Содержание

Введение

"Алгебра – живая ветвь математики, обладающая значительной притягательной силой и основывающаяся на небольшом числе ясных, интуитивных начал" (А.И. Кострикин).

В предлагаемой работе рассматриваются основные алгебраические структуры: группы, кольца, поля и некоторые обобщающие их структуры.

Каждое понятие иллюстрируется на примерах.

Алгебраическая структура есть множество вместе с бинарными операциями, определенными на этом множестве.

Особое внимание в работе уделено конечным полям или полям Галуа (Galois Field). Так (после XIX века) иногда называют конечные поля по имени французского математика Галуа.

Эвари́ст Галуа́ — выдающийся французский математик, основатель современной высшей алгебры. Радикальный революционер-республиканец, он был застрелен на дуэли при неоднозначных обстоятельствах в возрасте двадцати лет.

Конечные поля находят широкое применение в теории и технике помехоустойчивого кодирования. В работе приводятся примеры конечных полей, представляющих интерес для криптографии.

В тексте иногда приводятся несколько названий или обозначений одного и то же понятия, так как имеются разночтения в литературе.

В предложенном пособии автор использовал уже имеющийся опыт [1-11] по преподаванию данной дисциплины.

1. Группоид. Полугруппа. Группа

Определение бинарной алгебраической операции. Пусть X — произвольное множество. Бинарной алгебраической операцией на X называется произвольное (но фиксированное) отображение $\tau : X \times X \to X$ декартова квадрата $X^2 = X \times X$ в X.

Таким образом, любой упорядоченной паре (a,b) элементов $a,b \in X$ ставится в соответствие однозначно определенный элемент $\tau(a,b)$ того же множества X. Иногда вместо $\tau(a,b)$ пишут $a\tau b$, а еще чаще бинарную операцию на X обозначают каким-нибудь специальным символом: $*, \circ, \cdot, +$. Заметим, что $a \cdot b$ называют **произведением**, а $a+b$ — **суммой**. В дальнейшем бинарная операция чаще будет обозначаться ab, без всякого значка между a и b.

Определение группоида. Всякое непустое множество, в котором задана алгебраическая операция, называется группоидом.

Для проверки того, что множество X является группоидом (X,τ) относительно операции τ необходимо проверить **замкнутость** X относительно τ, т.е. что $\tau(a,b) \in X$ для любых $a,b \in X$.

Пример. Пусть X – множество комплексных чисел, обозначаемое в дальнейшем C. Суммой двух комплексных чисел $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ называется комплексное число $z = x_1 + x_2 + i(y_1 + y_2)$. C — группоид относительно сложения (**аддитивный** группоид).

На множестве комплексных чисел C также задано произведение, определяемое следующим образом: $z_1 \cdot z_2 = (x_1 + iy_1)(x_2 + iy_2) = x_1x_2 - y_1y_2 + i(x_1y_2 + x_2y_1)$. C – группоид относительно умножения (**мультипликативный** группоид).

Определение полугруппы. Множество G с бинарной операцией называется полугруппой, если от операции требуется **ассоциативность**, т.е. $(ab)c = a(bc)$ для любых $a,b,c \in G$.

Для проверки того, что множество X является полугруппой (X,τ) относительно операции τ необходимо сначала установить, что (X,τ) — группоид, а затем проверить ассоциативность операции τ.

Пусть в G существует такой элемент e, называемый **единицей** (или нейтральным элементом), что $ae = ea = a$ для любого $a \in G$.

Пример. Единицей в C относительно сложения является нулевой элемент $z = 0$. Единицей в C относительно умножения является элемент $z = 1$.

Определение моноида. Полугруппа с единицей называется моноидом.

Примеры. а) C — полугруппа с единицей (моноид) как относительно умножения, так и относительно сложения.

б) Рассмотрим множество всех квадратных матриц фиксированной размерности $n \times n$ с элементами из целых чисел Z с операцией **симметрирования** $A \bullet B = AB + BA$.

Покажем, что операция $\bullet$ не ассоциативна:

$(A \bullet B) \bullet \tilde{C} = (AB + BA) \bullet \tilde{C} = AB\tilde{C} + BA\tilde{C} + \tilde{C}AB + \tilde{C}BA$;

$A \bullet (B \bullet \tilde{C}) = A \bullet (B\tilde{C} + \tilde{C}B) = AB\tilde{C} + A\tilde{C}B + B\tilde{C}A + \tilde{C}BA$.

Так как в общем случае для матриц $B(A\tilde{C} - \tilde{C}A) \neq (A\tilde{C} - \tilde{C}A)B$ и $BA\tilde{C} + \tilde{C}AB \neq A\tilde{C}B + B\tilde{C}A$, то операция не ассоциативна и множество не является полугруппой. Однако данное множество является группоидом.

Частным случаем **моноида** является группа.

Существуют два определения группы:

1 определение группы. Множество G с бинарной операцией называется **группой**, если

1) операция **ассоциативна**, т.е. $(ab)c = a(bc)$ для любых $a, b, c \in G$.

2) операция **гарантирует единицу**, т.е. в G существует такой элемент e, называемый единицей, что $ae = ea = a$ для любого $a \in G$.

3) операция **гарантирует обратные элементы**, т.е. для любого $a \in G$ существует $x \in G$, называемый обратным к a, что $ax = xa = e$.

Замечание. Если бинарная операция коммутативна, т.е. $ab = ba$, то группа называется **абелевой**.

Проверку того, что множество X является группой (X, τ) относительно операции τ, можно разбить на четыре части: а) (X, τ) — группоид, б) (X, τ) — полугруппа, в) (X, τ) — моноид, г) гарантировано существование обратных элементов.

Примеры. Множество целых чисел Z является абелевой группой относительно сложения, при этом для получения обратного элемента по сложению меняем знак на противоположный. Однако Z не является группой относительно умножения, так как целые числа за исключением ± 1 не обратимы. R_+ — множество положительных вещественных чисел, абелева мультипликативная группа. Множество всех невырожденных матриц $GL(R,n)$, в частности $GL(R,3)$ — матриц вида $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ с вещественными элементами a_{ij}, является группой относительно умножения, так как множество **замкнуто** относительно умножения, т.е. произведение двух невырожденных матриц — невырожденная матрица в силу свойства определителей. Кроме того, операция умножения ассоциативна, единичная матрица является единицей в группе, существует обратный элемент A^{-1}. В то же время $GL(R,3)$ не является абелевой, так как умножение не коммутативно.

Пример. Неотрицательное вещественное число $|z| = \sqrt{x^2 + y^2}$ называется **модулем** комплексного числа $z = x + iy$, а число $z^* = x - iy$, обозначаемое также как $\bar{z}$, называется **комплексно сопряженным** числу $z = x + iy$. Заметим, что $|z|^2 = zz^*$.

Определена операция деления комплексных чисел. Для любых двух комплексных чисел z_1 и $z_2 \neq 0$ существует только одно число z такое, что $z \cdot z_2 = z_1$. Это число называется частным чисел z_1 и z_2 и обозначается $z_1 : z_2$ или $\frac{z_1}{z_2}$. Если $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$, то

$$\frac{z_1}{z_2} = \frac{z_1\bar{z}_2}{z_2\bar{z}_2} = \frac{z_1\bar{z}_2}{|z_2|^2} = \frac{(x_1+iy_1)(x_2-iy_2)}{x_2^2+y_2^2} = \frac{x_1x_2+y_1y_2+i(x_2y_1-x_1y_2)}{x_2^2+y_2^2} = \frac{x_1x_2+y_1y_2}{x_2^2+y_2^2} + i\frac{x_2y_1-x_1y_2}{x_2^2+y_2^2}.$$

Следовательно, при $z \neq 0$ определен обратный элемент относительно умножения $\frac{1}{z} = \frac{\bar{z}}{|z|^2} = \frac{x}{x^2+y^2} - i\frac{y}{x^2+y^2}$. Если комплексное число $z \neq 0$ задано в показательной форме записи $z = |z|e^{i\arg z}$, то $\frac{1}{z} = \frac{1}{|z|}e^{-i\arg z}$. Множество всех комплексных чисел без нуля $C\setminus\{0\}$ является группой относительно умножения (мультипликативной группой).

В следующих двух теоремах доказываются свойства комплексных чисел, используемые в дальнейшем для иллюстрации алгебраических понятий.

Теорема 1.1 (о свойствах модуля и аргумента при умножении и делении комплексных чисел). При умножении двух комплексных чисел $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ их модули перемножаются (растяжение или сжатие) $|z_1z_2| = |z_1|\cdot|z_2|$, а аргументы складываются (поворот на плоскости) $\arg z_1z_2 = \arg z_1 + \arg z_2$; при делении двух комплексных чисел их модули делятся (модуль знаменателя не равен 0), а аргументы вычитаются.

Доказательство. Действительно, рассмотрим комплексные числа $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ в тригонометрической форме: $z_1 = |z_1|(\cos\arg z_1 + i\sin\arg z_1)$ и $z_2 = |z_2|(\cos\arg z_2 + i\sin\arg z_2)$. Тогда, используя правило умножения и известные тригонометрические формулы, получим

$$z_1z_2 = |z_1|\cdot(\cos\arg z_1 + i\sin\arg z_1)|z_2|(\cos\arg z_2 + i\sin\arg z_2) = |z_1||z_2|[\cos\arg z_1\cos\arg z_2 -$$
$$-\sin\arg z_1\sin\arg z_2 + i(\cos\arg z_1\sin\arg z_2 + \cos\arg z_2\sin\arg z_1)] =$$
$$= |z_1||z_2|[\cos(\arg z_1 + \arg z_2) + i\sin(\arg z_1 + \arg z_2)].$$

$$\frac{z_1}{z_2} = z_1\cdot\frac{1}{z_2} = |z_1|\cdot(\cos\arg z_1 + i\sin\arg z_1)\frac{1}{|z_2|}(\cos\arg z_2 - i\sin\arg z_2) = \frac{|z_1|}{|z_2|}[\cos\arg z_1\cos\arg z_2 +$$
$$+\sin\arg z_1\sin\arg z_2 + i(\cos\arg z_1\sin\arg z_2 - \cos\arg z_2\sin\arg z_1)] =$$
$$= \frac{|z_1|}{|z_2|}[\cos(\arg z_1 - \arg z_2) + i\sin(\arg z_1 - \arg z_2)].$$

Теорема доказана.

Следствие. $z^n = |z|^n(\cos n\arg z_1 + i\sin n\arg z_1)$ (формула Муавра).

Теорема 1.2 (о свойствах комплексно сопряженных). Отображение $z \to z^*$ (или $z \to \bar{z}$) удовлетворяет свойствам: а) $(z_1 \pm z_2)^* = z_1^* \pm z_2^*$; б) $(z^*)^* = z$;

в) $(z_1z_2)^* = z_1^* z_2^*$; г) $z + z^* = 2\operatorname{Re} z$; д) $z - z^* = 2i\operatorname{Im} z$; е) $\left(\dfrac{z_1}{z_2}\right)^* = \dfrac{z_1^*}{z_2^*}$; ж) $|z|^2 = z\bar{z}$ или $|z|^2 = zz^*$ — неотрицательное вещественное число.

Доказательство. Все свойства проверяются непосредственно. Действительно, если $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$, то комплексно сопряженное $z_1^* = x_1 - iy_1$, $z_2^* = x_2 - iy_2$. Поэтому

а) $(z_1 \pm z_2)^* = x_1 + x_2 \mp i(y_1 + y_2) = z_1^* \pm z_2^*$;

г) $z + z^* = x + iy + x - iy = 2x = 2\operatorname{Re} z$;

д) $z - z^* = x + iy - x + iy = 2iy = 2i\operatorname{Im} z$;

ж) $zz^* = (x+iy)(x-iy) = x^2 - (iy)^2 = x^2 + y^2 = |z|^2$.

Заметим, что геометрически отображение $z \to z^*$ сводится к отражению комплексной плоскости C относительно вещественной оси. Если комплексное число задано в показательной форме записи $z = |z| e^{i\arg z}$, то $z^* = |z| e^{-i\arg z}$, т.е. $|z| = |z^*|$, а аргумент меняет знак на противоположный. Следовательно, б) $(z^*)^* = z$, а в силу теоремы 1.1:

в) $(z_1z_2)^* = |z_1z_2|\, e^{-i(\arg(z_1+z_2))} = |z_1||z_2|\, e^{-i(\arg z_1 + \arg z_2)} = |z_1|\, e^{-i\arg z_1}\, |z_2|\, e^{-i\arg z_2} = z_1^* z_2^*$;

е) $\left(\dfrac{z_1}{z_2}\right)^* = \left|\dfrac{z_1}{z_2}\right| e^{-i\arg\frac{z_1}{z_2}} = \dfrac{|z_1|}{|z_2|} e^{-i(\arg z_1 - \arg z_2)} = \dfrac{|z_1|\, e^{-i\arg z_1}}{|z_2|\, e^{-i\arg z_2}} = \dfrac{z_1^*}{z_2^*}$.

Теорема доказана.

Замечание. В анализе путем разложения функции комплексной переменной в степенные ряды доказывается формула Эйлера $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Из определения модуля следует, что $|e^{i\varphi}| = \sqrt{\cos^2\varphi + \sin^2\varphi} = 1$ не зависимо от φ.

Функция $e^{i\varphi}$ обладает свойствами показательной функции, например,

$$e^{i\varphi_1} \cdot e^{i\varphi_2} = e^{i(\varphi_1+\varphi_2)}, \qquad \frac{e^{i\varphi_1}}{e^{i\varphi_2}} = e^{i(\varphi_1-\varphi_2)}, \qquad \left(e^{i\varphi}\right)^n = e^{in\varphi}.$$

Учитывая это, находим **формулу извлечения целого корня**:

$$\sqrt[n]{z} = \sqrt[n]{|z|}\, e^{i\frac{\arg z + 2\pi k}{n}} = \sqrt[n]{|z|}\left(\cos\frac{\arg z + 2\pi k}{n} + i\sin\frac{\arg z + 2\pi k}{n}\right). \tag{1.1}$$

Замечание. Корень n-й степени из z имеет n различных значений, которые получаются подстановкой $k = 0,1,\ldots,n-1$. Функция $\sqrt[n]{z}$ является многозначной.

Все n значений корня n-й степени из z расположены в вершинах правильного n-угольника, вписанного в окружность с центром в нуле и радиуса $\sqrt[n]{|z|}$.

Корень n-й степени из 1 называется **примитивным** (или первообразным), если он не является корнем из 1 никакой меньшей степени. Таковыми будут, например, $\varepsilon = \varepsilon_1 = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ и ε_{n-1}. В силу формулы Муавра любой другой корень ε_k является степенью примитивного $\varepsilon_k = \varepsilon_1^k$.

Пример. По формуле (1.1) найдем все корни 3-й степени из 1. Запишем в показательной форме $1 = 1e^{i0} = 1e^{i2\pi k}$. Следовательно, $\varepsilon_k = \cos\frac{2\pi k}{3} + i\sin\frac{2\pi k}{3}$; $\varepsilon_0 = \cos 0 + i\sin 0 = 1$; $\varepsilon_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$; $\varepsilon_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$, среди них примитивные — $\left\{-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$.

