі групи S_3 за підгрупою H

одержуються класи: 1) $\{e, \pi_5\}$ (суміжний клас $eH = H$), 2) $\{\pi_1, \pi_3\}$ (суміжний клас $\pi_1 H$), 3) $\{\pi_2, \pi_4\}$ (суміжний клас $\pi_2 H$). А при правосторонньому розкладі одержаться класи: 1) $\{e, \pi_5\}$ (суміжний клас $He = H$), 2) $\{\pi_1, \pi_4\}$ (суміжний клас $H\pi_1$), 3) $\{\pi_2, \pi_3\}$ (суміжний клас $H\pi_2$).

Теорема 3.1. (Лагранжа) У всякій скінченній групі порядок довільної її підгрупи є дільником порядку групи.

Доведення. Нехай G - скінченна група порядку n, а H - її підгрупа порядку k. Розглянемо лівосторонній розклад групи G за підгрупою H. Нехай він складається з j класів; число j називається *індексом* підгрупи H в групі G

$$G = H \cup g_1 H \cup g_2 H \cup ... \cup g_{j-1} H. \qquad (3.5)$$

Кожний лівий клас $g_i H$ складається з k елементів, бо якщо $g_i h_1 = g_i h_2$, де $h_1, h_2 \in H$, то $h_1 = h_2$. Отже, з розкладу (3.5) випливає, що

$$n = kj, \qquad (3.6)$$

що і потрібно було довести.

Наслідок 1. Порядок кожного елемента скінченої групи є дільником порядку групи.

Справді, порядок елемента a в групі G співпадає з порядком породжуваної ним підгрупи, а тому, за теоремою Лагранжа, є дільником порядку групи.

Наслідок 2. Кожна скінченна група, порядок якої – просте число, є циклічною.

Дійсно, ця група повинна співпадати з циклічною підгрупою, породженою будь-яким її елементом, відмінним від одиничного.

Вправи

1. Нехай H - підгрупа G. Довести, що: а) одиничні елементи в G і H співпадають; б) якщо a -елемент підгрупи H, то елементи, обернені до a в G і H співпадають.

2. Для того, щоб підмножина H була підгрупою групи G необхідно і достатньо, щоб виконувались дві умови:

1) разом з кожними двома елементами a, b H містить також їх добуток ab;
2) разом з кожним елементом a H містить також обернений елемент a^{-1}.

Довести.

3. Довести, що умови 1) і 2) попередньої вправи еквівалентні такій одній умові: для будь-яких елементів a, b із H добуток ab^{-1} також належить H .

4. Дати означення порядку елемента і циклічної групи в "адитивній" термінології.

5. Довести, що всяка підгрупа циклічної групи циклічна.

6. Довести, що сукупність цілих чисел, кратних натуральному числу k є підгрупою адитивної групи цілих чисел.

7. Знайти порядки всіх елементів в групах симетрій рівностороннього трикутника, квадрата і ромба.

8. Довести, що всі повороти площини (без перевертань), які переводять правильний n-кутник в себе, утворюють циклічну групу порядку n.

9. Знайти всі твірні елементи в групах обертань правильного трикутника і квадрата.

10. Довести, що група G парного порядку обов'язково містить елемент $g \neq e$ порядку 2.

11. Нехай елемент a має простий порядок p і m - довільне ціле число. Довести, що або $a^m = e$, або a^m має порядок p.

12. Нехай найбільший спільний дільник натуральних чисел m і n дорівнює d і елемент a має порядок n. Довести, що елемент a^m має порядок n/d.

13. Нехай a - елемент нескінченного порядку. Довести, що елементи $...a^{-2}, a^{-1}, a^0 = e, a, a^2, ...$ всі різні.

14. Знайти всі підгрупи в групах симетрій правильного трикутника і квадрата.

15. Знайти всі підгрупи в циклічних групах п'ятого, восьмого і п'ятнадцятого порядків.

16. Довести, що всі підгрупи циклічної групи порядку n мають вид

$$\left\{ e, a^d, a^{2d}, ..., a^{\left(\frac{n}{d}-1\right)d} \right\},$$

де a - твірний елемент групи і d - дільник n.

17. Довести, що всі підгрупи нескінченної циклічної групи мають вид

$$\left\{ ..., a^{-2r}, a^{-r}, e, a^r, a^{2r}, ... \right\},$$

де a - твірний елемент, а r - довільне натуральне число.

18. Довести, що у всякої нескінченної групи нескінченно багато підгруп.

19. Побудувати лівосторонній і правосторонній розклад групи симетрій правильного трикутника за підгрупою: а) обертань $\{e, a, b\}$; б) відображень відносно одної осі $\{e, c\}$.

20. Група G не містить підгруп, відмінних від G і від одиничної тоді і тільки тоді, коли вона містить p елементів, де p - просте число, або 1.

21. Довести, що елементи ab і ba мають однакові порядки.

4 Нормальні дільники, фактор-групи

4.1 Нормальні дільники

Підгрупа H групи G називається *нормальним дільником* цієї групи (або *інваріантною* чи *нормальною підгрупою*), якщо лівосторонній розклад групи G за підгрупою H співпадає з правостороннім.

Таким чином, всі підгрупи абелевої групи є в ній нормальними дільниками. З другого боку, у всякій групі G одинична підгрупа і сама ця група будуть нормальними дільниками: обидва розклади групи G за одиничною підгрупою співпадають з розкладом групи на окремі елементи, обидва розклади групи G за самою цією групою складаються з одного класу G.

Вкажемо ще деякі приклади нормальних дільників. В симетричній групі n-го степеня S_n знакозмінна група n-го степеня A_n буде нормальним дільником. Справді, група A_n має порядок $n!/2$, тому всякий суміжний клас групи S_n за підгрупою A_n повинен містити стільки ж елементів і, таким чином, такий клас є ще тільки один, а саме сукупність всіх непарних підстановок.

В мультиплікативній групі невироджених квадратних матриць порядку n матриці, визначник яких дорівнює 1, утворюють підгрупу, яка буде нормальним дільником (переконатись самостійно).

Означенню нормального дільника можна надати виду:

Підгрупа H групи G називається нормальним дільником цієї групи, якщо для всякого елемента $g \in G$

$$gH = Hg, \tag{4.1}$$

тобто для будь-якого елемента $g \in G$ і елемента $a \in H$ можна вказати в H такі елементи a' і a'', що

$$ga = a'g, \qquad ag = ga''. \tag{4.2}$$

Справді, якщо виконано (4.1), то H буде, очевидно, нормальним дільником. Навпаки, якщо співпадають лівосторонній і правосторонній розклади групи G за підгрупою H, тобто для будь-якого g знайдеться g_1 таке, що $gH = Hg_1$, то враховуючи, що $g \in gH$ і $Hg_1 = Hg$, маємо $gH = Hg$.

Можна вказати і інші означення нормального дільника, еквівалентні наведеним вище. Так, назвемо елементи a і b групи G *спряженими*, якщо в G існує хоча б один такий елемент g, що

$$b = g^{-1}ag \ , \qquad (4.3)$$

тобто, як кажуть, елемент b одержується із елемента a *трансформуванням* елементом g. Із (4.3) випливає, очевидно, рівність

$$a = gbg^{-1} = \left(g^{-1}\right)^{-1} bg^{-1},$$

тобто тоді елемент a одержується із елемента b трансформуванням елементом g^{-1}.

Підгрупа H групи G буде нормальним дільником в G тоді і тільки тоді, коли разом з будь-яким своїм елементом вона містить і всі елементи, спряжені з ним в G.

Справді, якщо H - нормальний дільник, то згідно з (4.2) для елемента $a \in H$ і будь-якого елемента $g \in G$ існує елемент $a'' \in H$ такий, що $ag = ga''$. Звідси $g^{-1}ag = a''$, тобто всякий елемент, спряжений з a, міститься в H. Навпаки, якщо підгрупа H містить разом із всяким своїм елементом a і всі елементи, спряжені з ним, то в H міститься, зокрема, елемент $g^{-1}ag = a''$, звідки випливає друга з рівностей (4.2). З тієї ж причини в H міститься і елемент $\left(g^{-1}\right)^{-1} ag^{-1} = gag^{-1} = a'$, звідки випливає перша з

рівностей (4.2).

Використовуючи цей результат легко довести, що перетин нормальних дільників групи G буде нормальним дільником цієї групи (самостійно).

4.2 Фактор-групи

Нехай H - нормальний дільник групи G. В цьому випадку добуток двох суміжних класів G за H теж буде суміжним класом за H. Справді, зауваживши спочатку, що

$$H \cdot H = H \tag{4.4}$$

для будь-якої підгрупи H групи G, і використовуючи асоціативність множення підмножин групи, а також рівність (4.1), ми для будь-яких елементів $g_1, g_2 \in G$ одержимо

$$g_1 H \cdot g_2 H = g_1 \left(H g_2 \right) H = g_1 g_2 HH = g_1 g_2 H . \tag{4.5}$$

Рівність (4.5) показує, що для того, щоб знайти добуток двох даних суміжних класів групи G за нормальним дільником H, потрібно довільним чином вибрати в цих класах по одному представнику і взяти той суміжний клас, в якому лежить добуток цих представників. Пропонуємо самостійно переконатись, що добуток цих представників попадає завжди в один і той же клас суміжності.

Отже, в множині всіх суміжних класів групи за нормальним дільником визначена операція множення. Неважко бачити, що при цьому виконуються всі вимоги, які входять в означення групи. Справді, асоціативність множення суміжних класів випливає із асоціативності множення підмножин групи. Роль одиниці виконує сам нормальний дільник H, який є одним із суміжних класів, саме для будь-якого $g \in G$ маємо

$$gH \cdot H = gH , \qquad H \cdot gH = gHH = gH .$$

Нарешті, для суміжного класу gH оберненим буде клас $g^{-1}H$, оскільки

$$gH \cdot g^{-1}H = gg^{-1}HH = eH = H .$$

Побудована таким чином група називається *фактор-групою* групи G за нормальним дільником H і позначається G/H.

Зауважимо, що всяка фактор-група G/H абелевої групи G сама є абелевою, оскільки

$$g_1H \cdot g_2H = g_1g_2H = g_2g_1H = g_2H \cdot g_1H .$$

Крім того, всяка фактор-група G/H циклічної групи G сама циклічна. Справді, якщо $G = \langle a \rangle$, то для будь-якого суміжного класу gH існує таке ціле число k, що $g = a^k$ і тому

$$gH = a^kH = \left(aH\right)^k .$$

Порядок будь-якої фактор-групи G/H скінченної групи G є дільником порядку самої групи G. Дійсно, порядок фактор-групи дорівнює індексу нормального дільника H в групі G. Отже, можна скористатись рівністю (3.6).

Вправи

1. Нехай n - порядок групи G, m - порядок підгрупи H і $m = n/2$. Довести, що H є нормальним дільником в G.

2. Довести, що підгрупа обертань є нормальним дільником в групі симетрій правильного трикутника, а підгрупа $\{e, c\}$ (див. п. 2) нормальним дільником не є.

3. Множина елементів групи G, перестановочних з усіма елементами групи, називається *центром* групи G. Довести, що центр – підгрупа і, більше того, нормальний дільник групи G.

4. Довести, що множина матриць виду λE, $\lambda \neq 0$, є нормальним дільником в мультиплікативній групі невироджених матриць заданого порядку.

5. Довести, що центр симетричної групи S_n складається із одної тотожної підстановки.

6. Довести, що центр групи невироджених матриць заданого порядку співпадає з множиною матриць виду λE, $\lambda \neq 0$.

7. Довести, що в мультиплікативній групі всіх невироджених квадратних матриць n-го порядку множина матриць, визначник яких дорівнює 1, є нормальним дільником. Побудувати відповідну фактор-групу.

8. Дати означення нормального дільника і фактор-групи в "адитивній" термінології.

9. Побудувати фактор-групу адитивної групи цілих чисел за підгрупою цілих чисел, кратних деякому натуральному числу k.

10. Побудувати фактор-групу мультиплікативної групи всіх відмінних від нуля раціональних чисел за нормальним дільником, який складається з чисел 1 і –1.

11. Нехай G - адитивна група всіх векторів площини, які виходять з початку координат, H - її підгрупа, яка складається з усіх векторів, які лежать на осі ординат. Довести, що H - нормальний дільник. Як влаштовані суміжні класи фактор-групи G/H ?

12. Довести, що коли множина суміжних класів, на які група G розкладається за якимось своїм дільником H, є група , то H є нормальний дільник в G.

5 Морфізми груп

5.1 Гомоморфізми

Для подальшого важливим буде поняття *відображення* (або *функції*). При даних множинах X і Y відображення f з областю визначення X і областю значень Y ставить у відповідність кожному елементу $x \in X$ однозначно визначений елемент $y \in Y$, який позначається ще символом $f(x)$: $y = f(x)$. При цьому елемент y називається *образом* елемента x при відображенні f. Символічно відображення записується у виді

$$f: X \to Y \text{ або } X \xrightarrow{f} Y.$$

Сукупність всіх елементів множини Y, які є образом хоча б одного елемента $x \in X$ позначається $f(X)$. Зрозуміло, що $f(X) \subset Y$; якщо ж $f(X) = Y$, то відображення f називають *сюр'єктивним*, або *відображенням на*. Відображення f називається *ін'єктивним*, якщо із $x \neq x'$ випливає $f(x) \neq f(x')$. Нарешті, відображення $f: X \to Y$ називається *бієктивним,* або *взаємно однозначним*, якщо воно одночасно сюр'єктивне і бієктивне. У випадку, коли $Y = X$ говорять ще про перетворення множини X в себе.

Нехай тепер задано дві групи G і G' з груповими операціями відповідно $*$ і $\circ$. Відображення $f: G \to G'$ групи G в групу G' називається *гомоморфізмом* або *гомоморфним відображенням*, якщо для будь-яких $a, b \in G$

$$f(a * b) = f(a) \circ f(b).$$

При цьому кажуть, що гомоморфізм – це відображення, яке зберігає операцію. Гомоморфне відображення групи в себе називається ще її *ендоморфізмом*.

Теорема 5.1. Якщо f - гомоморфізм групи G в групу G' і e і a - відповідно нейтральний і довільний елементи групи G, e' - нейтральний елемент групи G', то

$$f(e)=e',\quad f(a^{-1})=f(a)^{-1}. \tag{5.1}$$

Доведення. Маємо для будь-якого $a\in G$: $f(a)=f(a*e)=f(a)\circ f(e)$. Звідси видно, що $f(e)$ - нейтральний елемент групи G', тобто $f(e)=e'$ (див. також вправу 9 п.1). Далі, $e'=f(e)=f(a*a^{-1})=f(a)\circ f(a^{-1})$. Звідси одержуємо $f(a^{-1})=f(a)^{-1}$. Теорему доведено.

Із доведеної теореми легко одержати такий наслідок. Якщо f - гомоморфізм групи G в групу G',то $f(G)$ - підгрупа групи G' (самостійно).

Сукупність всіх елементів групи G, які при гомоморфізмі $f: G\to G'$ відображаються в нейтральний елемент групи G' називається *ядром* гомоморфізму f і позначається $Kerf$.

Теорема 5.2. Ядро всякого гомоморфізму групи G є нормальним дільником групи G.

Доведення. Дійсно, якщо $a,b\in Kerf$, тобто $f(a)=e',\ f(b)=e'$, то (ми тепер опускаємо знаки $*$ і $\circ$)

$$f(ab)=f(a)f(b)=e'e'=e',$$

тобто $ab\in Kerf$. З другого боку, якщо $a\in Kerf$, то

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

отже $a^{-1}\in Kerf$. Тому $Kerf$ - підгрупа групи G. Нарешті, якщо $a\in Kerf$, g - довільний елемент групи G, то

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

отже $g^{-1}ag\in Kerf$. Тобто, разом з елементом a ядро гомоморфізму містить і всі елементи, спряжені з ним; воно буде, таким чином, нормальним дільником групи G. Теорему доведено.

Нехай тепер H - довільний нормальний дільник групи G. Розглянемо відображення, яке ставить у відповідність всякому елементу g групи G той суміжний клас gH за нормальним

дільником H, в якому цей елемент лежить. Ми одержимо відображення групи G на всю фактор-групу G/H. Неважко перевірити, що одержане відображення буде гомоморфізмом, причому ядром цього гомоморфізму буде сам нормальний дільник H (самостійно). Одержаний гомоморфізм називається *природним гомоморфізмом* групи G на фактор-групу G/H.