Замечание. Если G — мультипликативная группа, a — ее фиксированный элемент и любой элемент $g \in G$ записывается в виде $g = a^n$ для некоторого $n \in Z$, то говорят, что $G = \langle a \rangle$ — **циклическая группа** с образующим a. При этом $(a^{-1})^k = a^{-k}$. Аналогично циклическая группа определяется в аддитивном случае $\langle a \rangle = \{na : n \in Z\}$. Это не означает, что все элементы различны.

Из ассоциативности операции следует, что все циклические группы являются абелевыми группами.

Предложение 1.1 (о циклической группе корней n-й степени из 1). Корни n-й степени из 1 образуют циклическую группу, обозначаемую U_n.

Доказательство. Запишем в показательной форме $1 = 1e^{i0} = 1e^{i2\pi k}$. Рассмотрим множество всех корней n-й степени из 1. По формуле (1.1) $\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}$.

В силу формулы Муавра любой другой корень ε_k является степенью примитивного $\varepsilon_k = \varepsilon_1^k$. Поэтому $\varepsilon_k\varepsilon_m = \varepsilon_1^k\varepsilon_1^m = \varepsilon_1^{k+m}$ — корень n-й степени из 1, так как $(\varepsilon_1^{k+m})^n = (\varepsilon_1^n)^{k+m} = 1$. Следовательно, множество всех корней n-й степени из 1 замкнуто относительно умножения (группоид). Кроме того, операция умножения ассоциативна (полугруппа), 1 является единицей в группе (моноид), существуют обратные элементы, поскольку $\varepsilon_k\varepsilon_{n-k} = \varepsilon_1^k\varepsilon_1^{n-k} = \varepsilon_1^n = 1$.

Итак, множество всех корней n-й степени из 1 — циклическая группа с образующим ε_1.

Предложение доказано.

2 определение группы. Множество G с бинарной операцией называется **группой**, если

1) операция **ассоциативна**, т.е. $(ab)c = a(bc)$ для любых $a, b, c \in G$.

2) операция **гарантирует однозначные правые и левые частные,** т.е. для любых $a, b \in G$ существуют $x, y \in G$, называемые соответственно левым и правым обратным частным от деления b на a, что $ax = b$, $ya = b$.

Теорема 1.3 (об эквивалентности двух определений группы). Определения 1 и 2 группы эквивалентны.

Доказательство. Покажем как из предположений 2) и 3) определения 1 следует второе предположение определения 2.

Итак, операция гарантирует обратные элементы, т.е. для любого $a \in G$ существует $x \in G$, такой что $ax = xa = e$.

Отсюда для любых $a,b \in G$ имеем $axb = eb = b$ и $bxa = be = b$, т.е. существует левый и правый обратный частный от деления b на a.

Осталось показать, что из второго определения следует первое.

Итак, операция гарантирует однозначные правые и левые частные, т.е., в частности, для любого $a \in G$ существуют $e_a \in G$, называемый правым обратным частным от деления a на a, что $ae_a = a$. Пусть b произвольный элемент множества G. Тогда операция гарантирует существование элемента y такого, что $ya = b$. Имеем $b = ya = y(ae_a) = (ya)e_a = be_a$. Отсюда e_a — правый обратный для всех элементов G. Обозначим его $\widehat{e}$.

Аналогично можно показать существование единственного элемента e такого, что $ea = a$ для всех элементов G.

В действительности элементы e и $\widehat{e}$ совпадают: из равенства $e = e\widehat{e} = \widehat{e}$. Поэтому существует единственный элемент, называемый единицей, обозначаемый в дальнейшем e.

Операция гарантирует для любого $a \in G$ существование $x, y \in G$: $ax = e$, $ya = e$.

Имеем $yax = (ya)x = ex = x$ и $yax = y(ax) = ye = y$. Поэтому $x = y$, т.е. существует обратный элемент x: $ax = xa = e$.

Теорема доказана.

Определение порядка группы. Мощность $|G|$ группы G называется порядком группы. Если эта мощность конечна, то группа называется конечной.

Пример. Циклическая группа корней n-й степени из 1 имеет порядок n.

Задачи

1.1. Пусть Z – множество целых чисел; N – множество натуральных чисел; Q – множество рациональных чисел; C – множество комплексных чисел; R – множество вещественных чисел; R_+ – множество положительных вещественных чисел. Охарактеризовать каждое множество с точки зрения групп, полугрупп, группоидов относительно операций сложения и умножения.

Решение. Сразу заметим, что для всех вышеуказанных множеств операции сложения и умножения коммутативны и ассоциативны.

Множество Z замкнуто относительно операции сложения, так как сумма целых чисел — целое число. Для каждого целого числа обратным является то же самое число, взятое с противоположным знаком.

Нетрудно видеть, что Z – аддитивная циклическая группа $\langle 1 \rangle = \{n \cdot 1 : n \in Z\}$, т.е. 1 — образующий элемент. Относительно операции умножения Z — моноид, поскольку содержит 1 и множество замкнуто относительно ассоциативной операции умножения (произведение целых чисел — целое число), но не является группой (целые числа за исключением ± 1 не обратимы). По тем же соображениям, что и Z, множество натуральных чисел N является всего лишь моноидом относительно умножения. Относительно сложения N — полугруппа, а не моноид, поскольку 0 (единица для аддитивной операции) не принадлежит N.

Множество Q замкнуто относительно операций сложения (умножения), так как сумма (произведение) рациональных чисел — рациональное число и включает 0 (единица для аддитивной операции) и 1 (единица для мультипликативной операции). Для каждого рационального числа обратным по сложению является то же самое число, взятое с противоположным знаком, но не существует обратного элемента относительно умножения для 0. Поэтому Q — абелева аддитивная группа и всего лишь моноид относительно умножения.

По тем же соображениям, что и Q, C и R — абелевы аддитивные группы и всего лишь моноиды относительно умножения. Поскольку R_+ не содержит 0 — единственный не обратимый элемент относительно умножения, R_+ –абелева мультипликативная группа. R_+ замкнуто относительно операции сложения, но единицу (0) и обратные элементы (отрицательные вещественные числа) не включает. Поэтому R_+ — аддитивная полугруппа.

1.2. Охарактеризовать множество всех квадратных матриц фиксированной размерности $n \times n$ с элементами из Z, N, Q, C, R, R_+ с точки зрения групп, полугрупп, группоидов относительно операции сложения и умножения.

Решение. Все множества замкнуты относительно обеих операций, к тому же ассоциативных в силу определений сложения и умножения матриц. Все указанные множества не являются группами относительно умножения, поскольку, в частности, не гарантировано $\det A \neq 0$ для существования обратных элементов:

$$A^{-1} = \frac{1}{\det A}\begin{pmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{pmatrix}.$$

Относительно обеих операций множества являются полугруппами в случае N, R_+, но не моноидами, так как не включают единичный элемент (единичную матрицу и нулевую матрицу).

В случае Z, Q, C, R множества — моноиды относительно умножения, так как включают единичный элемент (единичную матрицу) и абелевы аддитивные группы, так как включают обратные элементы $-A$ и единичный элемент (нулевую матрицу).

1.3. Охарактеризовать множество всех невырожденных квадратных матриц фиксированной размерности $n \times n$ с элементами из Z, N, Q, C, R, R_+ с точки зрения групп, полугрупп, группоидов относительно операции сложения и умножения.

Решение. В отличие от предыдущей задачи все множества не замкнуты относительно сложения, поскольку сумма двух невырожденных матриц может иметь нулевой определитель. Поэтому относительно $+$ — даже не группоиды.

Все множества замкнуты относительно операции умножения: определитель произведения матриц равен произведению определителей.

Относительно умножения, в отличие от предыдущей задачи, в случае Q, C, R гарантировано существование обратных элементов A^{-1}, так как $\det A \neq 0$, в случаях Z, N, R_+ элементы обратной матрицы могут оказаться за пределами Z, N, R_+.

Поэтому относительно умножения в случае Q, C, R — группы, обозначаемые как $GL(n,Q)$, $GL(n,C)$, $GL(n,R)$, соответственно.

По-прежнему относительно умножения в случае Z — моноид, в случае N, R_+ — полугруппы.

1.4. Охарактеризовать множество всех квадратных матриц фиксированной размерности $n \times n$ с элементами из целых чисел Z с точки зрения групп, полугрупп, группоидов относительно операции **коммутирования** $A * B = AB - BA$.

Решение. Покажем, что операция $*$ не ассоциативна:

$(A * B) * \tilde{C} = (AB - BA) * \tilde{C} = AB\tilde{C} - BA\tilde{C} - (\tilde{C}AB - \tilde{C}BA) = AB\tilde{C} - BA\tilde{C} - \tilde{C}AB + \tilde{C}BA$;

$A * (B * \tilde{C}) = A * (B\tilde{C} - \tilde{C}B) = AB\tilde{C} - A\tilde{C}B - (B\tilde{C}A - \tilde{C}BA) = AB\tilde{C} - A\tilde{C}B - B\tilde{C}A + \tilde{C}BA$.

Так как в общем случае для матриц $B(A\tilde{C} - \tilde{C}A) \neq (A\tilde{C} - \tilde{C}A)B$ и $-BA\tilde{C} - \tilde{C}AB \neq -A\tilde{C}B - B\tilde{C}A$, то операция не ассоциативна и множество не является полугруппой. Однако данное множество является группоидом.

1.5. Множество всех линейных функций $x \to ax + b$, $a \neq 0$, относительно суперпозиции.

Решение. Суперпозиция $x \to ax + b$ и $x \to cx + d$: $x \to a(cx + d) + b = acx + ad + b$ — опять линейная функция. Поэтому множество линейных функций замкнуто относительно суперпозиции, т.е. группоид.

Роль единицы играет тождественное отображение $x \to x$. Следовательно, множество — моноид.

Докажем существование обратного элемента к произвольной функции $x \to ax + b$.

Из равенства $acx + ad + b = x$ следует $ac = 1$ и $ad + b = 0$. Отсюда, полагая $c = \dfrac{1}{a}$ и $d = -\dfrac{b}{a}$ (по предположению $a \neq 0$), находим обратный элемент: $x \to \dfrac{1}{a}x - \dfrac{b}{a}$.

Множество является группой.

1.6. Найти все а) корни 4-й, б) 6-й степени из 1; указать примитивные.

Решение. а) По формуле (1.1) найдем все корни 4-й степени из 1. Запишем в показательной форме $1 = 1e^{i0} = 1e^{i2\pi k}$. Следовательно, $\varepsilon_k = \cos\dfrac{2\pi k}{4} + i\sin\dfrac{2\pi k}{4}$;

$\varepsilon_0 = \cos 0 + i\sin 0 = 1$; $\varepsilon_1 = \cos\dfrac{2\pi}{4} + i\sin\dfrac{2\pi}{4} = 0 + i = i$; $\varepsilon_2 = \cos\dfrac{4\pi}{4} + i\sin\dfrac{4\pi}{4} = -1$,

$\varepsilon_3 = \cos\dfrac{6\pi}{4} + i\sin\dfrac{6\pi}{4} = -i$, в итоге: $\{\pm 1, \pm i\}$, среди них примитивные — $\{\pm i\}$;

б) По формуле (1.1) найдем все корни 6-й степени из 1. Запишем в показательной форме $1 = 1e^{i0} = 1e^{i2\pi k}$. Следовательно, $\varepsilon_k = \cos\frac{2\pi k}{6} + i\sin\frac{2\pi k}{6}$; $\varepsilon_0 = \cos 0 + i\sin 0 = 1$; $\varepsilon_1 = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6} = \frac{1+i\sqrt{3}}{2}$; $\varepsilon_2 = \cos\frac{4\pi}{6} + i\sin\frac{4\pi}{6} = \frac{-1+i\sqrt{3}}{2}$, $\varepsilon_3 = \cos\frac{6\pi}{6} + i\sin\frac{6\pi}{6} = -1$, $\varepsilon_4 = \cos\frac{8\pi}{6} + i\sin\frac{8\pi}{6} = \frac{-1-i\sqrt{3}}{2}$, $\varepsilon_5 = \cos\frac{10\pi}{6} + i\sin\frac{10\pi}{6} = \frac{1-i\sqrt{3}}{2}$ в итоге: $\left\{\pm 1, \pm\frac{1+i\sqrt{3}}{2}, \pm\frac{1-i\sqrt{3}}{2}\right\}$, среди них примитивные — $\left\{\frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\right\}$.

2. Подгруппа

Определение подгруппы. Подмножество H группы G называется подгруппой этой группы, если оно само является группой относительно операции, определенной в группе. Обозначение $H \le G$, если $H \ne G$, то $H < G$.

При проверке того, является ли подмножество H группы G подгруппой этой группы, достаточно проверить: 1) замкнуто ли H относительно операции, т.е. вместе с любыми двумя своими элементами $a, b \in H$ содержит и их произведение $ab \in H$; 2) содержит ли H вместе со всяким своим элементом и его обратный элемент, обозначаемый в дальнейшем как a^{-1}.

Действительно, из справедливости закона ассоциативности в группе G следует его справедливость для элементов из H, а принадлежность H единицы группы G вытекает из 2) и 1).

Говорят, что операция **индуцирована** в H соответствующей операцией из G.

Подгруппы, отличные от единичной и всей группы, называются **собственными** или **истинными.**

Пример. $Z < Q < R < C$ для аддитивных групп и $Q \setminus \{0\} < R_+ < C \setminus \{0\}$ для мультипликативных групп ($Z \setminus \{0\}$ не является группой по умножению).

Предложение 2.1 (критерий подгруппы). Пусть H подмножество группы G. Пусть $HH = \{h_1 h_2 : \forall h_1 \in H, \forall h_2 \in H\}$, $H^{-1} = \{h^{-1} : h \in H\}$. Тогда $H \le G \Leftrightarrow HH \subseteq H, H^{-1} \subseteq H$.

Доказательство. Достаточность. Пусть $H \le G$. В этом случае H является группой относительно индуцированной операции. Поэтому H замкнуто относительно операции, т.е. $HH = \{h_1 h_2 : \forall h_1 \in H, \forall h_2 \in H\} \subseteq H$; H содержит вместе со всяким своим элементом и его обратный элемент, т.е. $H^{-1} = \{h^{-1} : h \in H\} \subseteq H$.

Достаточность доказана.

Необходимость. Предположим, что $HH \subseteq H, H^{-1} \subseteq H$. Тогда из $HH \subseteq H$ следует, что H — группоид. Индуцированная операция ассоциативна. Поэтому H — полугруппа. Из включения $H^{-1} \subseteq H$ следует, что в H существует единичный элемент и H содержит вместе со всяким своим элементом и его обратный элемент, т.е. H — группа, вложенная в G, и, следовательно, $H \le G$.

Предложение доказано.

Предложение 2.2 (о пересечении подгрупп). Пересечение любого набора подгрупп является подгруппой.

Доказательство. Если в пересечении $A \cap B$ подгрупп A и B группы G содержатся элементы x и y, то они лежат в подгруппе A, а поэтому A принадлежат и произведение xy, и обратный элемент x^{-1}. По тем же соображениям элементы xy и x^{-1} принадлежат и подгруппе B, а потому они входят и в $A \cap B$.

Полученный результат справедлив, как легко видеть, не только для двух подгрупп, но и для любого числа подгрупп, конечного или бесконечного.

Предложение доказано.

Предложение 2.3 (об объединении подгрупп). Объединение двух подгрупп является подгруппой тогда и только тогда, когда одна из подгрупп содержится в другой.

Доказательство. Требуется доказать, что $(A \cup B) \le G \Leftrightarrow A \le B \vee B \le A$.

Необходимость. Итак, пусть $(A \cup B) \le G$. Пусть $a \in A, b \in B$ произвольно выбраны. По определению подгруппы $ab \in A \cup B$. По определению объединения $ab \in A$ или $ab \in B$. Пусть $ab \in A \Rightarrow \exists a_1 \in A : ab = a_1$. Отсюда по определению подгруппы $b \in A$. В силу произвольности выбора $b \in B$ получаем $B \le A$. Аналогично можно показать: $ab \in B \Rightarrow A \le B$.

Достаточность. Если $A \le B \Rightarrow B \cup A = B$, $B \le A \Rightarrow B \cup A = A$, то $(A \cup B) \le G$.

Предложение доказано.

Предложение 2.4 (о подгруппе из объединения подгрупп). Если подгруппа H содержится в объединении подгрупп A и B, то либо $H \le A$, либо $H \le B$.

Доказательство. Требуется доказать, что если $H \subseteq (A \cup B)$, $H \le G$, $A \le G$, $B \le G$, G — группа, то либо $H \le A$, либо $H \le B$.

Очевидно $H = (A \cap H) \cup (B \cap H)$. В силу предложения 2.2 $(A \cap H) \le G$ и $(B \cap H) \le G$. Так как $H = (A \cap H) \cup (B \cap H)$ группа, то в силу предложения 2.3 либо $(A \cap H) \le (B \cap H)$, либо $(B \cap H) \le (A \cap H)$. В первом случае — $H \le B$, а во втором — $H \le A$.

Предложение доказано.

Интересным примером подгрупп служат так называемые **циклические** подгруппы.

Напомним, что, если n — любое натуральное число, то произведение n элементов, равных элементу a, называется n-й степенью элемента a и обозначается через a^n. **Отрицательные степени** элемента a можно определить или как элементы группы G, обратные положительным степеням этого элемента, или как произведения нескольких множителей, равных a^{-1}. В действительности эти определения совпадают,

$$(a^n)^{-1} = (a^{-1})^n, \; n > 0. \tag{2.1}$$

Заметим, что если операция в группе G **называется** сложением, то вместо степеней элемента a следует говорить о **кратных** этого элемента и записывать их через na.

Подгруппа $\langle a \rangle$, состоящая из всех степеней a, называется циклической подгруппой группы G, порожденной элементом a. Это всегда коммутативная подгруппа, даже если сама группа G и не коммутативна.

Определение порядка элемента. Если все степени элемента a являются различными, то a называется элементом бесконечного порядка.

Если это не так, и n — наименьшая положительная степень элемента a, равная единице, то a называется элементом конечного порядка n.

Пример. Определим порядок элемента $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$ в группе $GL(2,C)$, где $GL(2,C)$ — группа всех невырожденных квадратных матриц размерности 2×2 с элементами из C. Для этого нам необходимо найти наименьшую положительную степень n, такую что $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Заметим, что

$$i^n = \begin{cases} 1, & n = 4k, \\ i, & n = 4k+1, \\ -1, & n = 4k+2, \\ -i, & n = 4k+3; \end{cases}, \quad k = 0,1,2,\dots .$$

Вычисляем $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} = i\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Отсюда $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}^k = i^{2\mathrm{m}}\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}$, если $k = 2m+1$ и $\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}^k = i^{\mathrm{m}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, если $k = 2m$. Так как только четвертая степень i равна 1, то порядок равен 8.

Предложение 2.5 (о порядке произведения элементов). Для любых элементов a, b группы G элементы ab и ba имеют одинаковый порядок.

Доказательство. Пусть n порядок ab. Пусть m порядок ba. По определению

$$e = (ab)^n = a\underbrace{bab\ldots aba}_{n-1}b = a(ba)^{n-1}b .$$

Отсюда $(ba)^{n-1} = a^{-1}b^{-1}$. Следовательно, $(ba)^n = a^{-1}b^{-1}(ba) = e$. Тогда $m \le n$. По аналогии можно показать, что $(ab)^m = e$. Поэтому $n \le m$.

Предложение доказано.

Теорема 2.1 (о строении циклической группы конечного порядка). Пусть $G = \langle a \rangle$ — циклическая группа порядка n. Тогда n — порядок a; все элементы представимы в виде a^l ($l = 0,1,\dots,n-1$); порядок каждого элемента является делителем n; всякая подгруппа циклической группы сама циклическая.

Доказательство. По предположению $G = \{g_1, g_2, \dots, g_n\}$ и все элементы степени a. Сначала заметим, что n — порядок a. Действительно, пусть это не так и

$a^m = e$, где $0 < m < n$. Тогда $|G| \le m < n$, поскольку для произвольного числа $k = mr + l$, $0 \le l < m$, $a^k = \underbrace{a...aa}_{mr}\underbrace{a...aa}_{l} = e(a)^l = a^l$ и число различных элементов в G не превышает m. Мы также показали, что все элементы представимы в виде a^l ($l = 0,1,...,n-1$).

Рассмотрим произвольный элемент g из группы. Пусть s — порядок g, но s не является делителем n. Следовательно, $n = su + r$, где u, r — целые числа, причем $0 < r < s$. Тогда $e = g^n = g^{su+r} = g^{su}g^r = eg^r = g^r$. Полученное противоречие с определением порядка элемента доказывает, что порядок произвольного элемента является делителем n.

Пусть $H < G$. Можно считать, что подгруппа H отлична от единичной подгруппы, так как иначе доказывать было нечего. Предположим, что a^k есть наименьшая положительная степень элемента a, содержащаяся в H. Допустим, что в H содержится также элемент a^m, $m \ne 0$, причем m не делится на k. Тогда, если d, $d > 0$, есть наибольший общий делитель чисел k и m, то существуют такие целые числа u и v, что $ku + mv = d$, а потому в подгруппе H содержится элемент $(a^k)^u \cdot (a^m)^v = a^d$, но так как при наших предположениях $d < k$, то мы приходим в противоречие с выбором элемента a^k. Этим доказано, что $H = \langle a^k \rangle$.

Теорема доказана.

Замечание. Рассуждая так же как в последней части доказательства теоремы, можно показать, что всякая подгруппа произвольной циклической группы (не только конечной) сама циклическая.

Задачи

2.1. Найти порядок элементов в группе $GL(n,C)$ а) $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$; б) $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

Решение. Вычисляем: а) $\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Следовательно, порядок равен 2.

б) $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}^3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Следовательно, порядок равен 3.

2.2. Найти порядок элементов в мультипликативной группе $C \setminus \{0\}$:

а) $\frac{-\sqrt{3}}{2} + \frac{1}{2}i$; б) $\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$; в) $\frac{6}{5} + \frac{8}{5}i$.

Решение. а) Число $z = \frac{-\sqrt{3}}{2} + \frac{1}{2}i$ запишем в показательной форме записи:

$|z| = \sqrt{\left(\frac{-\sqrt{3}}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \sqrt{\frac{3}{4} + \frac{1}{4}} = 1$, $\arg z = \pi - arctg\frac{1}{\sqrt{3}} = \pi - \frac{\pi}{6} = \frac{5}{6}\pi$, $z = e^{i\frac{5\pi}{6}}$.

Следовательно, $z^k = e^{i\frac{5\pi k}{6}}$. Находим $k = 12$ как наименьшее положительное целое число $k = \frac{12m}{5}$ для некоторого $m \in Z$, при котором $z^{12} = e^{i10\pi} = 1$. Поэтому порядок равен 12.

б) Число $z = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i$ запишем в показательной форме записи:

$$|z| = \sqrt{\left(\frac{1}{\sqrt{2}}\right)^2 + \left(-\frac{1}{\sqrt{2}}\right)^2} = \sqrt{\frac{1}{2} + \frac{1}{2}} = 1,\ \arg z = -arctg1 = -\frac{\pi}{4},\ z = e^{-i\frac{\pi}{4}}.$$

Следовательно, $z^k = e^{i\frac{\pi k}{4}}$ и при $k = 8$ имеем $z^8 = e^{i2\pi} = 1$. Поэтому порядок равен 8.

в) Для числа $z = \frac{6}{5} + \frac{8}{5}i$ достаточно вычислить модуль:

$$|z| = \sqrt{\left(\frac{6}{5}\right)^2 + \left(\frac{8}{5}\right)^2} = \sqrt{\frac{36}{25} + \frac{64}{25}} = 2.$$

Следовательно, по теореме 1.1 о свойствах модуля $|z^k| = 2^k \to \infty$ при $k \to \infty$. Поэтому порядок равен ∞ (элемент бесконечного порядка).

2.3. Пусть $P = C \vee R \vee Q$. Пусть $UT(n,P)$ — множество всех матриц с нулевым углом под главной диагональю и с единицами по диагонали и элементами из P:

$$A = \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & 1 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Доказать, что $UT(n,P) < GL(n,P)$ (унитреугольная подгруппа).

Решение. $UT(n,P)$ состоит из матриц с определителем равным 1 и, следовательно, невырожденных. Поэтому осталось проверить, что $UT(n,P)$ — группа. Действительно, $UT(n,P)$ замкнуто относительно умножения; $UT(n,P)$ содержит вместе со всяким своим элементом и его обратный элемент.

2.4. Пусть $P = C \vee R \vee Q$. Пусть $O(n,P)$ — множество всех ортогональных матриц $\{A : AA' = E\}$ (штрих означает транспонирование, а E — единичную матрицу). Привести пример матрицы из $O(2,C)$, у которой хотя бы один элемент имеет ненулевую мнимую часть. Доказать, что $O(n,P) < GL(n,P)$ (ортогональная подгруппа).

Решение. В качестве примера матрицы из $O(2,C)$ рассмотрим матрицу

$$A = \begin{pmatrix} i & \sqrt{2} \\ \sqrt{2} & -i \end{pmatrix} \Rightarrow A' = \begin{pmatrix} i & \sqrt{2} \\ \sqrt{2} & -i \end{pmatrix} \Rightarrow AA' = \begin{pmatrix} i & \sqrt{2} \\ \sqrt{2} & -i \end{pmatrix}^2 = \begin{pmatrix} -1+2 & i\sqrt{2} - i\sqrt{2} \\ i\sqrt{2} - i\sqrt{2} & 2-1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Докажем, что $O(n,P) < GL(n,P)$. Из определения ортогональной матрицы следует существование обратной матрицы (обратного элемента) и, в частности, не вырожденность.

В силу свойств операции транспонирования матрицы $(A')' = A$; $(AB)' = B'A'$. Поэтому $O(n,P)$ содержит вместе с матрицей и обратный к ней элемент, т.е. $(O(n,P))^{-1} \subseteq O(n,P)$ и, кроме того, $O(n,P)O(n,P) \subseteq O(n,P)$, так как

$$A \in O(n,P), B \in O(n,P) \Rightarrow AB(AB)' = ABB'A' = E \Rightarrow AB \in O(n,P),$$

что в силу предложения 2.1 завершает доказательство того, что $O(n,P) < GL(n,P)$.

2.5. Пусть $U(n)$ — множество всех матриц $\{A : A\bar{A}' = E\}$ (штрих по-прежнему означает транспонирование, черта означает взятие комплексно-сопряженного элемента к каждому элементу a_{ij} матрицы). Привести пример матрицы из $U(2)$. Доказать, что $U(n) < GL(n,C)$ (унитарная подгруппа).

Решение. Приведем пример унитарной матрицы:

$$A = \begin{pmatrix} \frac{i}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{pmatrix} \Rightarrow \bar{A}' = \begin{pmatrix} -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix} \Rightarrow A\bar{A}' = \begin{pmatrix} \frac{i}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Докажем, что $U(n) < GL(n,C)$. Из определения унитарной матрицы следует существование обратной матрицы (обратного элемента) и, в частности, не вырожденность.

В силу свойств операции транспонирования матрицы и операции перехода к комплексно сопряженной матрице $\overline{(\bar{A}')}' = A$, $\overline{(AB)}' = \bar{B}'\bar{A}'$. Поэтому $U(n)$ содержит вместе с матрицей и обратный к ней элемент, т.е. $(U(n))^{-1} \subseteq U(n)$ и, кроме того, $U(n)U(n) \subseteq U(n)$, так как

$$A \in U(n), B \in U(n) \Rightarrow AB\overline{(AB)}' = AB\bar{B}'\bar{A}' = E \Rightarrow AB \in U(n),$$

что в силу предложения 2.1 завершает доказательство того, что $U(n) < GL(n,C)$.

3. Изоморфизм. Перестановки

Определение сюръекции. Отображение $f : M \to L$ называется сюръекцией или отображением “на”, если $f(M) = L$.

Пример. Отображение $z \to |z|$, ставящее модуль в соответствие произвольному комплексному числу $z \in C$, является сюръекцией $f : C \to R_+ \cup \{0\}$.

Определение инъекции. Если для любых двух различных элементов x_1 и x_2 из M их образы $y_1 = f(x_1)$ и $y_2 = f(x_2)$ также различны, то f называется инъекцией.

Пример. Отображение $z \to |z|$, ставящее модуль в соответствие произвольному комплексному числу $z \in C$, не является инъекцией $f : C \to R_+ \cup \{0\}$, в частности, потому, что $|e^{i\varphi}| = \sqrt{\cos^2\varphi + \sin^2\varphi} = 1$ для всех $\varphi \in R$.

Определение биекции. Отображение $f: M \to L$, которое одновременно является сюръекцией и инъекцией**,** называется биекцией или взаимно однозначным соответствием между M и L.

Пример. Отображение $z \to z^*$ (или $z \to \bar{z}$) является биекцией $f: C \to C$. Действительно, два комплексных числа $z_1 = x_1 + iy_1$ и $z_2 = x_2 + iy_2$ считаются равными тогда и только тогда, когда $x_1 = x_2$ и $y_1 = y_2$. Отсюда соответствие $x + iy \to x - iy$ однозначное, а в силу равенства $(z^*)^* = z$ (теорема 1.2) и взаимно однозначное.

Определение изоморфизма. Взаимно однозначное отображение группы G в группу G_1, $f: G \to G_1$, называется изоморфизмом, если оно сохраняет операцию, т.е. $f(x_1 \circ x_2) = f(x_1) \circ f(x_2)$, где $y_1 = f(x_1)$, $y_2 = f(x_2)$ и $\circ$ — произвольная операция.

Определение автоморфизма. Изоморфное отображение группы G в себя называется автоморфизмом.

Пример. Отображение $z \to z^*$ (или $z \to \bar{z}$) в силу теоремы 1.2 удовлетворяет свойствам: $(z_1 \pm z_2)^* = z_1^* \pm z_2^*$; $(z_1 z_2)^* = z_1^* z_2^*$; $\left(\dfrac{z_1}{z_2}\right)^* = \dfrac{z_1^*}{z_2^*}$. Поэтому отображение $z \to z^*$ является автоморфизмом как для аддитивной группы комплексных чисел C, так и для мультипликативной группы $C \setminus \{0\}$.