Звідси випливає, що нормальні дільники групи G і тільки вони можуть бути ядрами гомоморфізмів цієї групи.

Наведемо приклад гомоморфного відображення. Нехай $\mathbb{Z}$ - адитивна група всіх цілих чисел, G_m - циклічна група порядку m з твірним елементом a. Відображення $f: \mathbb{Z} \to G_m$ будуємо так: $f(n) = a^r$, де r - остача від ділення n на m, тобто $n = mq + r,\ 0 \le r \le m-1$. Нехай $n_1, n_2 \in \mathbb{Z}$ і r - остача від ділення $n_1 + n_2$ на m. Тоді $f(n_1 + n_2) = a^r$, з другого боку $a^{n_1} \cdot a^{n_2} = a^{n_1+n_2} = a^r$ (див. п. 3). Отже, $f(n_1 + n_2) = f(n_1) \cdot f(n_2)$, що свідчить про те, що відображення f є гомоморфізмом. Очевидно $f(n) = e$ тоді і тільки тоді, коли $n = mq$. Таким чином, ядром побудованого гомоморфізму є підгрупа цілих чисел, кратних m.

5.2 Ізоморфізми

Якщо гомоморфне відображення $f: G \to G'$ бієктивне (взаємно-однозначне), то воно називається *ізоморфним* або *ізоморфізмом*; при цьому групи G і G' називаються *ізоморфними*. Факт ізоморфізму груп часто позначається символічно $G \cong G'$.

Неважко довести таке твердження: для того, щоб гомоморфізм f групи на групу був ізоморфізмом необхідно і достатньо, щоб ядро цього гомоморфізму складалось із одного нейтрального елемента групи G (самостійно).

Якщо дві групи ізоморфні, то ізоморфну відповідність між ними можна встановити різними способами. Ізоморфні групи можуть відрізнятись одна від одної тільки природою своїх елементів і, може, назвою операції, визначеної в групі. Але всі

властивості ізоморфних між собою груп, які випливають із властивостей визначених в них операцій, і не залежні від природи елементів групи, однакові. Наприклад, якщо група абелева, то всі ізоморфні їй групи теж абелеві. В алгебрі ізоморфні одна одній групи не вважаються суттєво різними. Можна вважати їх екземплярами одної і тої ж групи.

Розглянемо дві групи: мультиплікативну групу всіх додатних дійсних чисел і адитивну групу всіх дійсних чисел. Ставлячи у відповідність додатному числу a дійсне число $\ln a$, ми одержимо взаємно однозначне відображення першої групи на другу, яке буде ізоморфізмом в силу рівності

$$\ln(ab) = \ln a + \ln b.$$

Ізоморфне відображення групи на себе називається *автоморфізмом* цієї групи.

5.3 Теорема про гомоморфізми

Виявляється, що всі групи, на які група G може гомоморфно відображатись, по суті вичерпуються її фактор-групами, а всі гомоморфізми групи G - її природними гомоморфізмами на свої фактор-групи. Точніше, справедлива наступна

Теорема 5.3. (про гомоморфізми). Нехай дано гомоморфізм f групи G на групу G' і нехай H - ядро цього гомоморфізму. Тоді група G' ізоморфна фактор-групі G/H, причому існує таке ізоморфне відображення φ першої з цих груп на другу, що результат послідовного виконання відображень f і φ співпадає з природним гомоморфізмом групи G на фактор-групу G/H.

Доведення. Нехай g' - довільний елемент групи G', а $g \in G$ - такий елемент, що $f(g) = g'$. Нехай $a \in H$, тобто $f(a) = e'$, тоді

$$f(ga) = f(g) \cdot f(a) = g'e' = g',$$

тобто всі елементи суміжного класу gH відображаються в елемент g'. З другого боку, якщо g_1 - будь-який елемент групи G, такий що $f(g_1) = g'$, то

$$f\left(g^{-1}g_1\right)=f\left(g^{-1}\right)f\left(g_1\right)=f\left(g\right)^{-1}f\left(g_1\right)=\left(g'\right)^{-1}g'=e',$$

тобто $g^{-1}g_1$ міститься в ядрі H гомоморфізму f. Якщо покласти $g^{-1}g_1=a$, то $g_1=ga$, тобто елемент g_1 міститься в суміжному класі gH. Отже, збираючи всі ті елементи, групи G, які при гомоморфізмі f відображаються в фіксований елемент g' групи G', ми одержуємо суміжний клас gH.

Відповідність φ, яка співставляє кожному $g'\in G'$ той суміжний клас групи G за нормальним дільником H, який складається із всіх елементів групи G, що гомоморфізмом f відображаються в g', буде взаємно однозначним відображенням групи G' на фактор-групу G/H. Це відображення буде ізоморфізмом, оскільки, якщо $\varphi\left(g'\right)=gH$, $\varphi\left(g_1'\right)=g_1H$, тобто $f\left(g\right)=g'$, $f\left(g_1\right)=g_1'$, то $f\left(gg_1\right)=f\left(g\right)f\left(g_1\right)=g'g_1'$ і тому $\varphi\left(g'g_1'\right)=gg_1H=gH\cdot g_1H=\varphi\left(g'\right)\varphi\left(g_1'\right)$. Нарешті, якщо g - довільний елемент групи G і $f\left(g\right)=g'$, то $\varphi\left(f\left(g\right)\right)=\varphi\left(g'\right)=gH$. Тобто послідовне виконання гомоморфізму f і ізоморфізму φ насправді відображає елемент g в породжуваний ним суміжний клас gH. Теорему доведено.

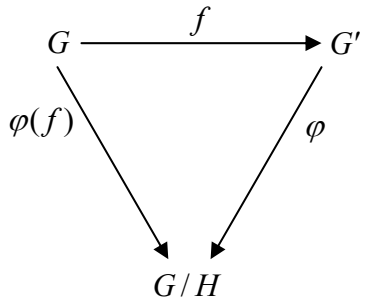

Рисунок 5.1

Щойно отриманий результат можна зобразити наступною діаграмою (див. рис. 5.1).

Вправи

1. Нехай $f : G \to G'$ - гомоморфізм групи G на групу G'. Якщо група G комутативна, то G' теж комутативна. Довести. Чи вірне обернене твердження?

2. Нехай $f_1 : G \to F$ і $f_2 : F \to H$ - гомоморфізми груп. Довести, що $f_2 f_1 : G \to H$ - теж гомоморфізм.

3. Довести, що образ підгрупи H групи G при гомоморфізмі $f : G \to G'$ є підгрупою в групі G'.

4. Нехай $f : G \to G'$ - гомоморфізм і H' - підгрупа групи G'. Довести, що $f^{-1}\left(H'\right)$ - підгрупа групи G (під $f^{-1}\left(H'\right)$ ми розуміємо підмножину G таку, що $f\left(f^{-1}\left(H'\right)\right) = H'$).

5. Нехай H - нормальний дільник в G і $f : G \to G'$ - гомоморфізм групи на групу G'. Довести, що $f\left(H\right)$ - нормальний дільник в G'.

6. Нехай H' - нормальний дільник в G' і $f : G \to G'$ - гомоморфізм. Довести, що $f^{-1}\left(H'\right)$ - нормальний дільник в G.

7. Довести, що не існує гомоморфного відображення адитивної групи всіх раціональних чисел на групу всіх цілих чисел.

8. Нехай G - мультиплікативна група додатних раціональних чисел і H - множина всіх раціональних чисел, які представляються у виді відношення двох додатних непарних чисел. Довести, що H - підгрупа групи G і що фактор-група G/H ізоморфна адитивній групі всіх цілих чисел.

9. Довести, що всі групи порядку 2 ізоморфні між собою.

10. Довести, що всі групи порядку 3 ізоморфні між собою.

11. Нехай H - підгрупа групи G і g - якийсь елемент G. Довести, що $g^{-1}Hg$ - теж підгрупа G, ізоморфна H.

12. Нехай $f : G \to G'$ - ізоморфізм і $f\left(g\right) = g'$. Довести, що елементи g і g' мають однакові порядки.

13. Довести, що адитивна група всіх цілих чисел ізоморфна адитивній групі всіх парних чисел.

14. Нехай G - група і $g \in G$. На множині G визначимо операцію $\circ$, поклавши $x \circ y = xgy$. Довести, що множина G з цією операцією є групою і що відображення $f : G \to G$, де $f\left(x\right) = xg^{-1}$, є ізоморфізмом старої групи на нову.

15. Нехай G - мультиплікативна група всіх невироджених матриць n-го порядку, H - нормальний дільник цієї групи, який складається з усіх матриць, визначник яких дорівнює 1 (див. вправу 7 п. 4). Довести, що фактор-група G/H ізоморфна мультиплікативній групі всіх відмінних від нуля дійсних чисел.

16. Нехай g - довільний елемент групи G. Розглянемо відображення φ_g множини елементів групи G в себе, визначене наступним чином: $\varphi_g\left(x\right) = gx$ для всякого $x \in G$. Довести, що φ_g є перетворенням множини елементів групи G (тобто взаємно однозначним відображенням множини елементів групи G на себе).

17. Нехай для кожного елемента g групи G побудоване перетворення φ_g (див. попередню вправу). Довести, що множина цих перетворень утворює групу із звичайною операцією множення перетворень.

18. Довести, що група G ізоморфна побудованій у попередній вправі групі перетворень.

19. Нехай $\langle a \rangle$ - нескінченна циклічна група, $\langle b \rangle$ - циклічна група порядку n. Поставимо у відповідність елементу a^k групи $\langle a \rangle$ елемент b^k групи $\langle b \rangle$. Довести, що одержане відображення є гомоморфізмом групи $\langle a \rangle$ на групу $\langle b \rangle$, ядром якого є циклічна підгрупа групи $\langle a \rangle$, породжена елементом a^n, а фактор-група $\langle a \rangle / \langle a^n \rangle$ ізоморфна групі $\langle b \rangle$.

20. Нехай $\mathbb{Z}$ - адитивна група всіх цілих чисел. Довести, що відображення $f : \mathbb{Z} \to \mathbb{Z}$, де $f(a) = -a$ є автоморфізмом групи $\mathbb{Z}$.

21.* Довести теорему Келі: всяка скінченна група ізоморфна деякій групі підстановок.

6 Кільця

6.1 Означення і приклади

Переходимо до розгляду алгебраїчних структур з двома бінарними операціями.

Нехай K - непорожня множина, на якій задані дві (бінарні алгебраїчні) операції + (додавання) і $\cdot$ (множення), які задовольняють умовам:

1) $(K, +)$ - абелева група;

2) $(K, \cdot)$ - півгрупа;

3) операції додавання і множення зв'язані дистрибутивними законами (іншими словами: множення дистрибутивне відносно додавання):

$$(a+b)c = ac + bc, \quad c(a+b) = ca + cb$$

для всіх $a, b, c \in K$.

Тоді $(K, +, \cdot)$ називається *кільцем.*

Структура $(K, +)$ називається *адитивною групою кільця*, а $(K, \cdot)$ - його *мультиплікативною півгрупою*. Якщо $(K, \cdot)$ - моноїд, то кажуть, що $(K, +, \cdot)$ - *кільце з одиницею*. Кільце називається *комутативним*, якщо комутативна його мультиплікативна півгрупа (тобто $ab = ba$ для всіх $a, b \in K$).

В силу 1) кільце містить нуль. Одиничний елемент мультиплікативної півгрупи (якщо він існує) називається *одиницею кільця* і позначається звичайною одиницею 1. Замість $a + (-b)$ пишуть $a - b$ і називають різницею елементів a і b.

Наведене вище означення кільця еквівалентне такому:

Непорожня множина K називається *кільцем*, якщо на ній визначені операції додавання і множення, причому виконуються такі умови:

1) операція додавання асоціативна, тобто для будь-яких $a, b, c \in K$ $(a+b)+c = a+(b+c)$;

2) операція додавання комутативна, тобто для будь-яких $a, b \in K$ $a + b = b + a$;

3) для операції додавання в множині K здійсненна обернена операція – віднімання , тобто для будь-яких $a,b \in K$ рівняння $b + x = a$ має в K єдиний розв'язок (цей розв'язок і є різницею елементів a і b: $x = a - b$);

4) операція множення асоціативна, тобто для будь-яких $a, b,c \in K$ $(ab)c = a(bc)$;

5) операція множення дистрибутивна відносно операції додавання, тобто для будь-яких $a,b,c \in K$ $(a + b)c = ac + bc$, $c(a + b) = ca + cb$.

Підмножина L кільця K називається *підкільцем*, якщо вона є підгрупою адитивної групи і підпівгрупою мультиплікативної півгрупи кільця. Ясно, що підкільце є кільцем відносно операцій, визначених в самому кільці K. Можна довести, що L - підкільце, якщо із того, що $a,b \in L$ випливає, що $a - b \in L$ і $ab \in L$ (самостійно).

Очевидно, що перетин будь-якої кількості підкілець є підкільце.

Наведемо деякі приклади.

1) Множина цілих чисел $\mathbb{Z}$ є комутативне кільце відносно визначених у ній операцій додавання і множення. Множина $m\mathbb{Z}$ цілих чисел, які діляться на m, буде в $\mathbb{Z}$ підкільцем (без одиниці при $m > 1$).

2) Множина раціональних чисел $\mathbb{Q}$ є комутативне кільце відносно визначених у ній операцій додавання і множення.

3) Множина $\mathbb{R}$ всіх дійсних чисел , очевидно, також є комутативне кільце відносно визначених у ній операцій додавання і множення.

4) Множина $M_n(\mathbb{R})$ всіх квадратних матриць порядку n з дійсними елементами при $n > 1$ є некомутативне кільце з одиницею відносно звичайних операцій додавання і множення матриць.

5) Множина всіх многочленів від одної змінної з дійсними коефіцієнтами відносно звичайних операцій додавання і множення многочленів утворює комутативне кільце.

6) Множина, що складається з одного числа 0, очевидно, є кільце. Це кільце називається *нульовим*, або *тривіальним*.

7) На всякій адитивній абелевій групі $(G,+)$ співвідношенням $ab=0$ для всіх $a,b\in G$ встановлюється структура *кільця з нульовим множенням*.

Зауважимо, що кільце, елементами якого є числа, називається *числовим кільцем*.

Багато властивостей кілець є переформулюванням відповідних властивостей груп і взагалі - множин з однією асоціативною операцією. Наприклад, $a^m\cdot a^n=a^{m+n}$, $\left(a^m\right)^n=a^{mn}$ для будь-яких невід'ємних цілих m і n і для всіх $a\in K$. Відмітимо інші властивості, які випливають із аксіом кільця і, по суті, моделюють властивості кільця цілих чисел $\mathbb{Z}$.

1) $a\cdot 0=0\cdot a=0$ для всіх $a\in K$.

Справді, $0\cdot a=(0+0)a=0\cdot a+0\cdot a$. Додавши до обох частин одержаної рівності $-0\cdot a$, одержимо: $-0\cdot a+0\cdot a=-0\cdot a+0\cdot a+0\cdot a$, тобто $0=0\cdot a$. Аналогічно доводимо, що $a\cdot 0=0$.

2) $a(-b)=(-a)b=-ab$ для всіх $a,b\in K$.

Дійсно, $0=a\cdot 0=a(b-b)=ab+a(-b)$; звідси $a(-b)=-ab$. Аналогічно доводимо, що $(-a)b=-ab$. Оскільки $-(-a)=a$, то з доведеного легко одержуємо рівності $(-a)(-b)=ab$, $-a=(-1)\cdot a$.

3) $(a-b)c=ac-bc$, $a(b-c)=ab-ac$ для всіх $a,b,c\in K$.

Тобто операція множення дистрибутивна і відносно операції віднімання. Справді, $b+(a-b)=a$, тому $\left[b+(a-b)\right]c=bc+(a-b)c=ac$; звідси $(a-b)c=ac-bc$. Аналогічно доводимо, що $a(b-c)=ab-ac$.

4) Із аксіоми дистрибутивності випливає *загальний закон дистрибутивності*:

$$\left(a_1 + a_2 + ... + a_n\right)\left(b_1 + b_2 + ... + b_m\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j .$$

Доведення легко одержати методом математичної індукції, спочатку по n (при $m = 1$), а потім по m.

Використовуючи доведені вище властивості, одержуємо

$$n\left(ab\right) = \left(na\right)b = a\left(nb\right)$$

для всіх $n \in \mathbb{Z}$ і всіх $a, b \in K$ (самостійно).