Определение перестановки (подстановки). Пусть Ω — конечное множество из n элементов, обозначаемое как $\{1,2,...,n\}$. Элементы множества $S_n = S(\Omega)$ всех взаимно однозначных преобразований $\Omega \to \Omega$ называются перестановками.

Обозначаются перестановки греческими буквами. Например, $\pi = \begin{pmatrix} 12...n \\ i_1 i_2 ... i_n \end{pmatrix}$.

Единичное преобразование обозначается как $e = e_\Omega$.

Перестановки перемножаются в соответствии с общим правилом композиции отображений и образуют группу, называемую симметрической группой перестановок степени n и обозначаемую S_n.

Предложение 3.1 (о порядке симметрической группы перестановок). $|S_n| = n!$.

Доказательство. Символ 1 можно подходящей перестановкой σ перевести в любой другой символ $\sigma(1)$, для чего существует в точности n возможностей. Но, зафиксировав $\sigma(1)$, мы имеем право брать в качестве $\sigma(2)$ лишь один из оставшихся $n-1$ символов (всего различных пар $\sigma(1), \sigma(2)$ имеется $(n-1)+(n-1)+...+(n-1) = n(n-1)$, в качестве $\sigma(3)$ — соответственно $n-2$ символов и т.д. Всего возможностей выбора $\sigma(1), \sigma(2), \ldots, \sigma(n)$, а стало быть, и всех различных перестановок будет $n(n-1)...2 \cdot 1 = n!$.

Предложение доказано.

Теорема 3.1 (Кэли). Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы $S_n = S(\Omega)$.

Доказательство. Пусть G — группа, $n = |G|$. Для любого элемента $a \in G$ рассмотрим отображение $L_a : G \to G$, определенное формулой $L_a(g) = ag$. Если $e = g_1, g_2, ..., g_n$ — все элементы группы G, то $a, ag_2, ..., ag_n$ будут теми же элементами, но расположенными в каком-то другом порядке. Это будет биективное отображение, поскольку

$$ag_i = ag_j \Rightarrow a^{-1}(ag_i) = a^{-1}(ag_j) \Rightarrow (a^{-1}a)g_i = (a^{-1}a)g_j \Rightarrow g_i = g_j.$$

Кроме того, $L_a^{-1} = L_{a^{-1}}$. Единичным отображением является, естественно, L_e.

Используя ассоциативность умножения в G, получаем

$L_{ab}(g) = (ab)g = a(bg) = L_a(L_b g)$, т.е. $L_{ab} = L_a L_b$.

Итак, множество $L_e, L_{g_2}, ..., L_{g_n}$ образует подгруппу в группе всех биективных отображений множества G на себя, т.е. в S_n.

Теорема доказана.

Теорема 3.2 (изоморфизм циклических групп). Все циклические группы одного и того же порядка (в том числе и бесконечного) изоморфны.

Доказательство. Если $\langle g \rangle$ — бесконечная циклическая группа, то все степени g^n образующего g различны, и мы получаем изоморфизм $\langle g \rangle$ в аддитивную группу целых чисел, полагая $f(g^n) = n$.

Пусть $G = \{e, g, ..., g^{n-1}\}$ и $\tilde{G} = \{\tilde{e}, \tilde{g}, ..., \tilde{g}^{n-1}\}$ — две циклические группы порядка n (см. теорему 2.1).

Отображение $f(g^k) = \tilde{g}^k$ является биекцией.

Теорема доказана.

Задачи

3.1. Пусть G — множество пар элементов (a,b), $a \neq 0$, из $P = C \vee R \vee Q$ относительно операции $(a,b) \circ (c,d) = (ac, ad + b)$. Доказать, что G является группой, изоморфной группе всех линейных функций $x \to ax + b$ относительно суперпозиции.

Решение. Докажем, что G является группой.

Ассоциативность имеет место, так как

$$\big((a,b) \circ (c,d)\big) \circ (p,q) = (ac, ad + b) \circ (p,q) = (acp, acq + ad + b),$$

$$(a,b) \circ \big((c,d) \circ (p,q)\big) = (a,b) \circ (cp, cq + d) = (acp, acq + ad + b).$$

Существует единичный элемент $(1,0)$, так как

$(1,0) \circ (c,d) = (c,d)$ $(a,b) \circ (1,0) = (a,b)$.

Для каждой пары (a,b), $a \neq 0$ существует обратный элемент, который находится из равенства $(a,b) \circ (c,d) = (1,0)$. Следовательно, $ac = 1 \Rightarrow c = 1/a$, $ad + b = 0 \Rightarrow d = -b/a$. Отсюда $(a,b)^{-1} = (1/a, -b/a)$.

G является группой.

Поставим в соответствие паре элементов (a,b), $a \neq 0$, линейную функцию $x \to ax+b$. Нетрудно видеть, что это будет взаимно однозначное отображение. Покажем, что операция сохраняется. Действительно, пусть $x \to cx+d$. Для нахождения суперпозиции введем обозначение $\tilde{x} = cx+d$. Тогда $\tilde{x} \to a\tilde{x}+b$ и $x \to a(cx+d)+b = acx+ad+b$, т.е. суперпозиции двух линейных функций $x \to cx+d$ и $x \to ax+b$ соответствует пара $(a,b)\circ(c,d) = (ac, ad+b)$. Изоморфизм доказан.

3.2. Является ли отображение $\frac{1}{|z|}$ мультипликативной группы $C \setminus \{0\}$ в мультипликативную группу вещественных чисел R_+ изоморфизмом?

Решение. Данное отображение не является изоморфизмом, так как оно не является биекцией.

Действительно, i и 1 имеют один и тот же образ.

3.3. Найти порядок группы S_3.

Решение. В силу предложения 3.1 $|S_3| = 3!$.

3.4. Найти произведение $\sigma\tau$ элементов из S_4, где $\sigma = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}$, $\tau = \begin{pmatrix} 1234 \\ 4321 \end{pmatrix}$.

Решение. $\sigma\tau = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}\begin{pmatrix} 1234 \\ 4321 \end{pmatrix} = \begin{pmatrix} 1234 \\ 3214 \end{pmatrix}$.

3.5. Найти обратный элемент к элементу $\sigma = \begin{pmatrix} 1234 \\ 2341 \end{pmatrix}$ из S_4.

Решение. $\sigma^{-1} = \begin{pmatrix} 2341 \\ 1234 \end{pmatrix}$ или $\sigma^{-1} = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix}$.

3.6. Какие из указанных ниже совокупностей отображений множества $M = \{1,2,...,n\}$ в себя образуют группу относительно суперпозиции:

а) множество всех отображений;

б) множество всех инъективных отображений;

в) множество всех сюръективных отображений.

Решение. В случае а) ответ отрицательный, поскольку нетрудно построить необратимое отображение.

В силу определений инъекции и сюръекции множество всех инъективных отображений $M = \{1,2,...,n\}$ в себя совпадает с множеством всех сюръективных отображений и, более того, изоморфно S_n. Поэтому в случае б) и в) ответ положительный.

4. Теорема Лагранжа. Нормальная подгруппа

Определение смежных классов группы по подгруппе. Пусть G группа и $H \leq G$. Для произвольного элемента $g \in G$ множество $gH = \{gh : h \in H\}$ называется левым смежным классом группы G по подгруппе H с представителем g,

$G=\bigcup_{g\in G} gH$ называется левосторонним разложением группы G по подгруппе H. Аналогично определяются правые смежные классы Hg.

Предложение 4.1 (критерий принадлежности одному смежному классу). Пусть $H\le G$. Два элемента g, g_1 группы принадлежат одному смежному классу группы G по подгруппе H тогда и только тогда, когда $g_1^{-1}g\in H$ (левая смежность) и $gg_1^{-1}\in H$ (правая смежность) для мультипликативной операции и, соответственно, $(-g_1+g)\in H$, $(g-g_1)\in H$ для аддитивной операции.

Доказательство. Так как подгруппа H включает единицу, то $gH=g_1H\Rightarrow g_1e=g_1\in gH$. Поэтому изучим условия совпадения $gH=g_1H$.

$$gH=g_1H\Rightarrow \exists h\in H: ge=g_1h\Rightarrow g=g_1h\Rightarrow g_1^{-1}g=h\Rightarrow g_1^{-1}g\in H;$$
$$g_1^{-1}g\in H\Rightarrow \exists h\in H: g_1^{-1}g=h\Rightarrow g=g_1h\Rightarrow gH=g_1H;$$
$$gH=g_1H\Leftrightarrow g_1^{-1}g\in H.$$
$$Hg=Hg_1\Rightarrow \exists h\in H: eg=hg_1\Rightarrow g=hg_1\Rightarrow gg_1^{-1}=h\Rightarrow gg_1^{-1}\in H;$$
$$gg_1^{-1}\in H\Rightarrow \exists h\in H: gg_1^{-1}=h\Rightarrow g=hg_1\Rightarrow Hg=Hg_1;$$
$$Hg=Hg_1\Leftrightarrow gg_1^{-1}\in H.$$
$$g+H=g_1+H\Rightarrow \exists h\in H: g+e=g_1+h\Rightarrow -g_1+g\in H;$$
$$-g_1+g\in H\Rightarrow \exists h\in H: -g_1+g=h\Rightarrow g=g_1+h\Rightarrow g+H=g_1+H;$$
$$g+H=g_1+H\Leftrightarrow -g_1+g\in H.$$
$$H+g=H+g_1\Rightarrow \exists h\in H: e+g=h+g_1\Rightarrow g-g_1\in H;$$
$$g-g_1\in H\Rightarrow \exists h\in H: g-g_1=h\to g=h+g_1\Rightarrow H+g=H+g_1;$$
$$H+g=H+g_1\Leftrightarrow g-g_1\in H.$$

Предложение доказано.

Следствие. Произвольный элемент смежного класса является представителем смежного класса.

Пример. Найдем смежные классы мультипликативной группы $C\setminus\{0\}$ по подгруппе $R\setminus\{0\}$. Заметим, что операция умножения коммутативная. Поэтому левые и правые смежные классы совпадают. В силу критерия 4.1 два комплексных числа $z=a+ib$ и $z_1=a_1+ib_1$ принадлежат одному смежному классу группы $C\setminus\{0\}$ по подгруппе $R\setminus\{0\}$, если

$$\frac{z}{z_1}=\frac{a+ib}{a_1+ib_1}=\frac{(a+ib)(a_1-ib_1)}{a_1^2+b_1^2}=\frac{aa_1+bb_1+i(ba_1-ab_1)}{a_1^2+b_1^2}\in R\to ba_1-ab_1=0\to\frac{b}{b_1}=\frac{a}{a_1}=\lambda\in R.$$

В итоге смежный класс имеет вид $\{\lambda z:\forall\lambda\in R\setminus\{0\}\}$ с представителем $z\in C\setminus\{0\}$.

Пример. Найдем смежные классы аддитивной группы C по подгруппе R. Операция сложения также коммутативная. Поэтому левые и правые смежные классы совпадают. В силу критерия 4.1 два комплексных числа $z=a+ib$ и $z_1=a_1+ib_1$ принадлежат одному смежному классу аддитивной группы C по подгруппе R, если $z_1-z=a_1+ib_1-(a+ib)=a_1-a+i(b_1-b)\in R\to b_1-b=0\to b_1=b$.

Смежный класс имеет вид $\{x+ib:\forall x\in R\}$ с представителем ib.

Замечание. Так как соответствие $gH \Leftrightarrow Hg^{-1}$ взаимно однозначно, то мощность множества смежных классов не зависит от того, левые или правые смежные классы рассматриваются.

Определение индекса подгруппы H в группе G. Мощность множества смежных классов группы G по подгруппе H называется индексом подгруппы H в группе G. Обозначение $|G:H|$.

С подгруппой H свяжем отношение эквивалентности $g \sim g_1 \Leftrightarrow g^{-1}g_1 \in H$ (левая смежность), $g \sim g_1 \Leftrightarrow gg_1^{-1} \in H$ (правая смежность).

Напомним, что бинарное отношение R называется эквивалентностью, если оно удовлетворяет условиям:

а) рефлексивности, т.е. aRa;

б) симметричности, т.е. из aRb следует bRa;

с) транзитивности, т.е. из aRb, bRc следует aRc.

Отношение эквивалентности разбивает множество на непересекающиеся классы (классы эквивалентности).

Теорема 4.1 (Лагранжа). Во всякой конечной группе порядок любой подгруппы является делителем порядка самой группы.

Доказательство. Пусть в конечной группе G порядка n дана подгруппа $H \le G$ порядка k. Пусть j — индекс подгруппы H в группе G. Рассмотрим левостороннее разложение группы G по подгруппе H. Каждый левый класс gH состоит ровно из k элементов, так как если $gh = gh_1$ для некоторых $h \in H$, $h_1 \in H$, то $h = h_1$. Таким образом $n = kj$, что и требовалось доказать.

Теорема доказана.

Следствие. Так как порядок элемента совпадает с порядком его циклической подгруппы, то из теоремы Лагранжа мы получаем другое доказательство того, что порядок всякого элемента конечной группы является делителем порядка группы.

Предложение 4.2 (о группе, порядок которой — простое число). Всякая конечная группа, порядок которой есть простое число, будет циклической.

Доказательство. Пусть - G группа, порядок которой простое число. Тогда в силу следствия к теореме Лагранжа она совпадает с циклической подгруппой, порожденной любым ее элементом, отличным от единицы.

Предложение доказано.

Следствие. Для всякого простого числа p существует единственная, с точностью до изоморфизма, конечная группа порядка p.

Предложение 4.3 (об индексе пересечения подгрупп). Пусть A, B- подгруппы группы G. Тогда $|A : A \cap B| \le |G : B|$.

Доказательство. Заметим, что в силу предложения 2.2 $A \cap B$ является подгруппой A. Если $g \sim_1 g_1 \Leftrightarrow g^{-1}g_1 \in B$ и $h \sim_2 h_1 \Leftrightarrow h^{-1}h_1 \in A \cap B$ отношения левой смежности, соответственно, в G по B и в A по $A \cap B$, то второе является сужением на A первого отношения.

Предложение доказано.

Предложение 4.4 (о произведении индексов). Пусть A, B — подгруппы группы G, причем $A \leq B$. Индексы $|G:B|$, $|B:A|$ оба конечны тогда и только тогда, когда конечен индекс $|G:A|$. Если индекс $|G:A|$ конечен, то $|G:A|=|G:B||B:A|$.

Доказательство. Пусть $|G:A|<\infty$. Из предложения 4.4 следует, что $|B:B\cap A|=|B:A|\leq|G:A|<\infty$. Отсюда $|B:A|<\infty$.

Докажем, что $|G:A|=|G:B||B:A|$. Имеем $B=\bigcup\limits_{b\in B} Ab$ и $G=\bigcup\limits_{g\in G} Bg$. Пусть $g_1.g_2,...$ — представители различных классов смежности G по B. Пусть $|B:A|=k<\infty$ и $b_1.b_2,...b_k$ — представители различных классов смежности B по A. Тогда представителями различных классов смежности G по A будут элементы, получаемые путем умножения $b_j g_i$. Равенство $b_j g_i = b_k g_l$ влечет совпадение классов смежности Bg_i и Bg_l, а это невозможно по предположению. Так как $|G:A|<\infty$, то число различных произведений $b_j g_i$ конечно. Отсюда $|G:B|<\infty$ и $|G:A|=|G:B||B:A|$.