Для комутативного кільця відмітимо формулу бінома Ньютона:

$$\left(a + b\right)^n = \sum_{i=0}^{n} C_n^i a^{n-i} b^i .$$

6.2 Кільце класів лишків

Розглянемо ще один важливий приклад скінченного кільця. Нехай m - довільне відмінне від 1 натуральне число. Цілі числа a і b називають *конгруентними за модулем* m і записують

$$a \equiv b \left(\mathrm{mod}\, m\right),$$

якщо при діленні на m вони дають однакові остачі, тобто їх різниця ділиться на m. Число m при цьому називається *модулем порівняння*. Наприклад: $-4 \equiv 16 \left(\mathrm{mod}\, 5\right)$, $5 \equiv 8 \left(\mathrm{mod}\, 3\right)$ і т. д.

Позначимо символом C_r множину всіх цілих чисел, які при діленні на m дають остачу r $(0 \le r \le m-1)$, і назвемо її *класом конгруентних за модулем* m цілих чисел. Одержимо розбиття кільця всіх цілих чисел на класи

$$C_0, C_1, ..., C_{m-1} \qquad (6.1)$$

конгруентних за модулем m цілих чисел, причому ці класи, очевидно, не перетинаються.

В множині цих класів введемо операції додавання і множення. Нехай C_k і C_l - два які-небудь (не обов'язково різні) класи. Числа, які належать цим класам, представляються, відповідно, у виді $mp + k$ та $mq + l$, де p, q - цілі числа. Тоді

$$mp+k+mq+l=\begin{cases} m\left(p+q\right)+k+l\ , & k+l<m, \\ m\left(p+q\right)+k+l-m, & k+l\geq m. \end{cases}$$

Тобто сума будь-якого числа з C_k і будь-якого числа з C_l є число одного і того ж класу – класу C_{k+l}, якщо $k+l<m$ і класу C_{k+l-m}, якщо $k+l\geq m$.

Розглянемо добуток чисел із класів C_k і C_l:

$$\left(mp+k\right)\left(mq+l\right)=m\left(mpq+pl+qk\right)+kl=$$

$$=m\left(mpq+pl+qk\right)+ms+r=m\left(mpq+pl+qk+s\right)+r,$$

де s - ціле і $kl=ms+r\ \left(0\leq r\leq m-1\right)$. Тобто добуток будь-якого числа з C_k на будь-яке число з C_l є число одного і того ж класу C_r, де r - остача від ділення добутку kl на m.

Природно операції додавання і множення в множині класів (6.1) визначити так:

$$C_k+C_l=\begin{cases} C_{k+l}\ , & k+l<m, \\ C_{k+l-m}, & k+l\geq m. \end{cases}$$

$$C_k\cdot C_l=C_r\ ,\ \text{де}\ kl=ms+r,\quad 0\leq r\leq m-1.$$

Так визначені операції додавання і множення класів (6.1) асоціативні, комутативні і пов’язані законом дистрибутивності. Це випливає із справедливості цих законів для операцій із цілими числами і того зв’язку між операціями над цілими числами і над класами множин (6.1).

Клас C_0, який складається з чисел, які діляться на m, відіграє в множині класів роль нуля. Протилежним для класу C_k буде, очевидно, клас C_{m-k}. Тому в множині класів (6.1) здійсненна операція віднімання:

$$C_l-C_k=C_l+\left(-C_k\right)=C_l+C_{m-k}.$$

Отже, множина класів (6.1) є комутативне кільце. Назвемо його *кільцем класів лишків за модулем* m і позначимо $\mathbb{Z}\left(m\right)$. Зауважимо, що класи лишків (6.1) часто позначають $\overline{0},\overline{1},\ldots,\overline{m-1}$.

Видно, що чимало властивостей дій над числами

зберігається для дій, визначених в будь-якому кільці. Однак не слід думати, що всяка властивість додавання і множення чисел зберігається в будь-якому кільці. Так, наприклад, для чисел справедливе твердження: якщо добуток двох чисел дорівнює нулю, то принаймні один з множників дорівнює нулю. Це твердження не буде правильним для будь-якого кільця. Так, наприклад, якщо m - складене натуральне число, $m = pq$, то в кільці $\mathbb{Z}(m)$ кожен з класів C_p, C_q відмінний від нуля, проте $C_p \cdot C_q = C_0$.

Якщо $ab = 0$ при $a \neq 0$ і $b \neq 0$ в кільці K, то a називають *лівим*, а b - *правим дільником нуля* (в комутативному кільці говорять просто про дільники нуля).. Сам нуль в кільці $K \neq 0$ - тривіальний дільник нуля. Якщо інших дільників нуля нема, то K називається *кільцем без дільників нуля*.

6.3 Області цілісності; оборотні елементи

Комутативне кільце з одиницею $1 \neq 0$ і без дільників нуля називається *областю цілісності* (*кільцем цілісності*). Справедлива

Теорема 6.1. Нетривіальне комутативне кільце K з одиницею є областю цілісності тоді і тільки тоді, коли в ньому виконаний закон скорочення:

якщо $ab = ac$ і $a \neq 0$, то $b = c$.

Доведення. Якщо в K має місце закон скорочення, то із рівності $ab = 0 = a \cdot 0$ випливає, що або $a = 0$, або, якщо $a \neq 0$, то тоді $b = 0$. Навпаки, якщо K - область цілісності, то із $ab = ac$, $a \neq 0$, випливає

$$ab - ac = 0 \Rightarrow a(b - c) = 0 \Rightarrow b - c = 0 \Rightarrow b = c.$$

Теорему доведено.

Зауважимо, що всяке числове кільце є областю цілісності.

В кільці K з одиницею природно розглядати множину оборотних елементів: елемент a називається *оборотним* (або *дільником одиниці*), якщо існує елемент a^{-1} такий, що $aa^{-1} = 1 = a^{-1}a$. Точніше треба було б говорити про елементи оборотні зліва і справа, але для комутативних кілець, а також для кілець без дільників нуля ці поняття співпадають. Дійсно,

із $ab=1$ випливає $aba=a \Rightarrow aba-a=0 \Rightarrow a\left(ba-1\right)=0$. Оскільки $a\neq 0$, то $ba-1=0$, тобто $ba=1$.

Оборотний елемент кільця не може бути дільником нуля. Справді, якщо $ab=0$, то $a^{-1}\left(ab\right)=0$, звідси $\left(a^{-1}a\right)b=0\Rightarrow 1\cdot b=0\Rightarrow b=0$ (аналогічно доводимо, що із $ba=0$ випливає $b=0$). Має місце

Теорема 6.2. Всі оборотні елементи кільця K з одиницею складають групу $U\left(K\right)$ відносно множення.

Доведення. Справді, оскільки множина $U\left(K\right)$ містить одиницю, то досить переконатись, що вона замкнена відносно множення. Нехай $a,b\in U\left(K\right)$, тоді, як відомо $\left(ab\right)^{-1}=b^{-1}a^{-1}$ (тобто елемент ab теж оборотний), отже $ab\in U\left(K\right)$; теорему доведено.

Вправи

1. Довести, що множина K всіх чисел виду $a+b\sqrt{2}$, де a і b - будь-які раціональні числа, є комутативне кільце.

2. Діагональні матриці утворюють підкільце кільця матриць $M_n\left(\mathbb{R}\right)$. Довести.

3. Довести, що в ненульовому кільці з одиницею завжди $0\neq 1$.

4. Чи утворює кільце множина всіх чисел виду $a+b\sqrt[3]{2}$, де a і b - будь-які раціональні числа?

5. Скласти таблиці додавання і множення для $\mathbb{Z}\left(4\right)$ і $\mathbb{Z}\left(5\right)$.

6. Нехай Ω - довільна множина і $\mathbb{F}\left(\Omega\right)$ - множина всіх її підмножин. Довести, що $\mathbb{F}\left(\Omega\right)$ з операціями

$$A+B=\left(A\bigcup B\right)\setminus\left(A\bigcap B\right),\quad AB=A\bigcap B,\quad A,B\in\mathbb{F}\left(\Omega\right),$$

є кільцем з одиницею, всі елементи адитивної групи якого мають порядок два.

7. Множина всіх числових пар $\left(a,b\right)$ $(a,b\in\mathbb{Q})$ з

операціями додавання і множення, які визначаються формулами

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2),$$

утворюють комутативне кільце з одиницею, в якому є дільники нуля. Довести.

8. Довести, що в кільці, яке складається з n елементів, для будь-якого елемента a справджується рівність $na = 0$.

9. Довести комутативність довільного кільця, в якому кожний елемент задовольняє рівнянню $x^2 = x$. Чи вірно це при умові $x^3 = x$?

10. Нехай p - просте число і K - комутативне кільце з одиницею таке, що $px = 0$ для всіх $x \in K$. Показати, що тоді

$$(x + y)^{p^m} = x^{p^m} + y^{p^m}, \quad m = 1, 2, \ldots .$$

11. Нехай K - довільне кільце з одиницею 1 і a, b - його елементи. Довести, що

$$(1 - ab)c = 1 = c(1 - ab) \Rightarrow (1 - ba)d = d(1 - ba),$$

де $d = 1 + bca$, тобто із оборотності елемента $1 - ab$ випливає оборотність елемента $1 - ba$. Чому дорівнює елемент $1 + adb$?

12. Довести, що множина усіх комплексних чисел виду $a + bi$, де a, b - цілі дійсні числа (т. зв. цілі комплексні числа), утворює область цілісності.

13. Довести, що дільниками нуля в кільці матриць $M_n(\mathbb{R})$ є матриці з нульовим визначником і тільки вони. Вивести звідси, що в цьому кільці всякий елемент, що не є дільником нуля, - оборотний.

14. Елемент $x \neq 0$ кільця K називається *нільпотентним*, якщо $x^n = 0$ для деякого $n \in \mathbb{N}$. Довести, що з нільпотентності елемента x випливає оборотність елемента $1 - x$ в будь-якому кільці з одиницею.

15. Кільце $\mathbb{Z}(m)$ містить нільпотентні елементи тоді і тільки тоді, коли m ділиться на квадрат натурального числа > 1. Довести.

7 Ідеали, фактор-кільця, гомоморфізми кілець

7.1 Ідеали

Підкільце L кільця K називається *лівим* (*правим*) *ідеалом* цього кільця, якщо воно разом з кожним своїм елементом a містить також всі елементи виду ra (виду ar), де r - довільний елемент кільця K. Якщо ідеал є одночасно і лівим і правим, то він називається *двостороннім ідеалом*, або просто *ідеалом*. Зрозуміло, що в комутативному кільці поняття лівого і правого ідеалів співпадають, тобто всякий ідеал буде двостороннім. Двосторонні ідеали кільця аналогічні нормальним дільникам груп.

Наведемо деякі приклади ідеалів.

1) В кільці всіх цілих чисел числа, кратні деякому фіксованому числу m, утворюють двосторонній ідеал.

2) В кільці всіх квадратних матриць n-го порядку множина всіх матриць, у яких останній стовпчик складається із нулів, є лівим ідеалом, а множина всіх матриць, у яких останній рядок складається із нулів, є правим ідеалом (переконатись самостійно).

У всякому кільці 0 і саме кільце є двосторонніми ідеалами. Якщо інших ідеалів в кільці немає, то воно називається *простим кільцем*. Прикладом простого кільця служить кільце всіх квадратних матриць n-го порядку.

Нехай K - комутативне кільце, a - якийсь елемент K. Тоді множина aK є ідеалом в K. Дійсно, якщо $x, y \in K$, то

$$ax + ay = a(x + y), \qquad (ax)y = a(xy).$$

Кажуть, що aK - *головний ідеал*, породжений елементом a. Якщо K - кільце з одиницею, то воно є головним ідеалом, породженим одиничним елементом.

7.2 Гомоморфізми кілець

Нехай $(K, +, \cdot)$ і $(K', \oplus, \odot)$ - кільця. Відображення $f : K \to K'$ називається *гомоморфізмом*, якщо воно зберігає всі операції, тобто якщо

$$f(a+b) = f(a) \oplus f(b), \qquad f(ab) = f(a) \odot f(b).$$

При цьому, звичайно, $f(0)=0'$ і $f(na)=nf(a),\ n\in\mathbb{Z}$ (довести самостійно).

Ядром гомоморфізму f називається множина $Kerf$, яка складається із елементів a кільця K таких, що $f(a)=0'$. Ясно, що $Kerf$ - підкільце в K (переконатись самостійно). Але це не просто підкільце. Дійсно, якщо $L=Kerf\subset K$, то для будь-якого $x\in K$ $L\cdot x\subseteq L$ (оскільки $f(lx)=f(l)\odot f(x)=0'\odot f(x)=0'$) і $x\cdot L\subseteq L$. Тобто L - двосторонній ідеал кільця K. Отже, ядра гомоморфізмів завжди є ідеалами.

Як і у випадку з групами, взаємно однозначний гомоморфізм називається *ізоморфізмом*. Факт ізоморфізму кілець записується у виді $K\cong K'$.

7.3 Фактор-кільця

За аналогією з фактор-групою за нормальним дільником можна побудувати *фактор-кільце* кільця K за ідеалом L. При цьому вважатимемо, що "основу" кільця складає адитивна абелева група. За елементи фактор-кільця K/L беремо суміжні класи $a+L$ (які називаються *класами лишків за модулем ідеала* L). Додавання класів здійснюється за звичайним правилом:

$$(a+L)\oplus(b+L)=(a+b)+L,\quad \ominus(a+L)=-a+L.$$

За добуток тих же класів беремо

$$(a+L)\odot(b+L)=ab+L.$$

Важливо впевнитись, що таке множення визначене правильно, тобто не залежить від вибору представників класів. Нехай $a'=a+x,\ \ b'=b+y,\ \ x,y\in L$. Тоді

$$a'b'=ab+ay+xb+xy=ab+z,$$

де $z=ay+xb+xy\in L$, оскільки L - двосторонній ідеал. Отже $a'b'$ лежить в тому ж суміжному класі, що і ab, що означає, що добуток суміжних класів визначено правильно. Деколи для скорочення записів покладають $\overline{a}=a+L$, тоді

$$\overline{a}\oplus\overline{b}=\overline{(a+b)},\qquad \overline{a}\odot\overline{b}=\overline{ab}.$$

Зокрема, $\overline{0} = 0 + L$, $\overline{1} = 1 + L$ (якщо 1 є в K). Легко переконатись, що в множині $\overline{K} = K/L$ виконані всі аксіоми кільця. Це досить очевидно, оскільки операції над класами лишків в $\overline{K}$ зводяться до операцій над елементами з K. Зокрема, дистрибутивність перевіряється так:

$$\left(\overline{a} \oplus \overline{b}\right) \odot \overline{c} = \overline{\left(a + b\right)} \odot \overline{c} = \overline{\left(a + b\right)c} =$$
$$= \overline{\left(ac + bc\right)} = \overline{ac} \oplus \overline{bc} = \overline{a} \odot \overline{c} \oplus \overline{b} \odot \overline{c}.$$

7.4 Теорема про гомоморфізми

Нехай L - ідеал кільця K. Якщо кожному елементу a кільця поставити у відповідність суміжний клас $a + L$, то ми одержимо гомоморфне відображення кільця K на фактор-кільце K/L (перевірити самостійно). Одержаний гомоморфізм називається *природним*; неважко бачити, що ядром цього гомоморфізму є ідеал L.

Як і для груп, справедлива теорема, яка показує, що всі гомоморфізми даного кільця по суті вичерпуються його природними гомоморфізмами:

Теорема 7.1. (про гомоморфізми кілець). Нехай f - гомоморфізм кільця K на кільце K' і $L = Kerf$ - ядро цього гомоморфізму. Тоді кільце K' ізоморфне фактор-кільцю K/L.

Доведення таке ж, як і для груп. Шуканий ізоморфізм $\varphi: K/L \to K'$ встановлюється так:

$$\varphi\left(\overline{a}\right) = a' \text{ , якщо } f\left(a\right) = a'.$$

Тоді

$$\varphi\left(\overline{a} \oplus \overline{b}\right) = \varphi\left(\overline{a + b}\right) = f\left(a + b\right) =$$
$$= f\left(a\right) + f\left(b\right) = \varphi\left(\overline{a}\right) + \varphi\left(\overline{b}\right);$$
$$\varphi\left(\overline{a} \odot \overline{b}\right) = \varphi\left(\overline{ab}\right) = f\left(ab\right) = f\left(a\right) \cdot f\left(b\right) = \varphi\left(\overline{a}\right) \cdot \varphi\left(\overline{b}\right)$$

(тут операції в кільцях K і K' позначені однаково). Пропонуємо самостійно впевнитись у тому, що відображення φ є взаємно однозначним. Теорему доведено.

Вправи

1. Довести, що перетин будь-якого числа ідеалів деякого кільця теж є ідеалом цього кільця.

2. Нехай $M_2(\mathbb{Z})$ - кільце квадратних матриць другого порядку з цілими елементами. Довести, що множина матриць виду

$$\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix},\ \alpha,\beta,\gamma \in \mathbb{Z},$$

є підкільцем, але не ідеалом в $M_2(\mathbb{Z})$.

3. Знайти ідеали кілець $\mathbb{Z}(5), \mathbb{Z}(6), \mathbb{Z}(8)$.

4. Чи утворюють ідеал необоротні елементи кільця: 1) $\mathbb{Z}(16)$; 2) $\mathbb{Z}(24)$?

5. Якщо ідеал L кільця K містить оборотний елемент (зокрема, якщо $1 \in L$), то $L = K$. Довести.

6. Нехай K, L і H - множини всіх матриць виду

$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix},\quad \begin{pmatrix} 0 & g & h \\ 0 & 0 & 2k \\ 0 & 0 & 0 \end{pmatrix} \text{ і } \begin{pmatrix} 0 & l & 2m \\ 0 & 0 & 2n \\ 0 & 0 & 0 \end{pmatrix}$$

відповідно, де a,b,c,d,e,f,g,h,k,l,m,n - цілі числа. Довести, що K - кільце, L - ідеал кільця K, H - ідеал кільця L, але H не є ідеалом кільця K, проте є його лівим ідеалом.

7. Якщо K - кільце з одиницею і L - ідеал, то фактор-кільце K/L теж має одиницю. Довести.

8. Довести, що кільце K, яке складається з п'яти елементів, або ізоморфне $\mathbb{Z}(5)$, або є кільцем з нульовим множенням.

9. Кільце K називається *ніль-кільцем*, якщо для всякого елемента x із K знайдеться таке натуральне число n, що $x^n = 0$. Нехай K - деяке кільце, L - його ідеал, а кільце L і фактор-кільце K/L є ніль-кільцями. Довести, що K - теж ніль-кільце.

10. Нехай $f: K \to K'$ - ізоморфізм кілець. Довести, що якщо $f(a) = b$, то $f(-a) = -b$.

8 Поля

8.1 Означення і приклади

Полем P називається комутативне кільце з одиницею $1 \neq 0$, в якому кожний елемент $a \neq 0$ оборотний. Очевидно, множина всіх відмінних від нуля елементів поля утворює комутативну групу (*мультиплікативна група поля*).

Таким чином, поле являє собою гібрид двох абелевих груп – адитивної і мультиплікативної, зв'язаних законом дистрибутивності (одним, в силу комутативності). Зрозуміло, що жодне поле не має дільників нуля, тобто, якщо $ab = 0$, то принаймні один із співмножників a або b дорівнює нулю.

Прикладами полів служать: кільце всіх раціональних чисел $\mathbb{Q}$, кільце всіх дійсних чисел $\mathbb{R}$, кільце всіх комплексних чисел $\mathbb{C}$.

Поля, елементами яких є числа, називають *числовими полями*.

Наведемо приклад нечислового поля. Розглянемо комутативне кільце $\mathbb{Z}(p)$ класів лишків за модулем p, де p - деяке просте число. Доведемо, що кільце $\mathbb{Z}(p)$ є поле. Для цього досить показати, що в кільці $\mathbb{Z}(p)$ здійсненна операція ділення, крім ділення на нульовий елемент C_0. Нехай C_k і C_s - будь-які класи з кільця $\mathbb{Z}(p)$, причому $C_k \neq C_0$. Покажемо, що клас C_s можна поділити на клас C_k, тобто що в кільці $\mathbb{Z}(p)$ міститься, і притому лише один, клас C_l, який задовольняє умову $C_k \cdot C_l = C_s$. Якщо $C_s = C_0$, то і $C_l = C_0$. Припустимо, що $C_s \neq C_0$. Розглянемо ряд натуральних чисел

$$k, 2k, 3k, \ldots, (p-1)k. \qquad (8.1)$$

Жодне з цих чисел не ділиться на p, і тому жодне з чисел ряду (8.1) не міститься в класі C_0. Крім того, ніякі два числа rk і tk $(t > r)$ ряду (8.1) не містяться в одному класі, бо тоді різниця $tk - rk = (t-r)k$ повинна була б ділитися на p, чого не може бути. Отже, в кожному з ненульових класів

кільця $\mathbb{Z}(p)$, зокрема й у класі C_s міститься одне і тільки одне число ряду (8.1). Нехай у класі C_s міститься число $lk\ (1 \le l \le p-1)$. Тоді $C_k \cdot C_l = C_s$ і, отже, клас C_l і є шуканим, причому, як випливає з викладеного вище, це єдиний клас, який задовольняє умову $C_k \cdot C_l = C_s$.

Отже, кільце $\mathbb{Z}(p)$ є поле, причому скінченне: воно складається з p елементів.

8.2 Дроби і дії з ними

Добуток ab^{-1} записують, як правило, у виді *дробу* (*відношення, частки*) $\frac{a}{b}$. Дріб, який має зміст тільки при $b \neq 0$, є єдиним розв'язком рівняння $bx = a$.

Дії з дробами підпорядковуються деяким правилам:

1) $\frac{a}{b} = \frac{c}{d}$ тоді і тільки тоді, коли $ad = bc$ $(b \neq 0,\ d \neq 0)$;

2) $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$ $(b \neq 0,\ d \neq 0)$;

3) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ $(b \neq 0,\ d \neq 0)$;

4) $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$ $(b \neq 0,\ d \neq 0,\ c \neq 0)$;

5) $\frac{-a}{b} = \frac{a}{-b} = -\frac{a}{b}$ $(b \neq 0)$;

6) $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$ $(a \neq 0,\ b \neq 0)$.

Як бачимо, це звичайні "шкільні" правила, але їх потрібно виводити із аксіом поля. Доведемо деякі з цих рівностей.

Перша рівність може бути доведена так: Нехай $b \neq 0,\ d \neq 0$, тоді в полі є обернені елементи b^{-1}

і d^{-1}. Тоді $\frac{a}{b}=ab^{-1}$, $\frac{c}{d}=cd^{-1}$. Припустимо, що $\frac{a}{b}=\frac{c}{d}$, або $ab^{-1}=cd^{-1}$. Останню рівність домножимо на bd: $ab^{-1}bd=cd^{-1}bd$, або $ad=bc$; цим доведена необхідність умови. Припустимо тепер, що $ad=bc$. Помножимо обидві частини цієї рівності на $b^{-1}d^{-1}$: $adb^{-1}d^{-1}=bcb^{-1}d^{-1}$, або $ab^{-1}=cd^{-1}$, тобто $\frac{a}{b}=\frac{c}{d}$. Цим доведена достатність умови.

Другу рівність можна довести таким чином:

$$\frac{a}{b}\pm\frac{c}{d}=ab^{-1}\pm cd^{-1}=\left(ab^{-1}\pm cd^{-1}\right)\left((bd)(bd)^{-1}\right)=$$

$$=\left(\left(ab^{-1}\pm cd^{-1}\right)(bd)\right)(bd)^{-1}=$$

$$=\left(\left(ab^{-1}\right)(bd)\pm\left(cd^{-1}\right)(bd)\right)(bd)^{-1}=$$

$$(ad\pm bc)(bd)^{-1}=\frac{ad\pm bc}{bd}.$$

Решту рівностей можна довести аналогічно (самостійно).

8.3 Підполе, розширення поля; ізоморфізм полів

Підмножина P' поля P називається *підполем* цього поля, якщо вона сама є полем відносно бінарних операцій, визначених в полі P. P' тоді і тільки тоді є підполем поля P, якщо разом з всякими двома елементами a,b містить також $a+b,\ ab,\ a-b,\ \frac{a}{b}$ (якщо $b\neq 0$). Якщо P' є підполем поля P, то P називають *розширенням* поля P'. Поле, яке не має підполів, відмінних від нього самого, називається *простим полем*. Приклади простих полів – поле класів лишків за модулем p, поле всіх раціональних чисел.

Так, поле раціональних чисел $\mathbb{Q}$ є підполем поля дійсних чисел виду $a+b\sqrt{2}$ (a і b - довільні раціональні числа, див. вправу 1) і поля дійсних чисел $\mathbb{R}$; поле дійсних чисел виду

$a+b\sqrt{2}$ також є підполем поля дійсних чисел $\mathbb{R}$.

Якщо P' - підполе поля P, то нуль 0 і одиниця 1 поля P містяться в P' і служать для P' нулем і одиницею. Справді, якщо $a \in P'$, $a \neq 0$, то $a-a=0 \in P'$ і $\frac{a}{a}=1 \in P'$.

Очевидним є таке твердження: перетин будь-якої сукупності підполів поля P також є підполе поля P.

Нехай P' - підполе поля P і c - будь-який елемент цього поля, що не міститься в підполі P'. Розглянемо всі підполя поля P, кожне з яких містить P' і елемент c. Такі підполя існують, бо до них , зокрема, належить саме поле P. Для кожного з цих підполів P' є підполем. Перетин усіх цих підполів є підполе поля P, що містить елемент c. Позначимо його P''. Отже P'' є розширенням поля P' і містить елемент c. Причому у полі P'' нема, відмінного від нього самого, підполя, яке було б розширенням поля P' і містило елемент c. Підполе P'' називають *мінімальним розширенням* поля P', що містить елемент c. В цьому випадку кажуть, що поле P'' утворене приєднанням до поля P' елемента c і записують $P''=P'(c)$. Поле $P'(c)$ містить усі елементи поля P', елемент c, а також усі елементи, які дістаємо з елементів поля P' і елемента c за допомогою операцій додавання, множення, віднімання і ділення.

Якщо при цьому c є коренем деякого многочлена $f(x)$ з коефіцієнтами із поля P' , то поле $P''=P'(c)$ називається *простим алгебраїчним розширенням* поля P', а елемент c називається *алгебраїчним відносно* P'; якщо ж не існує многочлена $f(x)$ з коефіцієнтами із P', коренем якого був би елемент c, то $P''=P'(c)$ називається *простим трансцендентним розширенням* поля P'.

Наприклад:

1) Множина всіх чисел виду $a+b\sqrt{2}$, де a і b - раціональні числа, є розширенням поля раціональних чисел

$\mathbb{Q}$ приєднанням до нього елемента $\sqrt{2}$, тобто, це буде поле $\mathbb{Q}\left(\sqrt{2}\right)$. Очевидно, це буде просте алгебраїчне розширення, оскільки $\sqrt{2}$ є коренем многочлена з раціональними коефіцієнтами x^2-2.

2) Як відомо, не існує многочлена з раціональними коефіцієнтами, коренем якого було б число π, тому розширення $\mathbb{Q}\left(\pi\right)$ буде простим трансцендентним розширенням поля раціональних чисел $\mathbb{Q}$.

3) Поле всіх комплексних чисел $\mathbb{C}$ є простим алгебраїчним розширенням поля всіх дійсних чисел $\mathbb{R}$, одержаним із нього приєднанням кореня i многочлена x^2+1: $\mathbb{C}=\mathbb{R}\left(i\right)$.

Поля P і P' називаються *ізоморфними*, якщо вони ізоморфні як кільця. За означенням $f\left(0\right)=0'$ і $f\left(1\right)=1'$ для будь-якого ізоморфного відображення $f: P\to P'$. Не має змісту говорити про гомоморфізм полів, оскільки, якщо $Kerf\neq 0$, то існує $a\neq 0$ ($a\in P$) таке, що $f\left(a\right)=0'$. Звідси $f\left(1\right)=f\left(aa^{-1}\right)=f\left(a\right)f\left(a^{-1}\right)=0'\cdot f\left(a^{-1}\right)=0'$. Тоді для будь-якого $b\in P$ одержуємо

$$f\left(b\right)=f\left(1\cdot b\right)=f\left(1\right)f\left(b\right)=0'\cdot f\left(b\right)=0',$$

тобто $Kerf=P$.

8.4 Характеристика поля

Нехай P - поле. Додатне число p називається *характеристикою поля* P, якщо $\underbrace{1+1+...+1}_{p}=0$ і ніяке додатне число, менше, ніж p, цією властивістю не володіє. Якщо вказана властивість не має місця ні для якого додатного числа, то кажуть, що поле має *характеристику* 0. Полем характеристики 0 є всяке числове поле. Характеристику p, де p - просте число, має поле $\mathbb{Z}\left(p\right)$ класів лишків за модулем p. Має місце

Теорема 8.1. Характеристикою поля може бути тільки 0 або просте число.

Доведення. Якщо $n = kl$, де $1 < k, l < n$, є характеристикою поля P, то $a = \underbrace{1+...+1}_{k}$ і $b = \underbrace{1+...+1}_{l}$ відмінні від нуля. Але $ab = \underbrace{1+1+...+1}_{n=kl} = 0$, що суперечить відсутності в полі дільників нуля. Теорему доведено.

Неважко довести, що якщо P - поле характеристики p, то $pa = 0$ для будь-якого елемента a поля P (самостійно).

Теорема 8.2. В кожному полі P міститься одне і тільки одне просте поле P_0. Це просте поле ізоморфне або $\mathbb{Q}$, або $\mathbb{Z}(p)$ для деякого p.

Доведення. Припустивши існування двох різних простих підполів $P', P'' \subset P$, ми приходимо до висновку, що їх перетин $P' \bigcap P''$ (очевидно, непорожній, оскільки 0 і 1 містяться як в P', так і в P'') буде полем, відмінним від P' і P''. Але це неможливо в силу їх простоти. Отже, просте підполе $P_0 \subset P$ єдине.

В P_0 разом з одиничним елементом 1 містяться всі його кратні $n \cdot 1 = 1+...+1$. Із властивостей операцій в кільцях випливає, що

$$s \cdot 1 + t \cdot 1 = (s+t) \cdot 1, \quad (s \cdot 1)(t \cdot 1) = (st) \cdot 1, \qquad s, t \in \mathbb{Z}.$$

Тому відображення f кільця $\mathbb{Z}$ в P, визначене правилом $f(n) = n \cdot 1$ є гомоморфізмом, ядро якого, будучи ідеалом в $\mathbb{Z}$, має вид $Kerf = m\mathbb{Z}$. Якщо $m = 0$. То f - ізоморфізм, і дроби $(s \cdot 1)/(t \cdot 1)$, які мають смисл в P (оскільки P - поле), утворюють поле P_0, ізоморфне $\mathbb{Q}$. Воно і буде простим підполем в P.

Якщо $m > 0$, то, очевидно, відображення f^*, визначене за правилом

$$f^*(C_k) = f(k) = k \cdot 1,$$

буде ізоморфним вкладенням $\mathbb{Z}(m) \to P$. Але це можливо тільки тоді, коли $m = p$ - просте число. Отже, $f^*(\mathbb{Z}(m))$ - просте підполе в P. Теорему доведено.

Вправи

1. Довести, що множина чисел виду $a + b\sqrt{2}$, де a і b - будь-які раціональні числа, є полем.

2. З'ясувати, чи є полем множина всіх дійсних чисел виду $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ (a, b, c - деякі раціональні числа) відносно звичайних операцій додавання і множення над ними.

3. Знайти обернені елементи для всіх відмінних від нуля елементів поля $\mathbb{Z}(7)$.

4. Довести, що всяка скінченна область цілісності є поле.

5. Довести, що поле $\mathbb{Q}$ раціональних чисел – просте.

6. Нехай K і K_1 - ізоморфні кільця: $K \cong K_1$. Припустимо, що кільце K є поле. Довести, що кільце K_1 також є поле.

7. Довести, що комутативне кільце з одиницею $1 \neq 0$, яке не має ідеалів, відмінних від нуля і всього кільця, є поле. Показати, що не можна відмовитись від вимоги існування одиниці.

8. Довести, що матриці виду $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, де a,b - раціональні числа, утворюють поле, ізоморфне полю, утвореному дійсними числами виду $a + b\sqrt{2}$, де a,b - раціональні числа.

9. Довести, що будь-яке підполе поля $\mathbb{Q}(\sqrt{2})$ всіх дійсних чисел виду $a + b\sqrt{2}$ (a,b - деякі раціональні числа) є або поле $\mathbb{Q}$, або поле $\mathbb{Q}(\sqrt{2})$.