Рассуждая по аналогии в случае, если индексы $|G:B|$, $|B:A|$ конечны, получим, что $|G:A|=s<\infty$.

Предложение доказано.

Определение нормальной подгруппы. Подгруппа H называется нормальной (нормальным делителем или инвариантной подгруппой), если левые и правые классы смежности совпадают, т.е. $gH=Hg$ для любого $g\in G$.

Обозначение: $H \trianglelefteq G$.

Определение сопряженных элементов. Элементы a и b группы G называются сопряженными, если в G существует хотя бы один такой элемент g, что $b=g^{-1}ag$, т.е. b получается из a трансформированием элементом g или элемент a сопряжен с элементом b посредством элемента g. Используются также степенные обозначения: $b=g^{-1}ag=a^g$. Так как по определению группы вместе с любым элементом g она содержит и обратный элемент g^{-1}, то элементы a и b группы G будут сопряженными, если $b=gag^{-1}$.

Предложение 4.5 (критерий нормальной подгруппы). Подгруппа H группы G будет нормальной тогда и только тогда, если вместе со всяким своим элементом a она содержит и все элементы, сопряженные с ним в G или $H \trianglelefteq G \Leftrightarrow H^G \subseteq H$, где $H^G=\{h^g : h\in H, g\in G\}$.

Доказательство. Если H - нормальная подгруппа, то для любого элемента $g\in G$ имеет место $gH=Hg$. Отсюда для элемента $a\in H$ найдется такой элемент $b\in H$, что $ga=bg$ или $a=g^{-1}bg$. Отсюда H вместе со всяким своим элементом a содержит и все элементы, сопряженные с ним в G.

Пусть подгруппа H вместе со всяким своим элементом a содержит и все элементы, сопряженные с ним в G. Тогда для любого $g\in G$ имеем $b=g^{-1}ag\in H$.

Отсюда $g^{-1}Hg \subseteq H \Rightarrow Hg \subseteq gH$ и наоборот $gHg^{-1} \subseteq H \Rightarrow gH \subseteq Hg$. Поэтому для любого элемента $g \in G$ имеет место $gH = Hg$, т.е. H - нормальная подгруппа группы G.

Предложение доказано.

Задачи

4.1. Пусть H — подгруппа в конечной группе G. Пусть индекс $|G:H| = m$, $|H| = k$. Найти $|G|$.

Решение. По теореме Лагранжа $|G| = |H||G:H| = km$.

4.2. Найти смежные классы аддитивной группы вещественных (3×2)-матриц по подгруппе всех (3×2)-матриц (a_{ij}) с условием $a_{31} = a_{32} = a_{22} = 0$.

Решение. Так как аддитивная группа вещественных (3×2)-матриц абелева, то левые и правые смежные классы совпадают. По условию H — это множество матриц вида $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & 0 \\ 0 & 0 \end{pmatrix}$. Пусть $\tilde{C} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \\ c_{31} & c_{32} \end{pmatrix}$. В один класс смежности с $\tilde{C}$ попадают только те матрицы $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \\ b_{31} & b_{32} \end{pmatrix}$, для которых $B - \tilde{C} \in H$, т.е. матрицы $B = \begin{pmatrix} * & * \\ * & c_{22} \\ c_{31} & c_{32} \end{pmatrix}$ с такими же элементами c_{22}, c_{31}, c_{32} как у матрицы $\tilde{C}$.

4.3. Доказать, что подгруппа H группы G нормальна, если

а) G — абелева группа, H — любая ее подгруппа;

б) G — группа невырожденных матриц порядка n, $GL(C,n)$, H — подгруппа матриц с определителем, равным 1.

Решение. В силу критерия нормальной подгруппы

$$H \trianglelefteq G \Leftrightarrow g^{-1}ag \in H, \forall a \in H, \forall g \in G.$$

В случае а) $H \trianglelefteq G$, так как $g^{-1}ag = g^{-1}ga = ea = a \in H, \forall a \in H, \forall g \in G$.

В случае б) заметим сначала, что $H < G$, так как $H^{-1} \subseteq H$ и $HH \subseteq H$. Действительно,

$$\forall B, \det B = 1, B^{-1}B = E \Rightarrow \det(B^{-1})\det B = 1 \Rightarrow \det(B^{-1}) = 1,$$

$$\forall A, \forall B, \det A = 1, \det B = 1 \Rightarrow \det(AB) = \det A \det B = 1.$$

Более того, $H \trianglelefteq G$, так как

$$\forall B \in G, B^{-1}B = E \Rightarrow \det(B^{-1})\det B = 1 \Rightarrow \det(B^{-1}) = \frac{1}{\det B},$$

$$\det(B^{-1}AB) = \det(B^{-1})\det A \det B = \det(B^{-1})\det B \det A = \det A.$$

4.4. Найти смежные классы:

а) аддитивной группы Z по подгруппе nZ, n — натуральное число;

б) аддитивной группы C по подгруппе $Z[i]$ целых гауссовых чисел, т.е. чисел $a+bi$ с целыми a, b;

в) аддитивной группы R по подгруппе Z;

г) мультипликативной группы $C\setminus\{0\}$ по подгруппе чисел U с модулем 1;

д) мультипликативной группы $C\setminus\{0\}$ по подгруппе положительных вещественных чисел R_+.

Решение. а) Заметим сначала, что $nZ\cdot nZ\subseteq nZ, (nZ)^{-1}=(-n)Z\subseteq nZ\Rightarrow nZ<Z$. Разложение аддитивной группы целых чисел Z по подгруппе чисел, кратных n, состоит из n различных смежных классов с представителями $0,1,\ldots,n-1$. При этом в классе $l+nZ$ с представителем l, $0\le l\le n-1$, собраны все те числа, которые при делении на n дают остаток l.

б) Нетрудно проверить, что $Z[i]<C$ в силу определения операции сложения комплексных чисел. Обозначим через $[x]$ целую часть вещественного числа, т.е. округление x до ближайшего целого в меньшую сторону ($[x]\le x$ и $x-[x]\ge 0$). Пусть $x+iy$ — произвольное комплексное число. Тогда в один класс смежности с $x+iy$ попадают все комплексные числа $\tilde{x}+i\tilde{y}$, для которых $\tilde{x}-[\tilde{x}]=x-[x]\Rightarrow \tilde{x}-x=([\tilde{x}]-[x])\in Z$ и $\tilde{y}-[\tilde{y}]=y-[y]\Rightarrow(\tilde{y}-y)\in Z$ или $\tilde{x}+i\tilde{y}-(x+iy)=(\tilde{x}-x)+i(\tilde{y}-y)\in Z[i]$. Другими словами, класс смежности имеет вид $\lambda+Z+i(\beta+Z)$ с представителем $\lambda+i\beta$, где $\lambda\in[0,1)$, $\beta\in[0,1)$.

в) Найдем смежные классы аддитивной группы R по подгруппе Z. Операция сложения коммутативная. Поэтому левые и правые смежные классы совпадают. Пусть a — произвольное вещественное число. В силу критерия 4.1 два вещественных числа a и a_1 принадлежат одному смежному классу аддитивной группы R по подгруппе Z, если $a_1-a\in Z\Rightarrow a_1-[a_1]=a-[a]$.

Смежный класс имеет вид $\{x+a-[a]:\forall x\in Z\}$ с представителем $a-[a]\in[0,1)$.

г) Заметим сначала, что в силу свойств модуля комплексных чисел множество $U=\{z\in C: |z|=1\}$ образует подгруппу в мультипликативной группе комплексных чисел $C\setminus\{0\}$. Поэтому смежными классами будут множества комплексных чисел, расположенных на окружностях $\{z\in C: |z|=r\}$ $\forall r>0$.

д) Найдем смежные классы мультипликативной группы $C\setminus\{0\}$ по подгруппе R_+. Операция умножения коммутативная. Поэтому левые и правые смежные классы совпадают. В силу критерия 4.1 два комплексных числа $z=a+ib$ и $z_1=a_1+ib_1$ принадлежат одному смежному классу группы $C\setminus\{0\}$ по подгруппе R_+, если

$$\frac{z}{z_1}=\frac{a+ib}{a_1+ib_1}=\frac{(a+ib)(a_1-ib_1)}{a_1^2+b_1^2}=\frac{aa_1+bb_1+i(ba_1-ab_1)}{a_1^2+b_1^2}\in R_+\Rightarrow ba_1-ab_1=0\to\frac{b}{b_1}=\frac{a}{a_1}=\lambda\in R_+.$$

В итоге смежный класс имеет вид $\{\lambda z:\forall\lambda\in R_+\}$ с представителем $z\in C\setminus\{0\}$.

5. Нормализатор. Центр. Порождающее множество. Коммутант

Если A, B — два подмножества группы, то обозначают $A^B = \{a^b : a \in A, b \in B\}$. Как было доказано (предложение 4.5) H — нормальная подгруппа группы G $H \trianglelefteq G \Leftrightarrow H^G \subseteq H$.

Определение нормализатора. Нормализатором множества M в подгруппе H называется множество

$$N_H(M) = \{h : h \in H, M^h = M\}.$$

Теорема 5.1 (о нормализаторе). Если M — подмножество, H — подгруппа группы G, то $N_H(M) \le G$ и мощность класса подмножеств, сопряженных с M элементами из H, равна индексу $|H : N_H(M)|$. В частности, $|a^G| = |G : N_G(a)|$.

Доказательство. Пусть M — подмножество, H — подгруппа группы G. Докажем, что $N_H(M) \le G$. Очевидно, $e \in N_H(M)$. Заметим, что для $a, b \in M$, где $a = h^{-1}bh$, имеем $b = hah^{-1}$. Отсюда из $h \in N_H(M)$ следует, что $h^{-1} \in N_H(M)$.

Кроме того, $N_H(M)$ замкнуто относительно операции. Пусть $h, h_1 \in N_H(M)$, по определению имеем $M^h = M$ и $M^{h_1} = M$. Тогда $M^{hh_1} = (M^h)^{h_1} = M^{h_1} = M$. Итак, $N_H(M) \le G$. Отобразим множества M^h, $h \in H,$ на правые смежные классы группы H по подгруппе $N = N_H(M)$, полагая $(M^h)^\varphi = Nh$ для $h \in H$. Отображение φ однозначно, так как из $M^h = M^{h_1}$ следует, что $Nh = Nh_1$. Отображение φ переводит разные элементы в разные, так как из $Nh = Nh_1$ следует $M^h = M^{h_1}$. Наконец, φ - отображение “на”, так как каждое Nh имеет прообраз M^h.

Теорема доказана.

Пусть M — подмножество, H — подгруппа группы G.

Определение централизатора. Централизатором M в подгруппе H называется

$$C_H(M) = \{h : h \in H, a^h = a \quad \forall a \in M\}.$$

Предложение 5.1 (о централизаторе нормальной подгруппы). Централизатор нормальной подгруппы сам является нормальной подгруппой.

Доказательство. Пусть $H \trianglelefteq G$. Докажем, что $(C_G(H))^g \subseteq C_G(H)$.

$$a \in C_G(H), g \in G, h \in H \Rightarrow (g^{-1}ag)^{-1}hg^{-1}ag = g^{-1}a^{-1}(ghg^{-1})ag.$$

$$H \trianglelefteq G \Rightarrow \exists h_1 \in H : h_1 = ghg^{-1} \Rightarrow h = g^{-1}h_1g \Rightarrow g^{-1}a^{-1}(ghg^{-1})ag = g^{-1}a^{-1}h_1ag.$$

$$a \in C_G(H) \Rightarrow g^{-1}a^{-1}h_1ag = g^{-1}h_1g = h \Rightarrow g^{-1}ag \in C_G(H) \Rightarrow C_G(H) \trianglelefteq G.$$

Предложение доказано.

Определение центра. Централизатор всей группы G называется центром и обозначается $C(G)$.

Предложение 5.2 (об индексе централизатора нормальной подгруппы). Если H — конечная нормальная подгруппа группы G, то индекс ее централизатора конечен.

Доказательство. По определению централизатора $C_G(H)=\bigcap_{h\in H} C_G(h)$. В силу предложения 4.3 $|G:C_G(H)|=|G:\bigcap_{h\in H} C_G(h)|\le \prod_{h\in H}|G:C_G(h)|$.

Каждому смежному классу $(C_G(h))g$ можно поставить в соответствие однозначно элемент $g^{-1}hg=h_1\in H$, так как H — нормальная подгруппа группы G и для любого $a\in C_G(h)$ имеем $(ag)^{-1}hag=g^{-1}a^{-1}hag=g^{-1}hg=h_1$. Поэтому $|G:C_G(h)|\le|H|$ и $|G:C_G(H)|=|G:\bigcap_{h\in H} C_G(h)|\le \prod_{h\in H}|G:C_G(h)|\le|H|^{|H|}$.

Предложение доказано.

Определение подгруппы, порожденной множеством. Если M — подмножество группы G, то пересечение (M) всех подгрупп, содержащих M, называется подгруппой, порожденной M.

Теорема 5.2 (о подгруппе, порожденной множеством). Если M — подмножество группы G, то

$$(M)=\{a_1^{\varepsilon_1}...a_m^{\varepsilon_m}: a_i\in M, \varepsilon_i=\pm1, m=1,2,...\}.$$

Доказательство. Обозначим правую часть через H. Так как подгруппа (M) содержит все a_i из M, то $(M)\supseteq H$. С другой стороны $HH\subseteq H$, $H^{-1}\subseteq H$. Поэтому H подгруппа, содержащая M. Отсюда $H\supseteq(M)$ и окончательно $H=(M)$.

Теорема доказана.

Определение коммутатора. Коммутатором элементов a,b группы G называется выражение $a^{-1}b^{-1}ab$ и обозначается $[a,b]$.

Определение коммутанта. Подгруппа, порожденная в G всевозможными коммутаторами, называется коммутантом группы G.

Замечание. Группа G тогда и только тогда абелева, когда ее коммутант состоит из e.

Определение взаимного коммутанта. Если L, M — подмножества группы G, то их взаимным коммутантом называют подгруппу

$$[L,M]=([a,b]: a\in L, b\in M).$$

Предложение 5.3 (о взаимном коммутанте нормальных подгрупп). Взаимный коммутант нормальных подгрупп $[H,H_1]$ является нормальной подгруппой.

Доказательство. $H\trianglelefteq G\Rightarrow a^g\in H, \forall a\in H, \forall g\in G$, $H_1\trianglelefteq G\Rightarrow b^g\in H, \forall b\in H_1, \forall g\in G$.

$[a,b]^g=g^{-1}a^{-1}b^{-1}abg=(g^{-1}a^{-1}g)(g^{-1}b^{-1}g)(g^{-1}ag)(g^{-1}bg)=(a^g)^{-1}(b^g)^{-1}a^gb^g=[a^g,b^g]$.

Отсюда порождающее множество взаимного коммутанта нормальных подгрупп инвариантно относительно сопряжения произвольным элементом $g\in G$.

Предложение доказано.

Задачи

5.1. Доказать, что если $|G:H|=2$, то $H\triangleleft G$.

Решение. Так как $|G:H|=2$, то для произвольного элемента $g\notin H$ имеем $G=H\cup gH$ и $G=H\cup Hg$. Так как $Hg\cap H=\emptyset$, то $Hg=gH$. Следовательно, H является нормальной подгруппой.