10. Нехай $f: P \to P'$ - ізоморфізм полів. Якщо $f(a) = b$, то $f(a^{-1}) = b^{-1}$. Довести.

11. Довести, що всяке поле, яке складається з двох елементів, ізоморфне полю $\mathbb{Z}(2)$.

12. Довести, що матриці виду $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, де $a,b \in \mathbb{Z}(3)$ утворюють поле з 9 елементів і що мультиплікативна група цього поля – циклічна, порядку 8.

13. Довести, що поле квадратних матриць виду $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, де a, b - дійсні числа, ізоморфне полю комплексних чисел.

14. Довести такі твердження:

а) якщо для деякого елемента a поля P знайдеться ціле $n \neq 0$ таке, що $na = 0$, то для будь-якого елемента $b \in P$ теж буде виконуватись рівність $nb = 0$;

б) нехай $p > 0$ - найменше ціле, для якого $pa = 0$; тоді для довільного елемента b поля p буде також найменшим, що задовольняє умову $pb = 0$; причому p є просте число >1.

9 Інші алгебраїчні структури

9.1 Півкільця

Розглянемо ще деякі алгебраїчні структури, які зустрічаються в математиці та її застосуваннях.

Півкільцем називається непорожня множина з двома асоціативними бінарними операціями $+$ і $\cdot$ (додаванням і множенням), які зв'язані законами дистрибутивності

$$(a+b)\cdot c = a\cdot c + b\cdot c, \quad a(b+c) = ab + ac.$$

Як правило вважається, що додавання комутативне і існує 0, для якого $a+0=a$ при будь-якому a. Очевидно, всяке кільце буде півкільцем. Ще один приклад півкільця – множина невід'ємних цілих чисел із звичайними операціями додавання і множення.

9.2 Тіла

Кільцем з діленням, або *тілом* називається кільце, у якому всі відмінні від нуля елементи утворюють групу відносно операції множення. Це означає, що кожний ненульовий елемент тіла оборотний, тобто для всякого $a \neq 0$ і будь-якого b кожне з рівнянь $ax = b$ і $ya = b$ має єдиний розв'язок. Зрозуміло, що тіло не містить дільників нуля. Відмінність тіла від поля полягає в тому, що множення в тілі не зобов'язано бути комутативним. Комутативні тіла – це в точності поля.

Важливим прикладом тіла, яке не є полем, є *тіло кватерніонів* H. Формально кватерніон записується у виді

$$z = a\cdot 1 + bi + cj + dk \quad (\text{або } z = a + bi + cj + dk)$$

де a,b,c,d - дійсні числа, i,j,k - деякі символи. Додаються і перемножаються кватерніони як комплексні числа, тобто

$$z_1 + z_2 = a_1 + b_1 i + c_1 j + d_1 k + a_2 + b_2 i + c_2 j + d_2 k =$$
$$= a_1 + a_2 + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

При множенні кватерніонів спираються на рівності

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j. \tag{9.1}$$

Тоді

$$z_1 z_2 = \left(a_1 + b_1 i + c_1 j + d_1 k\right)\left(a_2 + b_2 i + c_2 j + d_2 k\right) =$$
$$= a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2 + \left(a_1 b_2 + b_1 a_2 + c_1 d_2 - d_1 c_2\right) i +$$
$$+\left(a_1 c_2 - b_1 d_2 + c_1 a_2 + d_1 b_2\right) j + \left(a_1 d_2 + b_1 c_2 - c_1 b_2 + d_1 a_2\right) k .$$

Неважко перевірити, що множина кватерніонів з так введеними операціями додавання і множення є тіло. Дійсно, ці операції є асоціативними; операція додавання є комутативною, а операція множення – ні, в чому легко переконатись, перемноживши в тому і іншому порядку кватерніони $i = 0 + 1i + 0j + 0k$ і $j = 0 + 0i + 1j + 0k$. Роль нуля виконує кватерніон $0 = 0 + 0i + 0j + 0k$, роль одиниці – кватерніон $1 = 1 + 0i + 0j + 0k$. Протилежним до кватерніона $z = a + bi + cj + dk$ буде кватерніон $-z = -a - di - cj - dk$.

Щоб з'ясувати питання про існування оберненого елемента, введемо поняття норми кватерніона. *Нормою кватерніона* $z = a + bi + cj + dk$ є число

$$\left|z\right|^2 = a^2 + b^2 + c^2 + d^2$$

(норма позначається також $N\left(z\right)$). Очевидно $\left|z\right|^2 \geq 0$, причому $\left|z\right|^2 = 0 \Leftrightarrow z = 0$. Кватерніон $\overline{z} = a - bi - cj - dk$ називається *спряженим* з z. Неважко перевірити , що

$$z\overline{z} = a^2 + b^2 + c^2 + d^2 = \left|z\right|^2 = \left|\overline{z}\right|^2 .$$

Таким чином, оберненим до кватерніона $z \neq 0$ буде кватерніон $z^{-1} = \dfrac{\overline{z}}{\left|z\right|^2}$.

9.3 Алгебри

Кільце A називається *алгеброю* (або *лінійною алгеброю*) над полем P, якщо його адитивна група утворює векторний (лінійний) простір над полем P, тобто визначене множення елементів із A на елементи із P, виконані звичні аксіоми лінійного простору і, крім того,

$$\alpha\left(ab\right) = \left(\alpha a\right)b = a\left(\alpha b\right)$$

для всіх $\alpha \in P$, $a,b \in A$. Розмірність векторного простору A називається *розмірністю* (*рангом*) *алгебри* A. Алгебри скінченного рангу називаються ще *гіперкомплексними системами*. Якщо якась алгебра є не тільки кільце, а тіло, то вона називається *алгеброю з діленням*.

Якщо векторний простір над полем P, який служить адитивною групою алгебри A має базис $e_1, e_2, ..., e_n$, то досить знати, чому дорівнюють всі можливі попарні добутки елементів цього базису, щоб знати, чому дорівнює добуток будь-яких двох елементів алгебри. Отже задати алгебру скінченого рангу можна таблицею множення, де для будь-яких двох елементів e_i, e_j базису вказується лінійна комбінація елементів цього базису, яка дорівнює добутку $e_i e_j$.

Наведемо деякі приклади алгебр.

1) Всяке поле є алгеброю рангу 1 над самим собою.

2) Всі комплексні числа відносно звичайних операцій додавання і множення комплексних чисел і звичайної операції множення комплексних чисел на дійсні утворюють алгебру з діленням рангу 2 над полем дійсних чисел. Базисом цієї алгебри можуть служити елементи $1, i$ (як виглядає таблиця множення для такого базису?).

3) Множина всіх векторів тривимірного простору, в якій вектори додаються і множаться на числа звичайним чином, а добутком двох векторів є їх векторний добуток, є алгебра рангу 3 над полем дійсних чисел.

4) Алгеброю з діленням рангу 4 над полем дійсних чисел є тіло кватерніонів, розглянуте вище. Базисом цієї алгебри служать елементи $1, i, j, k$.

5) Множина всіх квадратних матриць n-го порядку з дійсними (комплексними) елементами, в якій звичайним чином визначені додавання і множення матриць і операція множення матриці на число є алгеброю рангу n^2 над полем дійсних (комплексних) чисел. Пропонуємо самостійно вибрати базис цієї алгебри і скласти таблицю множення.

9.4 Модулі

Комутативна група M називається *лівим модулем* над кільцем R з одиницею (або *лівим R-модулем*), якщо для елементів групи визначені добутки $\lambda a \in M$ для всіх $\lambda \in R$ і

$a \in M$, причому

1) $\lambda(a+b) = \lambda a + \lambda b$;

2) $(\lambda + \mu)a = \lambda a + \mu a$;

3) $(\lambda\mu)a = \lambda(\mu a)$;

4) $1a = a$

для будь-яких $\lambda, \mu \in R$ і $a, b \in M$.Аналогічно визначається *правий модуль* над R (*правий* R*-модуль*), для якого визначений добуток $a\lambda \in M$ і для якого властивості 1) – 4) видозмінюються очевидним чином. Якщо кільце R комутативне, то лівий і правий R-модулі можна не розрізняти, бо, поклавши $a\lambda = \lambda a$, $\lambda \in R$, $a \in M$, ми перетворюємо лівий R-модуль в правий, оскільки

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

Елементи модуля прийнято називати *векторами*.

Легко встановлюється справедливість властивостей (самостійно):

1) $0a = \lambda 0 = 0$;

2) $\lambda(-a) = (-\lambda)a = -\lambda a$;

3) $\lambda(a-b) = \lambda a - \lambda b$, $(\lambda - \mu)a = \lambda a - \mu a$;

де $a, b \in M$, $\lambda, \mu \in R$. Аналогічні рівності справедливі для правих R-модулів.

Наведемо деякі приклади модулів.

1) Всяка абелева група A є модулем над кільцем цілих чисел $\mathbb{Z}$, де для $n \in \mathbb{Z}$ і $a \in A$

$$na = \begin{cases} \underbrace{a + \ldots + a}_{n}, & n > 0, \\ 0, & n = 0, \\ \underbrace{(-a) + \ldots + (-a)}_{-n}, & n < 0. \end{cases}$$

2) Лінійний простір над полем P є P-модулем.

3) Лівий (правий) ідеал L кільця R (і, зокрема, саме кільце R) є лівим (правим) R-модулем, де добуток λa (чи $a\lambda$) для $\lambda \in R$, $a \in L$, співпадає з добутком, визначеним в R.

Вправи

1. Довести, що тіло кватерніонів ізоморфне тілу всіх матриць над полем комплексних чисел виду

$\begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix}$ (або $\begin{pmatrix} a+di & b+ci \\ -b+ci & a-di \end{pmatrix}$, a,b,c,d - дійсні).

2.Довести, що тіло кватерніонів ізоморфне тілу всіх матриць над полем дійсних чисел виду

$$\begin{pmatrix} a & -b & c & d \\ b & a & -d & c \\ -c & d & a & b \\ -d & -c & -b & a \end{pmatrix}.$$

3. Довести, що операція спряження кватерніонів має властивості

$$\overline{(z_1+z_2)} = \overline{z}_1 + \overline{z}_2; \qquad \overline{z} = z \Leftrightarrow z \in \mathbb{R};$$

$$\overline{z} = -z \Leftrightarrow a = 0; \qquad \overline{(z_1 z_2)} = \overline{z}_2 \overline{z}_1.$$

4. Довести, що для норми кватерніонів справджується рівність $N(z_1 z_2) = N(z_1) N(z_2)$.

5. Скільки розв'язків в алгебрі кватерніонів H має рівняння $x^2 + 1 = 0$?

10 Многочлени

10.1 Кільце многочленів

Многочленом (або *поліномом*) *степеня* n (n - натуральне число) від одної змінної x *над полем* P називається вираз виду

$$a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n \ , \qquad (10.1)$$

де $a_0, a_1, ..., a_{n-1}, a_n$ - елементи поля P, причому $a_0 \neq 0$. Якщо $a \in P$, то вираз a теж вважається многочленом над полем P, причому якщо $a \neq 0$, то це многочлен нульового степеня, якщо ж $a = 0$, то степінь такого многочлена вважається невизначеним. Елементи $a_0, a_1, ..., a_n$ називаються *коефіцієнтами* многочлена (10.1), a_0 називається *старшим коефіцієнтом*. Для скорочення запису многочлена ми будемо вживати символи $f(x)$, $g(x)$, $\varphi(x)$ і т. д.

Два многочлени вважаються рівними, $f(x) = g(x)$, тоді і тільки тоді, коли рівні їх коефіцієнти при однакових степенях змінної x.

Нехай

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n . \qquad (10.2)$$

Якщо в праву частину цієї рівності замість x підставити деякий елемент поля P і виконати вказані обчислення, розуміючи операції додавання і множення як операції в полі P, то в результаті одержиться деякий елемент b поля P. В цьому випадку записують $f(a) = b$. Якщо $f(a) = 0$, де 0 - нульовий елемент поля P, то кажуть, що a - *корінь многочлена* $f(x)$ (або *корінь рівняння* $f(x) = 0$).

Многочлени над довільним полем можна додавати, віднімати і множити.

Сумою (*різницею*) двох многочленів $f(x)$ і $g(x)$ називається многочлен $\varphi(x)$, у якого коефіцієнт при кожному степені змінної x дорівнює сумі (різниці) коефіцієнтів при цьому степені x в многочленах $f(x)$ і

$g(x)$. Очевидно, що степінь суми чи різниці двох многочленів не більший, ніж максимальний із степенів даних многочленів.

Щоб обчислити *добуток* двох многочленів $f(x)$ і $g(x)$ потрібно кожен доданок ax^k многочлена $f(x)$ помножити на кожний доданок bx^l многочлена $g(x)$ за правилом $ax^k bx^l = abx^{k+l}$, де ab - добуток в полі P, а $k+l$ - звичайна сума натуральних чисел. Після цього всі одержані добутки потрібно додати, зводячи подібні члени. Степінь добутку двох многочленів дорівнює сумі степенів співмножників. Звідси випливає, що добуток двох многочленів, відмінних від нуля, ніколи не буде дорівнювати нулю.

Враховуючи, що операції додавання і множення елементів в полі P наділені властивостями комутативності, асоціативності і дистрибутивності, неважко одержати, що введені нами операції додавання і множення многочленів над полем P також мають властивості комутативності, асоціативності і дистрибутивності. Крім того, множина многочленів над полем P містить нульовий елемент – ним буде нульовий елемент поля P, який ми включили в число многочленів, а також одиничний – одиниця 1 поля P, якщо її розглядати як многочлен нульового степеня. Зауважимо, що для кожного елемента в множині многочленів існує протилежний; протилежним для многочлена $f(x)$ (10.2) буде, очевидно, многочлен $-f(x) = -a_0 x^n - a_1 x^{n-1} - ... - a_{n-1} x - a_n$. З усього сказаного вище випливає, що множина многочленів над даним полем P утворює *комутативне кільце,* позначимо його $P[x]$. Оскільки в цьому кільці відсутні дільники нуля, то $P[x]$ буде *кільцем цілісності*. Неважко бачити, що в кільці $P[x]$ міститься само поле P.

10.2 Ділення з остачею

Очевидно, що для многочлена $f(x)$ існує обернений тоді і тільки тоді, коли $f(x)$ є многочленом нульового степеня.

Звідси випливає, що для множення многочленів обернена операція – ділення – не визначена. В цьому відношенні система всіх многочленів над полем P нагадує систему всіх цілих чисел. Ця аналогія проявляється і в тому, що для многочленів виконана операція *ділення з остачею*. Поділити многочлен $f(x)$ на многочлен $g(x)$ з остачею – це означає знайти такі многочлени $q(x)$ (*частку*) і $r(x)$ (*остачу*), що

$$f(x) = q(x) \cdot g(x) + r(x), \qquad (10.3)$$

причому степінь многочлена $r(x)$ менший ніж степінь $g(x)$, або ж $r(x) = 0$.

Нехай

$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, $g(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$.

Якщо $n < m$, то покладемо $q(x) = 0$ і $r(x) = f(x)$ і одержуємо частку і остачу. Якщо $n \geq m$, то розглянемо многочлен

$$f(x) - \frac{a_0}{b_0} x^{n-m} g(x) = f_1(x).$$

Многочлен $f_1(x)$ не містить члена з x^n, тому його степінь не більший, ніж $n-1$, або $f_1(x) = 0$. Якщо

$$f_1(x) = c_0 x^k + c_1 x^{k-1} + \ldots + c_k$$

і $k \geq m$, то розглянемо многочлен

$$f_1(x) - \frac{c_0}{b_0} x^{k-m} g(x) = f_2(x),$$

степінь якого не більший, ніж $k-1$ і т. д. Оскільки степінь одержуваного на кожному кроці многочлена строго менший, ніж степінь попереднього, то цей процес повинен закінчитись, тобто на деякому кроці ми одержимо

$$f_{s-1}(x) - \frac{d_0}{b_0} x^{l-m} g(x) = f_s(x)$$

і степінь многочлена $f_s(x)$ буде меншим, ніж степінь многочлена $g(x)$, або $f_s(x) = 0$. Тоді одержимо

$$f(x)=\frac{a_0}{b_0}x^{n-m}g(x)+f_1(x)=$$

$$=\frac{a_0}{b_0}x^{n-m}g(x)+\frac{c_0}{b_0}x^{k-m}g(x)+f_2(x)=\ldots=$$

$$=\frac{a_0}{b_0}x^{n-m}g(x)+\frac{c_0}{b_0}x^{k-m}g(x)+\ldots+\frac{d_0}{b_0}x^{l-m}g(x)+f_s(x)=$$

$$=\left(\frac{a_0}{b_0}x^{n-m}+\frac{c_0}{b_0}x^{k-m}+\ldots+\frac{d_0}{b_0}x^{l-m}\right)g(x)+f_s(x).$$

Тобто многочлени

$$q(x)=\frac{a_0}{b_0}x^{n-m}+\frac{c_0}{b_0}x^{k-m}+\ldots+\frac{d_0}{b_0}x^{l-m},\qquad r(x)=f_s(x)$$

дійсно задовольняють рівності (10.3), причому степінь $r(x)$ справді менший, ніж степінь $g(x)$. Описаний тут процес ділення многочлена на многочлен називається діленням “стовпчиком”.

Легко довести, що многочлени $q(x)$ і $r(x)$, які задовольняють рівності (10.3) визначаються однозначно (самостійно).

Вправи

1. Поділити з остачею $f(x)$ на $g(x)$ (многочлени над полем раціональних чисел), якщо:

1) $f(x)=x^3-1,\quad g(x)=x^2+x+1;$

2) $f(x)=2x^2-3x+1,\qquad g(x)=x^2-4x-1;$

3) $f(x)=x^3-2x^2-10x+3,\qquad g(x)=2x+5.$

11 Подільність многочленів; найбільший спільний дільник

11.1 Дільники

Якщо остача від ділення многочлена $f(x)$ на $\varphi(x)$ дорівнює нулю, тобто, як кажуть, $f(x)$ *ділиться* (або *націло ділиться*) на $\varphi(x)$, то многочлен $\varphi(x)$ називається *дільником* многочлена $f(x)$. Очевидно, многочлен $\varphi(x)$ буде дільником многочлена $f(x)$ тоді і тільки тоді, коли існує многочлен $\psi(x)$, який задовольняє рівності

$$f(x)=\psi(x)\cdot\varphi(x). \qquad (11.1)$$

Зрозуміло, що при цьому $\psi(x)$ теж буде дільником $f(x)$, і що степені $\varphi(x)$ і $\psi(x)$ не більші, ніж степінь $f(x)$.

Зауважимо, що якщо многочлен $f(x)$ і його дільник $\varphi(x)$ - многочлени над полем P, то і частка $\psi(x)$ - теж многочлен над полем P, що випливає з алгоритму відшукання частки. Але многочлен над полем P може мати і такі дільники, не всі коефіцієнти яких належать полю P, що показує, наприклад, рівність

$$x^2+1=(x-i)(x+i).$$

В лівій частині цієї рівності – многочлен над полем дійсних (навіть раціональних) чисел, а справа – многочлени над полем комплексних чисел.

Зауважимо, що многочлен $f(x)$ ділиться на многочлен першого степеня $x-c$ тоді і тільки тоді, коли c - корінь многочлена $f(x)$ (теорема Безу).

Вкажемо деякі очевидні властивості подільності многочленів, які використовуватимуться в подальшому.

1) Якщо $f(x)$ ділиться на $g(x)$, а $g(x)$ ділиться на $h(x)$, то $f(x)$ ділиться на $h(x)$.

2) Якщо $f(x)$ і $g(x)$ діляться на $\varphi(x)$, то і їх сума і різниця діляться на $\varphi(x)$.

3) Якщо $f(x)$ ділиться на $\varphi(x)$, то добуток $f(x)$ на будь-який многочлен теж буде ділитись на $\varphi(x)$.

4) Якщо кожний із многочленів $f_1(x), f_2(x), \dots, f_k(x)$ ділиться $\varphi(x)$, то на $\varphi(x)$ буде ділитись і многочлен

$$f_1(x)g_1(x)+f_2(x)g_2(x)+\dots+f_k(x)g_k(x),$$

де $g_1(x), g_2(x), \dots, g_k(x)$ - довільні многочлени.

5) Всякий многочлен ділиться на будь-який многочлен нульового степеня.

6) Якщо $f(x)$ ділиться на $\varphi(x)$, то $f(x)$ буде ділитись і на $c\varphi(x)$, де $c \neq 0$ - довільний елемент поля P.

7) Многочлени $cf(x)$, $c \neq 0$ і тільки вони будуть дільниками многочлена $f(x)$, які мають той же степінь, що і $f(x)$.

8) Многочлени $f(x)$ і $g(x)$ тоді і тільки тоді діляться один на одного, коли $g(x)=cf(x)$, $c \neq 0$.

9) Всякий дільник одного з двох многочленів $f(x)$ і $cf(x)$, де $c \neq 0$ буде дільником і для другого многочлена.

11.2 Найбільший спільний дільник

Нехай дані довільні многочлени $f(x)$ і $g(x)$. Многочлен називається *спільним дільником* для $f(x)$ і $g(x)$, якщо він є дільником для кожного з цих многочленів. До числа спільних дільників многочленів $f(x)$ і $g(x)$ належать, очевидно, всі многочлени нульового степеня. Якщо інших спільних дільників ці два многочлени не мають, то вони називаються *взаємно простими*.

Найбільшим спільним дільником (н. с. д.) многочленів $f(x)$ і $g(x)$ називається такий їх спільний дільник $d(x)$, який ділиться на всі інші спільні дільники цих многочленів. Найбільший спільний дільник многочленів $f(x)$ і $g(x)$ позначатимемо так: $d(x)=(f(x),g(x))$.

Для відшукання н. с. д. многочленів $f(x)$ і $g(x)$ можна застосувати алгоритм Евкліда, який полягає в наступному. Ділимо $f(x)$ на $g(x)$ і одержуємо деяку остачу $r_1(x)$. Далі ділимо $g(x)$ на $r_1(x)$ (якщо $r_1(x)\neq 0$) і одержуємо остачу $r_2(x)$, ділимо $r_1(x)$ на $r_2(x)$ (якщо $r_2(x)\neq 0$) і т. д. Оскільки степені остач зменшуються, то на деякому кроці ділення здійсниться націло і процес зупиниться. Та остача $r_k(x)$, на яку націло поділилась попередня остача $r_{k-1}(x)$ і буде найбільшим спільним дільником многочленів $f(x)$ і $g(x)$. Для доведення запишемо викладене вище у виді ланцюга рівностей:

$$\begin{aligned}
&f(x)=g(x)q_1(x)+r_1(x),\\
&g(x)=r_1(x)q_2(x)+r_2(x),\\
&r_1(x)=r_2(x)q_3(x)+r_3(x),\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&r_{k-2}(x)=r_{k-1}(x)q_k(x)+r_k(x),\\
&r_{k-1}(x)=r_k(x)q_{k+1}(x).
\end{aligned}\qquad (11.2)$$

Остання рівність показує, що $r_k(x)$ є дільником для $r_{k-1}(x)$. Звідси випливає, що обидва доданки правої частини передостанньої рівності діляться на $r_k(x)$, а тому $r_k(x)$ буде дільником для $r_{k-2}(x)$. Далі аналогічно, піднімаючись вгору, ми одержимо, що $r_k(x)$ буде дільником для

$r_{k-3}(x),...,r_2(x),r_1(x)$. Звідси, в силу другої рівності, випливає, що $r_k(x)$ є дільником для $g(x)$, а тому, на основі першої рівності, - і для $f(x)$. Отже $r_k(x)$ - спільний дільник для $f(x)$ і $g(x)$.

Нехай тепер $\varphi(x)$ - довільний спільний дільник многочленів $f(x)$ і $g(x)$. В силу першої із рівностей (11.2) $r_1(x)$ теж ділиться на $\varphi(x)$. Переходячи до другої рівності, одержуємо, що $r_2(x)$ теж ділиться на $\varphi(x)$. Спускаючись вниз, аналогічно одержуємо, що всі остачі, включаючи і $r_k(x)$ діляться на $\varphi(x)$. Таким чином $r_k(x)$ - найбільший спільний дільник $f(x)$ і $g(x)$.

Ми довели, що будь-які два многочлени мають н. с. д. і одержали спосіб його обчислення. Цей спосіб показує, що якщо многочлени $f(x)$ і $g(x)$ належать $P[x]$, то і їх н. с. д. $d(x)$ теж належить $P[x]$. Зрозуміло, що н. с. д. двох многочленів визначений з точністю до множника нульового степеня. В зв'язку з цим можна домовитись, що старший коефіцієнт н. с. д. двох многочленів буде вважатись рівним одиниці. А тоді можна сказати, що многочлени взаємно прості, якщо їх н. с. д. дорівнює 1.

Теорема 11.1. Якщо $d(x)$ є найбільший спільний дільник многочленів $f(x)$ і $g(x)$, то існують такі многочлени $u(x)$ і $v(x)$, що

$$f(x)u(x)+g(x)v(x)=d(x). \qquad (11.3)$$

При цьому можна вважати, що якщо степені многочленів $f(x)$ і $g(x)$ більші нуля, що степінь $u(x)$ менший, ніж степінь $g(x)$, а степінь $v(x)$ менший, ніж степінь $f(x)$.

Доведення базується на рівностях (11.2). Якщо врахувати, що $d(x)=r_k(x)$ і покласти $u_1(x)=1$, $v_1(x)=-q_k(x)$, то передостання із рівностей (11.2) запишеться так:

$$d(x) = r_{k-2}(x)u_1(x) + r_{k-1}(x)v_1(x).$$

Підставивши сюди вираз для $r_{k-1}(x)$ із попередньої рівності:

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

одержуємо

$$d(x) = r_{k-3}(x)u_2(x) + r_{k-2}(x)v_2(x),$$

де $u_2(x) = v_1(x),\ v_2(x) = u_1(x) - v_1(x)q_{k-1}(x)$.

Продовжуючи підніматись вгору в рівностях (11.2), ми прийдемо, нарешті, до рівності (11.3).

Для доведення другої частини теореми припустимо, що в рівності (11.3), скажімо, степінь $u(x)$ більший, ніж степінь $g(x)$. Поділимо $u(x)$ на $g(x)$:

$$u(x) = g(x)q(x) + r(x),$$

де степінь $r(x)$ менший, ніж степінь $g(x)$, і підставимо цей вираз в (11.3). Одержимо

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

Степінь множника при $f(x)$, очевидно, менший, ніж степінь $g(x)$. Степінь многочлена, який стоїть в квадратних дужках буде меншим, ніж степінь $f(x)$, оскільки в противному випадку степінь другого доданка в лівій частині був би не менший, ніж степінь добутку $f(x)g(x)$, а враховуючи, що степінь добутку $f(x)r(x)$ менший, ніж степінь цього добутку, одержуємо, що степінь лівої частини не менший, ніж степінь добутку $f(x)g(x)$, тоді як многочлен $d(x)$ має завідомо менший степінь. Теорему доведено.

Одночасно ми одержуємо, що якщо коефіцієнти многочленів $f(x)$ і $g(x)$ належать полю P (тобто $f(x), g(x) \in P[x]$), то і коефіцієнти многочленів $u(x)$ і $v(x)$ будуть належати цьому ж полю.

Із доведеної теореми випливає наступний наслідок:

Многочлени $f(x)$ і $g(x)$ взаємно прості тоді і тільки тоді, коли знайдуться такі многочлени $u(x)$ і $v(x)$, які задовольняють рівності

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

Спираючись на цей результат, можна довести кілька тверджень про взаємно прості многочлени (пропонуємо їх як вправи):

1) Якщо многочлен $f(x)$ взаємно простий з кожним із многочленів $\varphi(x)$ і $\psi(x)$, то він взаємно простий і з їх добутком.

2) Якщо добуток многочленів $f(x)$ і $g(x)$ ділиться на $\varphi(x)$, але $f(x)$ і $\varphi(x)$ взаємно прості, то $g(x)$ ділиться на $\varphi(x)$.

3) Якщо многочлен $f(x)$ ділиться на кожний із многочленів $\varphi(x)$ і $\psi(x)$, які між собою взаємно прості, то $f(x)$ ділиться на їх добуток.

Вправи

1. Нехай $f(x)$ і $g(x)$ - многочлени над полем раціональних чисел. Знайти їх н. с. д., якщо:

1) $f(x)=6x+12,\ g(x)=4x-2$;

2) $f(x)=3x^3-2x^2+x+4,\ g(x)=x^2-x-1$;

3) $f(x)=2x^4+2x^3+x^2-x-1,$
$g(x)=3x^4+2x^2-x+2$;

4) $f(x)=x^4+3x^3-x^2-4x-3,$
$g(x)=3x^3+10x^2+2x-3$;

5) $f(x)=x^3-3x^2-2x+6,\quad g(x)=x^3+x^2-2x-2$.

2. Нехай $f(x)$ і $g(x)$ - многочлени над полем раціональних чисел. Знайти для них многочлени $u(x)$ і $v(x)$ так, щоб виконувалась рівність (11.3), якщо:

1) $f(x)=x^7-2x^6-x^5-11x^4-6x^3-4x^2+5x+14$,
$g(x)=x^2+x+2$;
2) $f(x)=3x^5-4x^4+x^3-3x^2+4x-1$,
$g(x)=3x^5+5x^4+x^3-x^2-3x+1$;
3) $f(x)=2x^4-4x^3-3x^2+7x-2$,
$g(x)=6x^3+4x^2-5x+1$;
4) $f(x)=x^3-x^2+3x-10$, $g(x)=x^3+6x^2-9x-14$;
5) $f(x)=2x^5-3x^4-5x^3+x^2+6x+3$,
$g(x)=3x^4+2x^3-3x^2-5x-2$.

12 Розклад в кільці многочленів

12.1 Незвідні многочлени

Нехай задано многочлен $f(x)$ степеня $n, n \geq 1,$ над полем P. Як відомо, всі многочлени нульового степеня є дільниками для $f(x)$. З другого боку, всі многочлени виду $cf(x)$, де c - відмінний від нуля елемент поля P, теж будуть дільниками для $f(x)$. Причому ними вичерпуються всі дільники многочлена $f(x)$, які мають степінь n. Що ж стосується дільників для $f(x)$, степінь яких більший 0, але менший n, то вони можуть в кільці $P[x]$ існувати, а можуть і не існувати. В першому випадку многочлен $f(x)$ називається *звідним* в полі P (або над полем P), в другому – *незвідним* в цьому полі.

Інакше, многочлен $f(x)$ степеня n звідний в полі P, якщо він може бути розкладений в кільці $P[x]$ в добуток двох многочленів, степені яких менші n:

$$f(x) = \varphi(x) \cdot \psi(x) \qquad (12.1)$$

і $f(x)$ незвідний в полі P, якщо в будь-якому його розкладі виду (12.1) один із співмножників має степінь 0, а інший – степінь n.

Відзначимо, що говорити про звідність чи незвідність многочлена можна тільки по відношенню до даного поля P, оскільки многочлен, незвідний в цьому полі, може виявитись звідним в деякому його розширенні. Так, многочлен $x^2 - 2$ незвідний в полі раціональних чисел, але він звідний в полі дійсних чисел: $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

Наведемо деякі властивості незвідних многочленів.

1) Всякий многочлен першого степеня незвідний.

2) Якщо многочлен $p(x)$ незвідний, то незвідним буде і всякий многочлен виду $cp(x)$, де $c \neq 0$ - елемент поля P.

3) Якщо $f(x)$ - довільний, а $p(x)$ - незвідний многочлен, то або $f(x)$ ділиться на $p(x)$, або ці многочлени взаємно прості.

4) Якщо добуток двох многочленів $f(x)$ і $g(x)$ ділиться на незвідний многочлен $p(x)$, то хоча б один із цих множників ділиться на $p(x)$.

Остання властивість легко узагальнюється на випадок будь-якого скінченного числа співмножників.

12.2 Розклад многочленів на незвідні множники

Ми вже відзначали деяку схожість між кільцями цілих чисел і многочленів. Ця схожість проявляється і ще в одному. Як відомо, всяке ціле число можна розкласти в добуток простих множників. Щось подібне має місце і в кільці многочленів, якщо роль простих множників будуть виконувати незвідні многочлени.

Легко довести, що всякий многочлен $f(x)$ із кільця $P[x]$ степеня n $(n \geq 1)$ розкладається в добуток незвідних множників. Справді, якщо $f(x)$ сам незвідний, то вказаний добуток складається із одного множника. Якщо ж він звідний, то може бути розкладений в добуток множників меншого степеня. Якщо серед цих множників знову є звідні, то розкладаємо їх на множники і т. д. Очевидно цей процес закінчиться після скінченного числа кроків і ми одержимо потрібний розклад.