5.2. Доказать, что если $A\trianglelefteq G$, $B\trianglelefteq G$, то $AB\trianglelefteq G$.

Решение. Покажем сначала, что множество $AB=\{ab:\forall a\in A,\forall b\in B\}$ образует подгруппу.

Рассмотрим произведение двух элементов из этого множества aba_1b_1. Так как A нормальная подгруппа и $bA=Ab$, то найдется такой элемент $a_2\in A$, что $ba_1=a_2b$. Поэтому $aba_1b_1=aa_2bb_1\in AB$, т.е. AB замкнуто относительно операции.

Далее AB содержит единицу и обратные элементы: $b^{-1}a^{-1}=b^{-1}a^{-1}bb^{-1}=a_1b^{-1}\in AB$, где $a_1\in A$, поскольку A - нормальная подгруппа.

Подгруппа AB инвариантна относительно сопряжения $g^{-1}abg=(g^{-1}ag)(g^{-1}bg)\in AB$ и в силу предложения 4.5 является нормальной подгруппой.

5.3. Найти порождающее множество для мультипликативной группы положительных рациональных чисел Q_+, отличное от Q_+.

Решение. $Q_+=\left(\frac{1}{n}:n=1,2,...\right)$, так как $\frac{p}{q}=\frac{1}{q}\left(\frac{1}{p}\right)^{-1}$ для каждого рационального числа.

5.4. Проверить, что а) $(ab)^g=a^gb^g$; б) $a^{gg_1}=(a^g)^{g_1}$; в) $[a,b]^{-1}=[b,a]$, г) $[ab,c]=[a,c]^b[b,c]$, д) $[a^{-1},b]=[b,a]^{a^{-1}}$.

Решение. а) $(ab)^g=g^{-1}abg=(g^{-1}ag)(g^{-1}bg)=a^gb^g$.

б) $a^{gg_1}=(gg_1)^{-1}agg_1=g_1^{-1}(g^{-1}ag)g_1=g_1^{-1}a^gg_1=(a^g)^{g_1}$.

в) $[a,b]^{-1}=(a^{-1}b^{-1}ab)^{-1}=b^{-1}a^{-1}ba=[b,a]$.

г) $[ab,c]=(ab)^{-1}c^{-1}abc=b^{-1}a^{-1}c^{-1}abc=b^{-1}a^{-1}c^{-1}acc^{-1}bc=(b^{-1}a^{-1}c^{-1}acb)(b^{-1}c^{-1}bc)=[a,c]^b[b,c]$.

д) $[a^{-1},b]=ab^{-1}a^{-1}b=a(b^{-1}a^{-1}ba)a^{-1}=[b,a]^{a^{-1}}$.

5.5. Доказать, что а) порядки сопряженных элементов равны; б) $|Z:(n)|=n$.

Решение. а) $e=a^m\Rightarrow(g^{-1}ag)^m=g^{-1}a^mg=g^{-1}eg=e,\forall g$.

б) $(n)=nZ\Rightarrow Z=\bigcup_{k=0}^{n-1}(k+nZ)$. Следовательно, $|Z:(n)|=n$.

5.6. Найти а) централизатор диагональной матрицы в $GL(2,P)$, где $P=C\vee R\vee Q$; б) минимальное порождающее множество для аддитивной группы целых чисел.

Решение. а) Пусть A — диагональная матрица. По определению $C_{GL(2,P)}(A)=\{B\in GL(2,P):B^{-1}AB=A\vee AB=BA\}$.

$$AB=\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}=\begin{pmatrix}\alpha a_{11}&\alpha a_{12}\\\beta a_{21}&\beta a_{22}\end{pmatrix},\ BA=\begin{pmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{pmatrix}\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}=\begin{pmatrix}\alpha a_{11}&\beta a_{12}\\\alpha a_{21}&\beta a_{22}\end{pmatrix}.$$

Равенство $AB=BA$ возможно, если $\alpha a_{12}=\beta a_{12}$ и $\alpha a_{21}=\beta a_{21}$.

Следовательно, $C_{GL(2,P)}(A) = GL(2,P)$, если $\alpha = \beta$, и $C_{GL(2,P)}(A)$ состоит из всех невырожденных диагональных матриц, если $\alpha \neq \beta$.

б) минимальным порождающим множеством для аддитивной группы целых чисел является 1 или -1.

6. Гомоморфизм. Фактор-группа

Определение гомоморфизма. Отображение группы G в группу G_1, $f : G \to G_1$, называется гомоморфизмом, если оно сохраняет операцию, т.е. $f(x_1 \circ x_2) = f(x_1) \circ f(x_2)$, где $y_1 = f(x_1)$, $y_2 = f(x_2)$ и $\circ = +$ в случае аддитивной группы и $\circ = \cdot$ в случае мультипликативной группы.

Пример. Отображение $z \to |z|$, ставящее модуль в соответствие произвольному комплексному числу $z \in C$ является гомоморфизмом мультипликативной группы $C \setminus \{0\}$ в мультипликативную группу вещественных чисел $R \setminus \{0\}$, так как в силу свойств модуля комплексного числа сохраняет операцию.

Предложение 6.1. Гомоморфный образ группы $f(G)$ является подгруппой группы G_1.

Доказательство. Действительно, в силу $f(x_1 \circ x_2) = f(x_1) \circ f(x_2)$ имеем $f(G) \circ f(G) = f(G)$. Заметим, что $f(e \circ x) = f(e) \circ f(x) = f(x)$ и $f(x \circ e) = f(x) \circ f(e) = f(x)$, т.е. $f(e)$ является единицей.

Кроме того, $f(x \circ x^{-1}) = f(x) \circ f(x^{-1}) = f(e)$. Отсюда $(f(G))^{-1} = f(G)$.

Предложение доказано.

Далее по-прежнему будем опускать обозначение операции $\circ$.

Определение ядра гомоморфизма. Пусть f — гомоморфизм группы G в группу G_1. Совокупность элементов группы G, которые отображаются f в единицу e_1 группы G_1 называется ядром гомоморфизма. Обозначается $Ker\ f$ (от английского слова kernel).

Замечание. Изоморфизм групп является частным случаем гомоморфизма с ядром, состоящим из единицы.

Предложение 6.2 (о ядре гомоморфизма). Ядро всякого гомоморфизма f группы G является нормальной подгруппой группы G.

Доказательство. Из предложения 6.1 следует, что единица группы G принадлежит ядру гомоморфизма. Пусть g и $g_1 \in Ker\ f$. Тогда $gg_1 \in Ker\ f$, поскольку $f(g)f(g_1) = e_1e_1 = e_1$. Кроме того, $f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e_1$. Таким образом, ядро гомоморфизма замкнуто относительно операции и вместе с любым элементом содержит и обратный элемент. Кроме того, если $g \in Ker\ f$, то для любого элемента h группы G имеем $f(h^{-1}gh) = (f(h))^{-1} f(g) f(h) = (f(h))^{-1} e_1 f(h) = e_1$. Отсюда в силу предложения 4.5 $Ker\ f \trianglelefteq G$.

Предложение доказано.

Пример. Ядром гомоморфизма $z \to |z|$ мультипликативной группы $C \setminus \{0\}$ в мультипликативную группу вещественных чисел $R \setminus \{0\}$ является множество всех комплексных чисел $\{z \in C : |z| = 1\}$, являющееся нормальной подгруппой $C \setminus \{0\}$.

Предложение 6.3 (о фактор-группе). Множество всех смежных классов группы G по нормальной подгруппе H с операцией $gHg_1H = gg_1H$ образует группу, называемую фактор-группой G/H.

Доказательство. Пусть $H \trianglelefteq G$. В этом случае имеем равенство $gH = Hg$, следовательно, $gHg_1H = gg_1HH = gg_1H$, т.е. произведение любых двух смежных классов G по H само будет смежным классом G по H.

Таким образом, на множестве всех смежных классов группы G по нормальной подгруппе H операция определена корректно.

Покажем, что на множестве всех смежных классов группы G по нормальной подгруппе H выполняются все требования, входящие в определение группы.

В самом деле, ассоциативность умножения смежных классов следует из ассоциативности умножения в группе G. Роль единицы играет сама нормальная подгруппа H, являющаяся одним из смежных классов разложения G по H.

Наконец, для смежного класса gH обратным будет смежный класс $g^{-1}H$, так как

$$gHg^{-1}H = eH = H.$$

Предложение доказано.

Замечание. Чтобы найти произведение двух смежных классов группы G по нормальной подгруппе H, следует произвольным образом выбрать в этих смежных классах по одному представителю и взять тот смежный класс, в котором лежит произведение этих представителей.

Определение чисел, сравнимых по модулю. Два целых числа a, b называются сравнимыми по модулю d (пишем $a \equiv b(\mathrm{mod}\, d)$), где d - целое число, если $a - b = cd$ для некоторого целого числа c. Другими словами a, b при делении на d дают одинаковые остатки.

Пример. Числа 21 и 6 сравнимы по модулю 5, т.е. $21 \equiv 6(\mathrm{mod}\, 5)$. Числа 15 и 7 сравнимы по модулю 4, т.е. $15 \equiv 7(\mathrm{mod}\, 4)$.

Определение вычета. Число $a \in Z$ называется вычетом (в теории чисел) числа $b \in Z$ по модулю $m > 1$, если разность $a - b$ делится на m.

Пример. Число 21 — вычет числа 6 по модулю 5. Число 15 — вычет 7 по модулю 4.

Определение классов вычетов. Классы смежности в аддитивной группе Z по нормальной подгруппе mZ называются классами вычетов по модулю m, обозначаемые как $\{l\}_m$, где $0 \le l \le m-1$.

В дальнейшем фактор-группу $Z/(mZ)$ будем обозначать как Z_m.

Пример. Найдем фактор-группу $Z/(4Z) = Z_4$. Обозначим классы вычетов по модулю 4 по их представителям $0,1,2,3$. Построим таблицу Кэли:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Определение естественного гомоморфизма. Если каждому элементу $g \in G$ поставим в соответствие смежный класс $\tilde{g} = gH$ по нормальной подгруппе H, то это отображение гомоморфно, потому что сумма переходит в сумму (в случае аддитивной группы), а произведение в произведение (в случае мультипликативной группы). Указанное отображение называется естественным гомоморфизмом G в фактор-группу G/H.

Теорема 6.1 (о гомоморфизмах). Пусть задан гомоморфизм f группы G на группу G_1. Тогда G_1 изоморфна фактор-группе $G/Ker\, f$, причем существует такое изоморфное отображение σ первой группы на вторую, что результат последовательного выполнения отображений f и σ совпадает с естественным гомоморфизмом группы G на фактор-группу $G/Ker\, f$.

Доказательство. В самом деле, пусть $g_1 \in G_1$ будет произвольный элемент группы, g — такой элемент группы G, что $f(g) = g_1$. Так как для любого элемента a из ядра гомоморфизма $Ker\, f$ имеет место равенство $f(a) = e_1$, где e_1 — единица группы G_1, то

$$f(ga) = f(g)f(a) = f(g)e_1 = g_1,$$

т.е. все элементы смежного класса $gKer\, f$ отображаются f в элемент g_1.

С другой стороны, если h — любой такой элемент группы G, что $f(h) = g_1$, то

$$f(g^{-1}h) = f(g^{-1})f(h) = (f(g))^{-1}f(h) = g_1^{-1}g_1 = e_1,$$

т.е. $g^{-1}h$ содержится в $Ker\, f$. Если мы положим $g^{-1}h = a$, то $h = ga$, т.е. элемент h содержится в смежном классе $gKer\, f$. Таким образом, собирая все те элементы группы G, которые при гомоморфизме f отображаются в фиксированный элемент g_1 группы G_1, мы получаем в точности смежный класс $gKer\, f$.

Соответствие σ, относящее каждому элементу g_1 из G_1 тот смежный класс группы G по нормальной подгруппе $Ker\, f$, который состоит из всех элементов группы G, имеющих g_1 своим образом при отображении f, будет взаимно однозначным отображением группы G_1 на группу $G/Ker\, f$. Это отображение σ будет изоморфизмом, так как если $\sigma(g_1) = gKer\, f$, $\sigma(h_1) = hKer\, f$, т.е. $f(g) = g_1$, $f(h) = h_1$, то $f(gh) = f(g)f(h) = g_1h_1$, а поэтому

$$\sigma(g_1h_1) = ghKer\, f = gKer\, f\, hKer\, f = \sigma(g_1)\sigma(h_1).$$

Наконец, если g — произвольный элемент из G и $f(g) = g_1$, то $\sigma(f(g)) = \sigma(g_1) = gKer\, f$, т.е. последовательное выполнение гомоморфизма f и изоморфизма σ на самом деле отображает элемент g в порождаемый им смежный класс $gKer\ f$.

Теорема доказана.

Задачи

6.1. Какие из отображений $f : C \setminus \{0\} \to R \setminus \{0\}$ являются гомоморфизмами:

а) $f(z) = 2|z|$; б) $f(z) = \dfrac{1}{|z|}$; в) $f(z) = 1 + |z|$; г) $f(z) = |z|^2$; д) $f(z) = 1$; е) $f(z) = 2$?

Решение. а) Пусть $f(z) = 2|z|$, $f(z_1) = 2|z_1|$. f не является гомоморфизмом, так как $f(zz_1) = 2|zz_1| = 2|z||z_1| \neq f(z)f(z_1)$.

б) $f(zz_1) = \dfrac{1}{|zz_1|} = \dfrac{1}{|z||z_1|} = f(z)f(z_1)$. f является гомоморфизмом.

в) $f(zz_1) = 1 + |zz_1| \neq (1+|z|)(1+|z_1|)$. f не является гомоморфизмом.

г) $f(zz_1) = |zz_1|^2 = |z^2||z_1|^2 = f(z)f(z_1)$. f является гомоморфизмом.

д) $f(zz_1) = 1 = 1 \cdot 1 = f(z)f(z_1)$. f является гомоморфизмом.

е) $f(zz_1) = 2 \neq 4 = f(z)f(z_1)$. f не является гомоморфизмом.

6.2. Найти фактор-группу аддитивной группы четных чисел по подгруппе чисел, кратных 4.

Решение. Требуется найти фактор-группу $(2Z)/(4Z)$. Заметим, что $4 = 2 \cdot 2$. Остатки при делении на 2 — $0{,}1$. Следовательно, имеем 2 класса смежности с представителями $0{,}2$. Таблица Кэли:

+	0	2
0	0	2
2	2	0

.

6.3. Найти первообразный корень ε степени 2^2 из 1 и построить гомоморфное отображение f (отличное от $f \equiv 1$) 2-ичной дроби $\dfrac{m}{2^2}$ в группу корней степени 2^2 из 1.

Решение. В примере 1.6 были найдены все корни 4-й степени из 1: $\{\pm 1, \pm i\}$, среди них примитивные — $\{\pm i\}$. Отображение $f\left(\dfrac{m}{4}\right) = \varepsilon^m$, $m \in Z$, является гомоморфизмом, так как $f\left(\dfrac{m}{4} + \dfrac{k}{4}\right) = \varepsilon^{m+k} = \varepsilon^m \varepsilon^k = f\left(\dfrac{m}{4}\right) f\left(\dfrac{k}{4}\right)$.

6.4. Найти все гомоморфные отображения циклической группы $\langle a \rangle$ порядка 6 в циклическую группу $\langle b \rangle$ порядка 3.

Решение. Если $\langle a \rangle = \{e = a^0, a, a^2, a^3, a^4, a^5\}$, $\langle b \rangle = \{\tilde{e} = b^0, b, b^2\}$, то гомоморфные отображения: $f_1(a) = \tilde{e}$, $Ker\ f_1 = \langle a \rangle$; $f_2(a) = b$, $f_2(a^2) = b^2$, $f_2(a^3) = b^3 = \tilde{e}$, $f_2(a^4) = b^4 = b$, $f_2(a^5) = b^5 = b^2$, $Ker\ f_2 = \{e, a^3\}$; $f_3(a) = b^2$, $f_3(a^2) = b^4 = b$, $f_3(a^3) = b^6 = \tilde{e}$, $f_3(a^4) = b^8 = b^2$, $f_3(a^5) = b^{10} = b$, $Ker\ f_3 = \{e, a^3\}$.

7. Кольцо. Почти-кольцо. Подкольцо

Определение кольца. Множество K с двумя бинарными операциями сложением и умножением называется кольцом, если по сложению – это абелева группа, а умножение должно быть связано со сложением законами дистрибутивности: $a(b+c) = ab + ac$, $(b+c)a = ba + ca$.

Пример. Множество целых чисел Z образует кольцо относительно операций сложения и умножения. Действительно, по сложению – это абелева группа, а по умножению – это полугруппа. Умножение связано со сложением законами дистрибутивности.

Замечание. На само умножение в общем случае не накладывается никаких ограничений, т.е. кольцо K по умножению является лишь группоидом.

Если умножение в кольце ассоциативно, то кольцо называется ассоциативным кольцом и K — мультипликативная полугруппа.

Если умножение в кольце и ассоциативно, и коммутативно, то кольцо называется ассоциативно-коммутативным.

Пример. Множество целых чисел Z образует ассоциативно-коммутативное кольцо.

Предложение 7.1 (о дистрибутивности для разности). Во всяком кольце законы дистрибутивности выполняются и для разности, т.е. $a(b-c) = ab - ac$, $(b-c)a = ba - ca$.

Доказательство. Действительно,

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

Аналогично доказывается, что $(b-c)a = ba - ca$.

Предложение доказано.

Предложение 7.2 (о неассоциативном кольце с операцией симметрирования). Если в произвольном ассоциативном кольце K сохраним аддитивную группу, а операцию умножения заменим операцией симметрирования $a \bullet b = ab + ba$, то получим неассоциативное кольцо.

Доказательство. Покажем неассоциативность операции:

$a \bullet (b \bullet c) = a \bullet (bc + cb) = abc + acb + bca + cba$;

$(a \bullet b) \bullet c = (ab + ba) \bullet c = abc + bac + cab + cba$.

Так как по предположению кольцо является только ассоциативным, а коммутативность не предполагается, следовательно, в общем случае $acb \neq bac$, то операция не ассоциативна и множество не является полугруппой относительно операции симметрирования. Однако данное множество является группоидом относительно операции симметрирования. Поэтому получаем неассоциативное кольцо.

Предложение доказано.

Предложение 7.3 (о неассоциативном кольце с операцией коммутирования). Если в произвольном ассоциативном кольце K сохраним аддитивную группу, а операцию умножения заменим операцией коммутирования $a \bullet b = ab - ba$, то получим неассоциативное кольцо.

Доказательство. Покажем неассоциативность кольца. Имеем

$a \bullet (b \bullet c) = a \bullet (bc - cb) = a \bullet bc - a \bullet cb = abc - bca - acb + cba$;

$(a \bullet b) \bullet c = (ab - ba) \bullet c = (ab - ba)c - c(ab - ba) = abc - bac - cab + cba$.

Так как коммутативность не предполагалась, то в общем случае $acb \neq cab$. Поэтому данное множество является неассоциативным кольцом.

Предложение доказано.

Определение (почти-кольца). Множество NR (near-ring) с двумя бинарными операциями сложением и умножением называется (правым) почти-кольцом, если

1) NR — абелева группа относительно сложения; 2) NR — полугруппа относительно умножения; 3) для всех f, g и h имеет место (правая) дистрибутивность $(g + h)f = gf + hf$.

Аналогично можно определить левое почти-кольцо, заменив правую дистрибутивность на левую. Однако, как правило, почти-кольцо определяют как правое почти-кольцо.

Пусть K — произвольное кольцо.

Теорема 7.1 (о свойствах разности). В любом кольце разность элементов обладает следующими свойствами: а) $a - b = c - d$ тогда и только тогда, когда $a + d = b + c$; б) $(a - b) + (c - d) = (a + c) - (b + d)$; в) $(a - b) - (c - d) = (a + d) - (b + c)$; г) $(a - b)(c - d) = (ac + bd) - (ad + bc)$.

Доказательство. Прибавляя $b + d$ к обеим частям равенства $a - b = c - d$, получим: $a + d = b + c$. Обратно, прибавляя $(-b) + (-d)$ к обеим частям второго из этих равенств, получим первое. Этим доказано а). Равенство б), в) и г) доказываются аналогично.

Теорема доказана.

Определение подкольца. Подмножество K_1 кольца K называется подкольцом этого кольца, если оно само является кольцом относительно операций, определенных в кольце.

Замечание. При выяснении того, является ли данное множество кольца подкольцом, нет надобности проверять справедливость всех свойств кольца. Большинство из них автоматически переходит с кольца на любое его подмножество. Для того чтобы непустое подмножество K_1 кольца K было его подкольцом, необходимо и достаточно, чтобы сумма, разность и произведение любых двух элементов из K_1 снова принадлежали K_1. Удобнее всего пользоваться для этого такой теоремой:

Теорема 7.2 (критерий подкольца). Для того, чтобы некоторое подмножество K_1 из кольца K вновь было кольцом (подкольцом кольца K), необходимо и достаточно выполнение следующих условий:

1) это подмножество должно быть подгруппой аддитивной группы кольца; другими словами, вместе с любыми a и b оно должно содержать разность $a-b$ (свойство модулей);

2) вместе с a и b оно должно содержать произведение ab.

Доказательство. Для доказательства необходимости этих условий предположим, что K_1 является подкольцом K. Сложение в K_1 совпадает со сложением в K. Но из единственности обратной операции следует, что и вычитание в K_1 совпадает с вычитанием в K. Поэтому сумма, разность и произведение любых двух элементов из K_1 (определенные в кольце K) должны принадлежать снова K_1, так как иначе одна из этих операций для данных двух элементов K_1 была бы невыполнима в K_1, что противоречит определению кольца и следующей из него выполнимости вычитания. Для доказательства достаточности предположим, что множество K_1 удовлетворяет условиям теоремы. Из свойства модулей следует, что нуль принадлежит K_1, а также вместе с любым элементом a K_1 содержит и $-a$. Поэтому для произвольных элементов a и b оно содержит сумму, так как $a-(-b)=a+b$.Так как сумма и произведение (определенные в K) любых элементов из K_1 снова принадлежат к K_1, то их можно принять за результат сложения и умножения в K_1. Итак, сумма, разность и произведение любых двух элементов из K_1 снова принадлежат K_1. Свойства кольца переносятся автоматически с K на любое его подмножество и, значит, выполнены в K_1, т.е. K_1 является подкольцом кольца K.

Задачи

7.1. Доказать, что множество Λ всех $f:C\to C$ отображений образуют правое почти-кольцо относительно обычной операции сложения и операции суперпозиции в качестве умножения.

Решение. По определению суммы и разности отображений $(f\pm g)(x)=f(x)\pm g(x)$. Так как операция сложения для комплексных чисел коммутативна, то множество отображений образуют абелеву группу по сложению.

По определению суперпозиции имеем правую дистрибутивность:

$(f+g)h(x) = f(h(x)) + g(h(x))$.

7.2. Проверить, что кольцо четных чисел является подкольцом кольца целых чисел.

Решение. По теореме 7.2 достаточно проверить, что множество замкнуто относительно разности и произведения.

Действительно, разность четных чисел и произведение четных чисел вновь будут четными целыми числами.

7.3. Образует ли кольцо множество (2×2)-матриц с элементами a_{ij} из C:

а) с нулевыми последними строками $a_{21}=0$, $a_{22}=0$; б) верхних треугольных матриц?

В случае положительного ответа является ли множество: 1) ассоциативным кольцом; 2) коммутативным кольцом; 3) зависит ли ответ от размерности матриц?

Решение. В случае а) и б) множество замкнуто относительно обеих операций:

а)

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ 0 & 0 \end{pmatrix};$$

б)

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}\begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12}+a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix}, \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} \\ 0 & a_{22}+b_{22} \end{pmatrix}.$$

Сложение и умножение матриц ассоциативны и связаны законами дистрибутивности в силу определения действий над матрицами. Указанные множества — абелевы аддитивные группы, так как включают обратные элементы $-A$ и единичный элемент (нулевую матрицу). В итоге множества в случае а) и б) являются ассоциативными кольцами, но не являются коммутативными кольцами, поскольку операция умножения не перестановочна. Ответ не зависит от размерности матриц.

7.4. Образует ли кольцо множество:

а) неотрицательных целых чисел; б) рациональных чисел?

В случае положительного ответа является ли множество: 1) ассоциативным кольцом; 2) коммутативным кольцом?

Решение. а) множество неотрицательных целых чисел не образует кольцо, так как по сложению не является группой (не содержит обратные элементы).

б) и по сложению, и по умножению – это абелевы группы. Умножение связано со сложением законами дистрибутивности. Множество образует ассоциативно-коммутативное кольцо.

8. Идеал

Среди подколец особую роль играют подкольца, называемые **идеалами**; их роль аналогична роли нормальных подгрупп в теории групп.

Определение идеала. Непустое подмножество I кольца K называется идеалом, точнее, правым идеалом, если

1) из $a \in I$ и $b \in I$ следует, что $a - b \in I$ (свойство модулей);
2) из $a \in I$ следует $ar \in I$ для произвольного $r \in K$.

Аналогично определяется левый идеал.

Предложение 8.1 (о главном идеале кольца). Пусть K – произвольное кольцо, а $r \in K$ – произвольно выбранный элемент. Тогда множество rK является идеалом, называемым главным идеалом кольца K.

Доказательство. Проверим условия 1) и 2) из определения. Действительно, из $a \in rK$ и $b \in rK$ следует, что $a - b \in rK$; из $a \in rK$ следует $ar_1 \in rK$ для произвольного $r_1 \in K$.

Предложение доказано.

Определение смежных классов по идеалу. Любой левый или правый идеал I кольца K определяет некоторое разбиение кольца K на смежные классы по идеалу I или на классы эквивалентности. Два элемента a, b из K называются сравнимыми по идеалу I $(a \sim b)$, если они принадлежат одному классу смежности, т.е. $a - b \in I$.

Напомним, что отношение эквивалентности разбивает все множество на непересекающиеся **классы эквивалентности,** в данном случае, классы смежности по идеалу, называемые **классами вычетов по модулю идеала**.

Каждому элементу $a \in K$ соответствует класс вычетов $\tilde{a}$ (или смежный класс) по идеалу I и это отображение гомоморфно, потому что сумма переходит в сумму, а произведение в произведение. Следовательно, класс вычетов образует снова кольцо. Это кольцо называется кольцом вычетов K/I или фактор-кольцом по идеалу I.

Другими словами гомоморфный образ кольца называется фактор-кольцом.

Как и в случае гомоморфизма групп имеет место следующее утверждение:

Теорема 8.1 (основная теорема о гомоморфизмах). Любой идеал I кольца K определяет структуру кольца на фактор-множестве K/I, причем K/I является гомоморфным образом кольца K с ядром I. Обратно: каждый гомоморфный образ $f(K)$ кольца K изоморфен фактор-кольцу K/I.

Теорема 8.2 (о группе обратимых элементов кольца). Все обратимые элементы кольца K с единицей составляют группу $U(K)$ по умножению.

Доказательство. Очевидно, что единичный элемент $e \in U(K)$. Заметим также, что, если $a \in U(K)$, то $a^{-1} \in U(K)$ и обратный элемент для произведения двух элементов a, b из $U(K)$ также принадлежит $U(K)$, поскольку $(ab)^{-1} = b^{-1}a^{-1}$. В самом деле, предположив, что это не так, получим противоречие: $b^{-1}a^{-1}ab \neq e \Rightarrow a^{-1}ab \neq b \Rightarrow ab \neq ab$. Поэтому $U(K)$ замкнуто относительно умножения. Покажем ассоциативность. Предположим, что найдутся элементы a, b, c в $U(K)$, для которых $(ab)c \neq a(bc)$. Отсюда $a^{-1}(ab)c \neq (bc)$ и, следовательно,

$b^{-1}a^{-1}(ab)c \neq b^{-1}(bc)$ и получаем опять противоречие: $c \neq b^{-1}(bc)$. Поэтому по определению 1.1 $U(K)$ это группа.

Теорема доказана.

Задачи

8.1. Построить кольцо из четырех элементов.

Решение. Рассмотрим кольцо вычетов по модулю 4, т.е. фактор-кольцо $Z/4Z = Z_4$, с двумя операциями:
$$\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}, \quad \begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}.$$

Заметим, что класс вычетов с представителем 2 не обратим.

8.2. Доказать, что множество непрерывных функций вещественного переменного, обращающихся в 0 на некотором подмножестве $D \subseteq [a,b]$, является идеалом в кольце функций, непрерывных на $[a,b]$.

Решение. Покажем сначала, что множество $C[a,b]$ всех непрерывных функций образует кольцо. Как известно сумма и произведение непрерывных функций являются непрерывными функциями. Так как $(f \pm g)(x) = f(x) \pm g(x)$ и $(f \cdot g)(x) = f(x) \cdot g(x)$, то операции сложения и умножения ассоциативны и коммутативны и связаны законом дистрибутивности: $h(x)(f(x)+g(x)) = h(x)f(x) + h(x)g(x)$. Операция умножения в общем случае не обратима. Итак, множество всех непрерывных функций образует абелеву группу по сложению и абелеву полугруппу по умножению, т.е. ассоциативно-коммутативное кольцо.

Рассмотрим теперь множество I непрерывных функций, обращающихся в 0 на некотором подмножестве $D \subseteq [a,b]$. Так как по определению сложения и разности $(f \pm g)(x) = f(x) \pm g(x)$, то из $f \in I$ и $g \in I$ следует, что $f - g \in I$ и I удовлетворяет свойству модулей. Кроме того, из $f \in I$ следует $fh \in I$ для произвольной функции $h \in C[a,b]$. Поэтому множество непрерывных функций, обращающихся в 0 на некотором подмножестве $D \subseteq [a,b]$, является идеалом в кольце $C[a,b]$.

8.3. Доказать, что в кольце матриц $M_n(K)$ с элементами из произвольного кольца K идеалами являются в точности множества матриц, элементы которых принадлежат фиксированному идеалу I кольца K.