А як бути з єдністю розкладу? Зауважимо, що якщо

$$f(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_s(x)$$

розклад многочлена $f(x)$ на незвідні множники і якщо $c_1, c_2, \ldots, c_s$ - елементи поля P такі, що $c_1 \cdot c_2 \cdot \ldots \cdot c_s = 1$, то

$$f(x) = \left[c_1 p_1(x)\right] \cdot \left[c_2 p_2(x)\right] \cdot \ldots \cdot \left[c_s p_s(x)\right]$$

теж буде розкладом $f(x)$ на незвідні множники. Виявляється, цим вичерпуються всі розклади $f(x)$. А саме, якщо многочлен $f(x)$ із кільця $P[x]$ двома

способами розкладений в добуток незвідних множників

$$f(x)=p_1(x)p_2(x)\dots p_s(x)=q_1(x)q_2(x)\dots q_t(x), \quad (12.2)$$

то $s=t$ і при відповідній нумерації мають місце рівності

$$q_i(x)=c_i p_i(x), \quad i=1,2,\dots,s, \quad (12.3)$$

де c_i - відмінні від нуля елементи поля P.

Доведення цього твердження можна провести індукцією по n (n - степінь многочлена $f(x)$). При $n=1$ твердження очевидне. Нехай $n>1$, припустимо, що для многочленів меншого степеня твердження доведене. Оскільки $q_1(x)$ - дільник $f(x)$, то в силу рівності (12.2) і властивості 4) $q_1(x)$ буде дільником хоча б одного із многочленів $p_i(x)$, наприклад $p_1(x)$. Але многочлен $p_1(x)$ - незвідний, а степінь $q_1(x)$ більший нуля, отже існує елемент $c_1\in P$ такий, що $q_1(x)=c_1p_1(x)$. Підставляючи цей вираз в (12.2) і скорочуючи на $p_1(x)$ (що законно, оскільки в кільці $P[x]$ нема дільників нуля), одержуємо

$$p_2(x)p_3(x)\dots p_s(x)=\left[c_1q_2(x)\right]q_3(x)\dots q_t(x).$$

Оскільки степінь многочлена, який дорівнює цим добуткам, менший n, то уже доведено, що $s-1=t-1$, тобто $s=t$, і існують такі елементи $c_2', c_3,\dots,c_s$, що $c_2'p_2(x)=c_1q_2(x)$, звідси $q_2(x)=c_1^{-1}c_2'p_2(x)$ і $c_ip_i(x)=q_i(x)$, $i=3,\dots,s$. Поклавши $c_1^{-1}c_2'=c_2$, ми повністю одержуємо рівності (12.3).

Одержаному результату можна надати такого формулювання: всякий многочлен розкладається на незвідні множники однозначно з точністю до множників нульового степеня.

Але можна розглядати розклад наступного спеціального виду, який буде, очевидно, однозначним

$$f(x)=a_0p_1(x)p_2(x)\dots p_s(x), \quad (12.4)$$

де a_0 - старший коефіцієнт многочлена $f(x)$, а старші коефіцієнти незвідних многочленів $p_1(x),\dots,p_s(x)$

дорівнюють одиниці.

В розкладі (12.4) множники $p_i(x)$, $i=1,2,...,s$, не зобов'язані бути різними. Якщо незвідний многочлен $p(x)$ зустрічається в розкладі k раз, то він називається k-кратним. Збираючи однакові співмножники, розклад (12.4) можна записати у виді

$$f(x)=a_0 p_1^{k_1}(x)\,p_2^{k_2}(x)\ldots p_l^{k_l}(x), \qquad (12.5)$$

де k_i - кратність множника $p_i(x)$.

Якщо відомі розклади двох многочленів на незвідні множники, то легко знайти їх н. с. д., а саме: н. с. д. двох многочленів дорівнює добутку множників, які входять в обидва розклади, причому кожний множник береться в степені, який дорівнює меншій із його кратностей в обидвох даних многочленах.

Вправи

1. Нехай $f(x)$ і $g(x)$ - многочлени над полем раціональних чисел. Вияснити, з якою кратністю входить многочлен $g(x)$ в многочлен $f(x)$, якщо:

1) $f(x)=x^5-3x-3,\quad g(x)=x^2-2x-2$;

2) $f(x)=x^5+x^4-8x^3-8x^2+16x+16,\ \ g(x)=x^2-4$.

13 Розширення полів

13.1 Алгебраїчне розширення поля

Як відомо, можлива така ситуація, коли многочлен з коефіцієнтами з поля P не має в цьому полі коренів, але має їх в деякому розширенні поля P. Наприклад, многочлен x^2+1 з дійсними коефіцієнтами не має дійсних коренів, але має корені в полі комплексних чисел, яке є розширенням поля дійсних чисел.

Нехай дано многочлен $f(x)$ над полем P. Якщо многочлен $f(x)$ взагалі не має коренів в полі P, то чи існує таке розширення $\overline{P}$ поля P, в якому для $f(x)$ існує хоча б один корінь? При цьому можна вважати, що степінь $f(x)$ більший 1, оскільки для многочленів нульового степеня питання взагалі позбавлене сенсу, а многочлен першого степеня $ax+b$ має корінь $-\frac{b}{a}$ в самому полі P. З другого боку, можна обмежитись, очевидно випадком, коли $f(x)$ незвідний многочлен.

Приймемо без доведення, що для всякого многочлена $f(x)$, незвідного над полем P існує таке розширення $\overline{P}$ цього поля, в якому міститься корінь для $f(x)$.

Нехай

$$f(x)=a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_n, \qquad (13.1)$$

де $n\geq 2$, незвідний над полем P многочлен, який не має коренів в полі P і α - корінь $f(x)$, який міститься в розширенні $\overline{P}$. Знайдемо мінімальне підполе $P(\alpha)$ поля $\overline{P}$, яке містить поле P і елемент α.

Попередньо доведемо, що якщо α є коренем деякого іншого многочлена $g(x)$ із кільця $P[x]$, то $f(x)$ буде дільником для $g(x)$. Справді, над полем $\overline{P}$ $f(x)$і $g(x)$ мають спільний дільник $x-\alpha$ і тому не є взаємно простими, Властивість многочленів бути взаємно простими не залежить, очевидно, від вибору поля, тому можна перейти до поля P і скористатись властивістю 3) із 12.1.

Полю $P(\alpha)$ завідомо належать всі елементи виду

$$\beta = b_0\alpha^{n-1} + b_1\alpha^{n-2} + ... + b_{n-2}\alpha + b_{n-1}, \qquad (13.2)$$

де $b_0, b_1, ..., b_{n-1}$ - елементи поля P. Ніякий елемент поля $\overline{P}$ не може мати двох різних представлень (13.2); якщо припустити, що має місце рівність

$$\beta = c_0\alpha^{n-1} + c_1\alpha^{n-1} + ... + c_{n-2}\alpha + c_{n-1},$$

причому хоча б при одному k $c_k \neq b_k$, то α буде коренем многочлена

$$g(x) = (b_0 - c_0)\alpha^{n-1} + (b_1 - c_1)\alpha^{n-2} + ... + (b_{n-2} - c_{n-2})\alpha + (b_{n-1} - c_{n-1}),$$

що неможливо, оскільки степінь $g(x)$ менший, ніж степінь $f(x)$, а в силу доведеного вище $f(x)$ повинен бути дільником $g(x)$.

До числа елементів поля $\overline{P}$, які мають вид (13.2) належать всі елементи поля P (при $b_0 = b_1 = ... = b_{n-2} = 0$), а також сам елемент α (при $b_0 = b_1 = ... = b_{n-3} = b_{n-1}$, $b_{n-2} = 1$). Доведемо, що елементи виду (13.2) складають все шукане поле $P(\alpha)$. Справді, сума і різниця елементів виду (13.2) будуть, очевидно, елементами такого ж виду. Доведемо, що і добуток елементів виду (13.2) має ту ж властивість. Нехай

$$\gamma = c_0\alpha^{n-1} + c_1\alpha^{n-2} + ... + c_{n-2}\alpha + c_{n-1}.$$

Добуток $\beta\gamma$ містить α^n, а також більш високі степені α. Тому розглянемо многочлени

$$\varphi(x)=b_0x^{n-1}+b_1x^{n-2}+...+b_{n-2}x+b_{n-1},$$
$$\psi(x)=c_0x^{n-1}+c_1x^{n-2}+...+c_{n-2}x+c_{n-1},$$

очевидно $\varphi(\alpha)=\beta$, $\psi(\alpha)=\gamma$. Добуток многочленів $\varphi(x)$ і $\psi(x)$ поділимо на $f(x)$:

$$\varphi(x)\psi(x)=f(x)q(x)+r(x),$$

де $r(x)=d_0x^{n-1}+d_1x^{n-2}+...+d_{n-2}x+d_{n-1}$. Звідси $\varphi(\alpha)\psi(\alpha)=f(\alpha)q(\alpha)+r(\alpha)$, або, в силу того, що $f(\alpha)=0$, $\beta\gamma=r(\alpha)$, тобто

$$\beta\gamma=d_0\alpha^{n-1}+d_1\alpha^{n-2}+...+d_{n-2}\alpha+d_{n-1}.$$

Доведемо, нарешті, що елемент $\beta\neq 0$ виду (13.2) має обернений β^{-1}, який теж може бути записаний у такому ж виді. Для цього візьмемо многочлен

$$\varphi(x)=b_0x^{n-1}+b_1x^{n-2}+...+b_{n-2}x+b_{n-1}.$$

Оскільки степінь $\varphi(x)$ менший, ніж степінь $f(x)$, а $f(x)$ незвідний над P, то $f(x)$ і $\varphi(x)$ взаємно прості, тому в кільці $P[x]$ існують такі многочлени $u(x)$ і $v(x)$, що

$$\varphi(x)u(x)+f(x)v(x)=1,$$

при цьому можна вважати, що степінь $u(x)$ менший n:

$$u(x)=s_0x^{n-1}+s_1x^{n-2}+...+s_{n-2}x+s_{n-1}.$$

Звідси (враховуючи, що $f(\alpha)=0$) маємо $\varphi(\alpha)u(\alpha)=1$. І тому, в силу рівності $\varphi(\alpha)=\beta$, одержуємо

$$\beta^{-1}=u(\alpha)=s_0\alpha^{n-1}+s_1\alpha^{n-2}+...+s_{n-2}\alpha+s_{n-1}.$$

Отже, сукупність елементів поля $\overline{P}$, які мають вид (13.2) складає підполе поля $\overline{P}$, це і буде шукане поле $P(\alpha)$.

13.2 Поле розкладу

Нехай c - корінь многочлена $f(x)$. Оскільки всякий лінійний множник $x-c$ многочлена незвідний, то він повинен входити в той єдиний розклад на незвідні множники, яким володіє $f(x)$. Число ж лінійних множників в розкладі $f(x)$ на незвідні множники не може перевищувати степеня цього многочлена. Тому многочлен $f(x)$ степеня n може мати в полі P не більше n коренів, якщо навіть кожний корінь рахувати стільки разів, яка його кратність.

Назвемо *полем розкладу* для многочлена $f(x)$ степеня n над полем P таке розширення R поля P, в якому для $f(x)$ міститься n коренів (з урахуванням їх кратності). Над полем R многочлен $f(x)$ буде розкладатись, таким чином, на лінійні множники, причому ніяке подальше розширення поля R не може привести до появи нових коренів у $f(x)$.

Очевидно, для всякого многочлена $f(x)$ із кільця $P[x]$ існує над полем P поле розкладу.

Дійсно, якщо многочлен $f(x)$ степеня $n \geq 1$ має n коренів в самому полі P, то P і буде шуканим полем розкладу. Якщо ж $f(x)$ не розкладається над P на лінійні множники, то беремо один із його незвідних нелінійних множників $\varphi(x)$ і розширюємо P до поля P', яке містить корінь для $\varphi(x)$. Якщо над P' многочлен $f(x)$ все ще не розкладається на лінійні

множники, то знову розширюємо поле, створюючи корінь для одного із нелінійних множників, що залишився. Після скінченного числа кроків ми прийдемо, очевидно, до поля розкладу для $f(x)$.

14 Многочлени з раціональними коефіцієнтами

14.1 Примітивні многочлени

Поле раціональних чисел $\mathbb{Q}$ є найменшим серед усіх числових полів, воно є підполем будь-якого числового поля. Нас буде цікавити питання звідності многочленів над полем $\mathbb{Q}$, а також питання про раціональні корені многочленів з раціональними коефіцієнтами. Це два різних питання: многочлен

$$x^4 + 2x^2 + 1 = \left(x^2 + 1\right)^2$$

звідний над полем раціональних чисел, хоча не має жодного раціонального кореня.

Зауважимо, перш за все, що якщо дано многочлен $f\left(x\right)$, коефіцієнти якого раціональні, але не всі цілі, то зводячи коефіцієнти до спільного знаменника і множачи многочлен на цей спільний знаменник, скажімо k, ми одержимо многочлен $kf\left(x\right)$, всі коефіцієнти якого будуть цілими числами. Очевидно, що многочлени $f\left(x\right)$ і $kf\left(x\right)$ мають однакові корені і, крім того, вони одночасно будуть звідні чи незвідні над полем $\mathbb{Q}$.

Многочлен $f\left(x\right)$ з цілими коефіцієнтами називається *примітивним*, якщо його коефіцієнти взаємно прості в сукупності, тобто не мають спільних дільників, відмінних від 1 і –1. Якщо дано довільний многочлен з раціональними коефіцієнтами $\varphi\left(x\right)$, то його можна представити у виді добутку деякого нескоротного дробу на примітивний многочлен:

$$\varphi\left(x\right) = \frac{a}{b} f\left(x\right); \qquad (14.1)$$

для цього потрібно винести за дужки спільний знаменник всіх коефіцієнтів многочлена $\varphi\left(x\right)$, а потім і спільні множники із чисельників цих коефіцієнтів. Легко довести однозначність (з точністю до знаку) представлення (14.1) (самостійно).

Для цілочисельних примітивних многочленів справедлива

Лема 14.1 (Гаусса). Добуток двох цілочисельних примітивних многочленів сам є примітивний многочлен.

Доведення. Нехай

$$f(x) = a_0 x^k + a_1 x^{k-1} + ... + a_i x^{k-i} + ... + a_k ,$$

$$g(x) = b_0 x^l + b_1 x^{l-1} + ... + b_j x^{l-j} + ... + b_l$$

примітивні многочлени і нехай

$$f(x) \cdot g(x) = c_0 x^{k+l} + c_1 x^{k+l-1} + ... + c_{i+j} x^{(k+l)-(i+j)} + ... + c_{k+l} .$$

Якщо цей добуток не примітивний, то існує просте число p, яке буде спільним дільником всіх коефіцієнтів $c_0, c_1, ..., c_{k+l}$. Оскільки всі коефіцієнти примітивного многочлена $f(x)$ не можуть ділитись на p, то нехай коефіцієнт a_i є перший, який не ділиться на p; аналогічно через b_j позначимо перший коефіцієнт многочлена $g(x)$, який не ділиться на p. Якщо в добутку $f(x) \cdot g(x)$ зібрати члени, які містять $x^{(k+l)-(i+j)}$, то ми одержимо

$$c_{i+j} = a_i b_j + a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + ... + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + ...$$

Ліва частина цієї рівності ділиться на p. На нього за відомо діляться також всі доданки правої частини, крім першого, що неможливо. Лему доведено.

14.2 Звідність многочленів над полем раціональних чисел

Нехай, тепер, многочлен $g(x)$ степеня n з цілими коефіцієнтами звідний над полем раціональних чисел:

$$g(x) = \varphi_1(x) \varphi_2(x),$$

де $\varphi_1(x), \varphi_2(x)$ - многочлени з раціональними коефіцієнтами і їх степені менші n. Тоді

$$\varphi_i(x) = \frac{a_i}{b_i} f_i(x), \quad i = 1, 2 ,$$

де $\frac{a_i}{b_i}$ - нескоротні дроби, $f_i(x)$ - примітивні многочлени.

Звідси

$$g(x)=\frac{a_1a_2}{b_1b_2}\left[f_1(x)f_2(x)\right].$$

Оскільки ліва частина – цілочисельний многочлен, то знаменник b_1b_2 правої частини повинен скоротитись. Але многочлен $f_1(x)f_2(x)$, за лемою Гаусса, примітивний, тому a_1a_2 повинно поділитись на b_1b_2. Враховуючи, що a_1 взаємно просте з b_1, а a_2 - з b_2, одержуємо, що a_1 повинно поділитись на b_2, а a_2 - на b_1 : $a_2=b_1a_2'$, $a_1=b_2a_1'$. Звідси

$$g(x)=a_1'a_2'f_1(x)f_2(x).$$

Тепер множник $a_1'a_2'$ можна приєднати до одного з многочленів $f_1(x)$ чи $f_2(x)$ і одержати розклад многочлена $g(x)$ на множники меншого степеня з цілими коефіцієнтами. Цим доведена

Теорема 14.1. Многочлен з цілими коефіцієнтами, незвідний над кільцем цілих чисел, буде незвідним і над полем раціональних чисел.

Таким чином, при розгляді питання звідності многочленів над полем раціональних чисел, можна обмежитись розглядом розкладів цілочисельних многочленів на множники, всі коефіцієнти яких теж цілі.

Як відомо, над полем комплексних чисел звідний всякий многочлен, степінь якого більший одиниці, а над полем дійсних чисел – всякий многочлен, степінь якого більший двох. Що ж стосується поля раціональних чисел, то тут становище зовсім інше: для будь-якого n можна вказати многочлен n-го степеня з раціональним (навіть цілими) коефіцієнтами, незвідний над полем раціональних чисел. Доведення цього факту базується на наступній достатній умові незвідності многочлена над полем раціональних чисел, яка називається *критерієм Ейзенштейна*:

Нехай дано многочлен

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

з цілими коефіцієнтами. Якщо хоча б одним способом можна підібрати просте число p, яке задовольняє вимогам:

1) a_0 не ділиться на p,

2) всі решта коефіцієнти діляться на p,

3) a_n ділячись на p, не ділиться на p^2,

то многочлен $f(x)$ незвідний над полем раціональних чисел.

Справді, якщо припустити, що многочлен $f(x)$ звідний над полем $\mathbb{Q}$, то він розкладається на два множники меншого степеня з цілими коефіцієнтами:

$f(x)=(b_0x^k+b_1x^{k-1}+...+b_k)(c_0x^l+c_1x^{l-1}+...+c_l)$,

де $k<n$, $l<n$, $k+l=n$. Звідси, порівнюючи коефіцієнти в обидвох частинах цієї рівності, одержуємо:

$$\begin{aligned}
a_n &= b_kc_l,\\
a_{n-1} &= b_kc_{l-1}+b_{k-1}c_l,\\
a_{n-2} &= b_kc_{l-2}+b_{k-1}c_{l-1}+b_{k-2}c_l, \qquad (14.2)\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
a_0 &= b_0c_0\ .
\end{aligned}$$

Із першої із рівностей (14.2) випливає, оскільки a_n ділиться на p, а число p просте, що один із множників b_k, c_l повинен ділитися на p. Обидва вони не можуть ділитись на p, тому що a_n, за умовою, не ділиться на p^2. Нехай, наприклад, b_k ділиться на p і тому c_l взаємно просте з p. Переходимо тепер до другої із рівностей (14.2). Її ліва частина, а також перший доданок правої частини діляться на p, тому на p ділиться і добуток $b_{k-1}c_l$; оскільки c_l на p не ділиться, то на p буде ділитись b_{k-1}. Таким же чином із третьої рівності (14.2) ми одержимо, що b_{k-2} ділиться на p, і т. д. Нарешті із $(k+1)$-ї рівності буде одержано, що на p ділиться b_0; але тоді із останньої із рівностей (14.2) випливає, що на p ділиться a_0, що суперечить припущенню.

Дуже легко для будь-якого n написати цілочисельні многочлени n-го степеня, які задовольняють умовам критерію Ейзенштейна і, таким чином, незвідні над полем раціональних чисел. Таким, наприклад, є многочлен $x^n + 2$; до нього можна застосувати критерій Ейзенштейна при $p = 2$.

Вправи

1. Довести незвідність многочленів, користуючись критерієм Ейзенштейна:

1) $x^4 - 8x^3 + 12x^2 - 6x + 2$;
2) $x^5 - 12x^3 + 36x - 12$;
3) $3x^7 - 4x^6 + 2x^5 - 6x^3 - 8x - 2$;
4) $x^4 - x^3 + 2x + 1$;
5) $x^4 + x^3 + x^2 + x + 1$;
6) $x^5 + 5x + 9$.

2. Довести незвідність многочленів:

1) $f(x) = x^{p-1} + x^{p-2} + ... + 1$ (p - просте число) ;

2) $f(x) = \dfrac{x^p - 1}{x - 1}$ (p - просте число) ;

3)* $f(x) = \dfrac{x^{p^k} - 1}{x^{p^{k-1}} - 1}$ (p - просте число).

3. Довести, що многочлен третього степеня незвідний, якщо він не має раціональних коренів.

4. Довести незвідність многочлена $f(x) = (x - a_1)(x - a_2)...(x - a_n) - 1$, де $a_1, a_2, ..., a_n$ - різні між собою цілі числа.

15 Поля Галуа

15.1 Скінченні розширення скінченних полів

Поле, число елементів якого скінченне, називається *полем Галуа*. Поле Галуа з q елементами позначається $GF(q)$ (Galois Field – поле Галуа). Як відомо, один із способів вивчення полів – відштовхуючись від простих полів – одержувати опис всіх полів, вивчаючи структуру розширень.

Ми вже розглядали алгебраїчне розширення поля, яке одержується приєднанням до поля P кореня α деякого незвідного над полем P многочлена $f(x)$. Як відомо, таке розширення ототожнюється з множиною елементів виду

$$a_0\alpha^{n-1} + a_1\alpha^{n-2} + ... + a_{n-2}\alpha + a_{n-1},$$

де $a_0, a_1, ..., a_{n-1}$ - елементи поля P, n - степінь многочлена $f(x)$. Одержане таким чином розширення F поля P можна вважати векторним простором над полем P з базисними елементами $\alpha^{n-1}, \alpha^{n-2}, ..., \alpha, 1$.

У випадку довільного розширення $F \supset P$ також доцільно розглядати F як векторний простір над P. При цьому його розмірність називається *степенем розширення* F над P. Важливий клас алгебраїчних розширень складають *скінченні розширення*, тобто розширення, які є скінченновимірними векторними просторами над P.

Розглянемо детальніше такого роду розширення полів. Нехай поле P є підполем поля F. Елементи $\alpha_1, \alpha_2, ..., \alpha_k$ поля F називаються *лінійно залежними* над полем P, якщо існують такі елементи $a_1, a_2, ..., a_k$ поля P, не всі рівні нулю, що

$$a_1\alpha_1 + a_2\alpha_2 + ... + a_k\alpha_k = 0.$$

В противному випадку елементи $\alpha_1, \alpha_2, ..., \alpha_k$ називаються *лінійно незалежними* над полем P.Зрозуміло, що якщо поле F скінченне, то максимальна кількість лінійно незалежних його елементів над будь-яким підполем P буде скінченною. Нехай максимальна кількість елементів поля F, лінійно незалежних

над полем P, дорівнює n. Позначимо ці елементи $\alpha_1, \alpha_2, ..., \alpha_n$. Якщо до них добавити будь-який елемент α поля , то система елементів $\alpha_1, \alpha_2, ..., \alpha_n, \alpha$ буде вже лінійно залежною над P, тобто виконається рівність

$$a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n + a_{n+1}\alpha = 0,$$

де $a_1, a_2, ..., a_n, a_{n+1}$ - елементи поля P, причому, очевидно, $a_{n+1} \neq 0$. Тоді

$$\alpha = -a_{n+1}^{-1}a_1\alpha_1 - a_{n+1}^{-1}a_2\alpha_2 - ... - a_{n+1}^{-1}a_n\alpha_n.$$

Тобто, всякий елемент поля F може бути представлений як лінійна комбінація елементів $\alpha_1, \alpha_2, ..., \alpha_n$ з коефіцієнтами із поля P. Причому таке представлення єдине (довести самостійно). За своєю будовою поле F є не чим іншим, як n-вимірним векторним простором над полем P; елементи $\alpha_1, \alpha_2, ..., \alpha_n$ є базисом цього простору.

Враховуючи, що кожний елемент β поля F однозначно представляється у виді

$$\beta = a_1\alpha_1 + a_2\alpha_2 + ... + a_n\alpha_n, \qquad (15.1)$$

де кожен із коефіцієнтів $a_1, a_2, ..., a_n$ може незалежно від інших набувати q значень, де q - кількість елементів поля P, можна зробити висновок, що кількість елементів поля F дорівнює q^n.

Ще одне зауваження полягає в тому, що всяке скінченне поле F має скінченну характеристику p (p - просте число) і кількість елементів поля F є степенем p. Справді, просте підполе $P \subset F$ в силу скінченності F повинно бути ізоморфне деякому полю $\mathbb{Z}(p)$, яке, як відомо, містить p елементів. Згідно сказаного вище, якщо скінченне розширення $F \supset P$ має степінь n, то кількість елементів F є p^n. Надалі таке поле позначатимемо $GF(p^n)$.

Виключаючи з числа елементів поля $F = GF(p^n)$ нульовий, одержуємо мультиплікативну групу $F^* = F \setminus \{0\}$

порядку p^n-1. Нехай x - довільний елемент цієї групи. Якщо цей елемент має порядок k, тобто $x^k=1$, де 1 - одиниця поля F, то згідно з наслідком із теореми Лагранжа, k є дільником p^n-1: $p^n-1=kq$. Тоді $x^{p^n-1}=\left(x^k\right)^q=1^q=1$. Отже, всі ненульові елементи поля F задовольняють рівнянню

$$x^{p^n-1}-1=0. \qquad (15.2)$$

А рівнянню

$$x^{p^n}-x=0 \qquad (15.3)$$

задовольняють усі без винятку елементи поля F (включаючи 0). Таким чином, поле $GF\left(p^n\right)$ можна визначити як поле розкладу многочлена $x^{p^n}-x$. Тобто, справедлива рівність

$$x^{p^n}-x=x\left(x-a\right)\left(x-b\right)...\left(x-c\right),$$

де $a,b,...,c$ - всі ненульові елементи поля F.

15.2 Мультиплікативна група поля Галуа

Доведемо тепер, що мультиплікативна група F^* скінченого поля $GF\left(p^n\right)$ є циклічною групою порядку p^n-1. Доведення спиратиметься на дві леми.

Лема 15.1. Нехай a і b - перестановочні елементи групи G, які мають взаємно прості порядки s і t. Тоді елемент ab цієї групи має порядок st.

Доведення. Зауважимо спочатку, що $\langle a\rangle\bigcap\langle b\rangle=1$. Справді, якщо для деякого елемента d групи, який має порядок q, справедливі представлення $d=a^i=b^j$, то

$$d^s=\left(a^s\right)^i=1, \qquad d^t=\left(b^t\right)^j=1,$$

тобто q є дільником для s і для t. Із взаємної простоти s і t випливає, що $q=1$, тобто $d=1$.

Якщо, далі, елемент ab має порядок n, то $a^nb^n=\left(ab\right)^n=1$. Звідси $a^n=b^{-n}\in\langle a\rangle\bigcap\langle b\rangle$, тому $a^n=b^{-n}=1$. А це означає, що $a^n=1,\ b^n=1$. Отже, s і t є

дільниками n, а, значить, n ділиться на добуток st. Але $(ab)^{st} = (a^s)^t (b^t)^s = 1 \cdot 1 = 1$, тому st ділиться на n. Звідси випливає, що $n = st$. Лему доведено.

Показником групи G називається найменше натуральне число m таке, що $a^m = 1$ для всіх $a \in G$. Очевидно, для скінченної групи G таке число m існує, воно дорівнює найменшому спільному кратному порядків всіх елементів групи (довести самостійно). Справедлива

Лема 15.2. Абелева група G є циклічною тоді і тільки тоді, коли її показник співпадає з її порядком.

Доведення. Твердження про те, що показник циклічної групи співпадає з її порядком є очевидним.

Доведемо зворотне: нехай показник m групи G співпадає з її порядком. Доведемо, що ця група циклічна. Для цього, очевидно, досить довести, що в групі G знайдеться елемент, порядок якого дорівнює порядку групи, тобто m. Припустимо супротивне – порядки всіх елементів групи G строго менші m. Нехай a - елемент, який має найбільший порядок, позначимо його k. Може статись, що всі решта елементи групи G, відмінні від одиничного, теж мають порядок k. Тоді найменше спільне кратне порядків всіх елементів групи G, з одного боку дорівнює k, а з другого - m. Тобто, в цьому випадку порядки всіх елементів групи, відмінних від одиничного, дорівнюють її порядку. Таким чином, група G - циклічна, причому за твірний елемент можна взяти будь-який елемент цієї групи, відмінний від одиниці.

Нехай, тепер, в групі G є елементи, порядки яких строго менші k. Доведемо, що всі ці порядки є дільниками k. Припустимо протилежне: знайдеться елемент b, порядок якого $q < k$ і q не є дільником k. Існують дві можливості: q і k - взаємно прості. Тоді за попередньою лемою елемент ab матиме порядок $kq > k$, що суперечить тому, що a - елемент, який має найбільший порядок. Якщо ж q і k не є взаємно простими, то q можна представити у виді $q = st$, де один із співмножників, скажімо, t, взаємно простий з k. Розглянемо елемент $c = b^s$. Цей елемент має порядок t:

$$c^t = (b^s)^t = b^{st} = b^q = 1.$$

Тоді елемент ac за тою ж лемою 15.1 буде мати порядок $kt > k$. Отже, порядки всіх елементів групи G є дільниками k. Це означає, що і m, як найменше спільне кратне порядків всіх елементів групи G, є дільником k. Але, оскільки $k \le m$, то $k = m$. Це означає, що $G = \langle a \rangle$, тобто група G циклічна, породжена елементом a. Лему доведено.

Нехай тепер F^* - мультиплікативна група поля $F = GF\left(p^n\right)$. Порядок цієї групи дорівнює $p^n - 1$. Нехай m - показник групи F^*. Припустимо, що $m < p^n - 1$. Тоді, враховуючи, що $x^m = 1$ для будь-якого $x \in F^*$, одержуємо, що многочлен $x^m - 1$ має в полі F більше, ніж m коренів, що неможливо. Тому $m = p^n - 1$. А це означає, що група F^* циклічна. Зауважимо, що твірний елемент мультиплікативної групи поля Галуа називається *примітивним елементом*.

Вправи

1. Довести, що в будь-якому базисі векторного простору F над полем P кількість елементів одна і та ж.

2. Довести, що кожен елемент поля $GF\left(p^n\right)$ може бути представлений у виді

$$r_1 e_1 + r_2 e_2 + ... + r_n e_n,$$

де $e_1, e_2, ..., e_n$ - певні елементи цього поля, $r_k, k = 1, 2, ..., n,$ - цілі числа, кожне з яких незалежно від інших набуває значень $0, 1, 2, ..., p - 1$.

3. Довести, що розширення $F \supset P$ простого степеня не має власних ($\neq P, F$) підполів.

4. Знайти розмірність над $\mathbb{Q}$ поля розкладу многочлена $x^p - 2$.

5. Знайти примітивний елемент в полі $\mathbb{Z}(7)$.

Перелік використаних джерел

1. Курош А.Г. Курс высшей алгебры. – М.: Наука, 1968.
2. Кострикин А.И. Введение в алгебру. – М.: Наука, 1977.
3. Скорняков Л.А. Элементы алгебры. – М.: Наука, 1980.
4. Мишина А.П., Проскуряков И.В. Высшая алгебра. Линейная алгебра, многочлены, общая алгебра. – М.: Физматгиз, 1962.
5. Фор Р., Кофман А., Дени-Папен М. Современная математика. – М.: Мир, 1966.
6. Александров П.С. Введение в теорию групп. – М.: Наука, 1980.
7. Алексеев В.Б. Теорема Абеля в задачах и решениях. – М.: Наука, 1976.
8. Завало С.Т. Комплексні числа. – К.: Вища школа, 1982.
9. Калужнін Л.А., Сущанський В.І. Перетворення і підстановки. – К.: Вища школа, 1976.
10. Окунев Л.Я. Высшая алгебра. – М.: Просвещение, 1966.
11. Аршинов М.Н., Садовский Л.Е. Коды и математика. – М.: Наука, 1983.