Решение. Покажем сначала, что множество $M_n(K)$ образует кольцо. Пусть $A = (a_{ij})$, $B = (b_{ij})$ — матрицы с элементами из K. Пусть $\tilde{C} = AB = (c_{ij})$, где по определению умножения матриц $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}$. В силу определения кольца $c_{ij} \in K$. Сложение и умножение матриц ассоциативны и связаны законами дистрибутивности в силу определения действий над матрицами. $M_n(K)$ — абелева аддитивная группа, так как включает обратные элементы $-A$ и единичный элемент (нулевую матрицу) и полугруппа относительно умножения. Пусть I — идеал кольца K. $\tilde{A} \in M_n(I), B \in M_n(I) \to \tilde{A} - B \in M_n(I)$ по определению разности матриц. Так как

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + ... + a_{in}b_{nj} \in I(\forall a_{ij} \in K, \forall b_{kl} \in I),$$

то $A \in M_n(K), B \in M_n(I) \to AB \in M_n(I)$. Поэтому $M_n(I)$ — идеал кольца $M_n(K)$. Пусть J — идеал кольца $M_n(K)$, а $\tilde{J}$ — множество, состоящее из всех элементов матриц, входящих в J. По определению идеала кольца $M_n(K)$ имеем:

1) $A \in J, B \in J \Rightarrow A - B \in J \Rightarrow a - b \in \tilde{J} \forall a \in \tilde{J} \forall b \in \tilde{J}$;
2) $\forall a \in K, B \in J \Rightarrow aB \in J \Rightarrow \forall a \in K \forall b \in \tilde{J} \Rightarrow ab \in \tilde{J}$,
т.е. $\tilde{J}$ — идеал кольца K.

8.4. Найти все идеалы кольца целых чисел.

Решение. Пусть I — идеал кольца Z. Очевидно, что одноэлементное множество $\{0\}$ является идеалом. Пусть в идеале I есть ненулевые элементы и пусть r — наименьшее положительное число I. Тогда $I = rZ$, т.е все остальные числа нацело делятся на r. Допустим, это не так и найдется в I число $l = nr + q$, где $0 < q < r$. Но в этом случае $q = l - nr \in I$ по определению идеала и мы получили противоречие с тем, что r — наименьшее положительное число I.

9. Алгоритм Евклида

Определение многочлена. Многочленом (или полиномом) n-й степени от неизвестного x называется выражение вида $f(x) = x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$, т.е. лишь сумма целых неотрицательных степеней неизвестного x, взятых с некоторыми числовыми коэффициентами.

Замечание. Произвольная сумма одночленов не является многочленом, как это было принято в элементарной алгебре. В частности, мы не будем считать многочленами такие выражения, которые содержат неизвестное x с отрицательными или дробными показателями.

Определение примитивного многочлена. Многочлен называется примитивным, если наибольший общий делитель системы его коэффициентов является делителем единицы и поэтому может быть принят равным 1.

Если $f(x)$ - произвольный ненулевой многочлен и a — наибольший общий делитель его коэффициентов, то

$$f(x) = a\varphi(x),$$

где $\varphi(x)$- примитивный многочлен.

Определение делителя многочлена. Пусть даны ненулевые многочлены $f(x)$ и $\varphi(x)$ с комплексными коэффициентами. Если остаток от деления $f(x)$ на

$\varphi(x)$ равен нулю, т.е., как говорят, $f(x)$ **делится** (или **нацело делится**) на $\varphi(x)$, то многочлен $\varphi(x)$ называется делителем многочлена $f(x)$.

Многочлен $\varphi(x)$ тогда и только тогда будет делителем многочлена $f(x)$, если существует многочлен $\psi(x)$, удовлетворяющий равенству $f(x)=\varphi(x)\psi(x)$.

Определение общего делителя. Пусть даны произвольные многочлены $f(x)$ и $g(x)$. Многочлен $\varphi(x)$ будет называться общим делителем для $f(x)$ и $g(x)$, если он служит делителем для каждого из этих многочленов.

Определение взаимно простых многочленов. Два многочлена называются взаимно простыми, если общий делитель имеет нулевую степень.

Определение наибольшего общего делителя. Наибольшим общим делителем (н.о.д.) отличных от нуля многочленов $f(x)$ и $g(x)$ называется такой многочлен $d(x)$, который является их общим делителем и, вместе с тем, сам делится на любой другой общий делитель многочленов $f(x)$ и $g(x)$.

Теорема 9.1 (о существовании наибольшего общего делителя). Любые два многочлена обладают наибольшим общим делителем, который находится с помощью алгоритма Евклида.

Доказательство. Совместим доказательство с изложением алгоритма Евклида:

Пусть даны произвольные многочлены $f(x)$ и $g(x)$. Делим $f(x)$ на $g(x)$ и получаем, вообще говоря, некоторый остаток $r_1(x)$. Делим затем $g(x)$ на $r_1(x)$ и получаем остаток $r_2(x)$, делим $r_1(x)$ на $r_2(x)$ и т.д. Так как степени остатков все время понижаются, то в цепочке последовательных делений мы должны дойти до того места, на котором деление совершится нацело и потому процесс остановится. Тот остаток $r_k(x)$, на который нацело делится предыдущий остаток $r_{k-1}(x)$, и будет наибольшим общим делителем многочленов $f(x)$ и $g(x)$.

Для доказательства запишем изложенное:

$$\begin{aligned}
f(x)&=g(x)q_1(x)+r_1(x)\ ,\\
g(x)&=r_1(x)q_2(x)+r_2(x),\\
r_1(x)&=r_2(x)q_3(x)+r_3(x),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
r_{k-3}(x)&=r_{k-2}(x)q_{k-1}(x)+r_{k-1}(x),\\
r_{k-2}(x)&=r_{k-1}(x)q_k(x)+r_k(x),\\
r_{k-1}(x)&=r_k(x)q_{k+1}(x).
\end{aligned}\tag{9.1}$$

Возьмем теперь произвольный общий делитель $\varphi(x)$ многочленов $f(x)$ и $g(x)$. Так как левая часть и первое слагаемое правой части первого равенства делятся на $\varphi(x)$, то $r_1(x)$ также будет делиться на $\varphi(x)$. Переходя ко второму и следующему равенствам, мы таким же способом получим, что на $\varphi(x)$ делятся многочлены $r_2(x), r_3(x),\ldots$. Наконец, если уже будет доказано, что $r_{k-2}(x), r_{k-1}(x)$ делятся на $\varphi(x)$, то из предпоследнего равенства мы получим, что $r_k(x)$ делится на $\varphi(x)$. Таким образом, $r_k(x)$ - наибольший общий делитель $f(x)$ и $g(x)$.

Замечание. Если многочлены $f(x)$ и $g(x)$ имеют оба рациональные или действительные коэффициенты, то и коэффициенты их наибольшего общего делителя также будут рациональными или, соответственно, действительными.

Заметим также, что наибольший общий делитель определяется с точностью до постоянного множителя и имеет коэффициент при старшей степени равный 1. Поэтому можно умножать делимое и сокращать делитель в процессе нахождения наибольшего общего делителя.

Теорема 9.2 **(о связи двух многочленов с их наибольшим общим делителем).** Пусть $d(x)$ — наибольший общий делитель многочленов $f(x)$ и $g(x)$. Тогда найдутся такие многочлены $u(x)$ и $v(x)$, что

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

Можно считать при этом, если степени $f(x)$ и $g(x)$ больше нуля, то степень $u(x)$ меньше степени $g(x)$, а степень $v(x)$ меньше степени $f(x)$.

Доказательство. По теореме 9.1 любые два многочлена обладают наибольшим общим делителем, который находится с помощью алгоритма Евклида.

В предпоследнем равенстве (9.1) пусть $r_k(x)=d(x)$ и $u_1(x)=1$, $v_1(x)=-q_k(x)$. Тогда

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

Подставляя сюда выражения $r_{k-1}(x)$ через $r_{k-3}(x)$ и $r_{k-2}(x)$ из предыдущего равенства (9.1), мы получим:

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

где, очевидно, $u_2(x)=v_1(x)$, $v_2(x)=u_1(x)-v_1(x)q_{k-1}(x)$. Поднимаясь вверх в (9.1), получим утверждение теоремы.

Теорема доказана.

Следствие. Многочлены $f(x)$ и $g(x)$ взаимно просты тогда и только тогда, если можно найти такие многочлены $u(x)$ и $v(x)$, что

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

Задачи

9.1. Пусть $f(x)=x^3-x^2+3x-10$, $g(x)=x^3+6x^2-9x-14$, $d(x)$ — наибольший общий делитель многочленов $f(x)$ и $g(x)$. Найти такие многочлены $u(x)$ и $v(x)$, что $f(x)u(x)+g(x)v(x)=d(x)$.

Решение. Применим к этим многочленам алгоритм Евклида, причем теперь при выполнении делений уже нельзя допускать искажения частных, так как эти частные используются при разыскании многочленов $u(x)$ и $v(x)$. Мы получим такую систему равенств:

$f(x)=g(x)+(-7x^2+12x+4)$;

$$g(x) = (-7x^2 + 12x + 4)\left(-\frac{1}{7}x - \frac{54}{49}\right) + \frac{235}{49}(x-2);$$

$$-7x^2 + 12x + 4 = (x-2)(-7x-2).$$

Отсюда следует, что н.о.д. $f(x)$ и $g(x)$ равен $x-2$.

Из второго равенства находим

$$\frac{49}{235}g(x) - (-7x^2 + 12x + 4)\frac{49}{235}\left(-\frac{1}{7}x - \frac{54}{49}\right) = x-2,$$

а из первого

$$f(x) - g(x) = (-7x^2 + 12x + 4).$$

Поэтому

$$\frac{49}{235}g(x) - (f(x) - g(x))\frac{49}{235}\left(-\frac{1}{7}x - \frac{54}{49}\right) = x-2,$$

что равносильно

$$-f(x)\frac{49}{235}\left(-\frac{1}{7}x - \frac{54}{49}\right) + g(x)\frac{49}{235}\left(-\frac{1}{7}x + 1 - \frac{54}{49}\right) = x-2.$$

Ответ: $u(x) = \dfrac{7}{235}x + \dfrac{54}{235}$ и $v(x) = -\dfrac{7}{235}x - \dfrac{5}{235}$.

9.2. Разделить многочлен $f(x) = x^6 + x^5 + x^3$ с остатком на многочлен $g(x) = x^3 + x + 1$.

Решение:

$$\begin{array}{l|l}
_\,x^6 + x^5 + x^3 & x^3 + x + 1 \\
\quad x^6 + x^4 + x^3 & \overline{x^3 + x^2 - x - 1} \\
\hline
\quad_\,x^5 - x^4 & \\
\qquad x^5 + x^3 + x^2 & \\
\hline
\quad_\,-x^4 - x^3 - x^2 & \\
\qquad -x^4 - x^2 - x & \\
\hline
\qquad_\,-x^3 + x & \\
\qquad\quad -x^3 - x - 1 & \\
\hline
\qquad\qquad 2x + 1 &
\end{array}$$

9.3. Найти наибольший общий делитель н.о.д. многочленов: $f(x)$, $g(x)$, где $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$, $g(x) = 3x^3 + 10x^2 + 2x - 3$.

Решение. Разделим $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ на $g(x) = 3x^3 + 10x^2 + 2x - 3$ ($f(x)$ умножим на 3).

$$\begin{array}{l|l}
_\,3x^4 + 9x^3 - 3x^2 - 12x - 9 & 3x^3 + 10x^2 + 2x - 3 \\
\quad 3x^4 + 10x^3 + 2x^2 - 3x & \overline{\qquad x + 1} \\
\hline
\qquad x^3 - 5x^2 - 9x - 9 &
\end{array}$$

(умножаем на -3)

$$\begin{array}{r} \_3x^3+15x^2+27x+27 \\ 3x^3+10x^2+2x-3 \\ \hline 5x^2+25x+30 \end{array}$$

(остаток сокращаем на 5) $r_1(x)=x^2+5x+6$

$$\begin{array}{r|l} \_3x^3+10x^2+2x-3 & x^2+5x+6 \\ \cline{2-2} 3x^3+15x^2+18x & 3x-5 \\ \cline{1-1} \_-5x^2-16x-3 & \\ -5x^2-16x-3 & \\ \cline{1-1} 9x+27 & \end{array}$$

(остаток сокращаем на 9) $r_2(x)=x+3$

$r_1(x)=x^2+5x+6=r_2(x)(x+2)=(x+3)(x+2)$

Ответ: н.о.д. $f(x)$ и $g(x)$ равен $x+3$.

9.4. Разделить многочлен $f(x)$ с остатком на многочлен $g(x)$:

$f(x)=2x^4-3x^3+4x^2-5x+6$ и $g(x)=x^2-3x+1$;

Решение.

$$\begin{array}{r|l} \_2x^4-3x^3+4x^2-5x+6 & x^2-3x+1 \\ \cline{2-2} 2x^4-6x^3+2x^2 & 2x^2+3x+11 \\ \cline{1-1} \_3x^3+2x^2-5x+6 & \\ 3x^3-9x^2+3x & \\ \cline{1-1} \_11x^2-8x+6 & \\ 11x^2-33x+11 & \\ \cline{1-1} 25x-5 & \end{array}$$

9.5. Найти наибольший общий делитель многочленов:

$f(x)=(x-1)^3(x+2)^2(x-3)(x+4)$ и $g(x)=(x-1)^2(x+2)(x+5)$.

Решение. Заметим, что $(x-1)$ входит в разложение $f(x)$ и $g(x)$. Поэтому в н.о.д. $f(x)$ и $g(x)$ включаем $(x-1)$ в наименьшей степени 2. Аналогично рассуждаем относительно $(x+2)$. Других общих множителей в разложении $f(x)$ и $g(x)$ нет.

Ответ: н.о.д. $f(x)$ и $g(x)$ равен $d(x)=(x-1)^2(x+2)$.

10. Кольцо многочленов

Наряду с определением многочлена, данным в разделе 9, существует более общее определение.

Общее определение многочлена. Пусть K — некоторое кольцо. Построим с помощью нового, не принадлежащего кольцу K, символа x выражения вида $f(x)=\sum a_\nu x^\nu$, в которых суммирование ведется по какому-то конечному множеству целочисленных значений индекса $\nu \geq 0$ и “коэффициенты” a_ν принадлежат кольцу K; например,

$$f(x)=a_0x^0+a_3x^3+a_5x^5.$$

Такие выражения называются многочленами; символ x называется переменной.

Пример. Пусть $f(x)=a_0x^0+a_3x^3+a_5x^5$, $g(x)=b_0x^0+b_4x^4$. Тогда

$$f(x)g(x)=(a_0x^0+a_3x^3+a_5x^5)(b_0x^0+b_4x^4)$$

и

$$f(x)g(x)=a_0b_0x^0+a_3b_0x^3+a_0b_4x^4+a_5b_0x^5+a_3b_4x^7+a_5b_4x^9.$$

Кольцо многочленов обозначается в дальнейшем как $K[x]$ (если K – это R или C, то, соответственно, $R[x]$ и $C[x]$).

Определение степени многочлена. Степенью многочлена (отличного от нуля) называется наибольшее число ν, для которого $a_\nu \neq 0$. Элемент a_ν с таким максимальным ν называется старшим коэффициентом многочлена.

Теорема 10.1 (о кольце многочленов). Многочлены $K[x]$ образуют кольцо.

Доказательство. Определим операцию сложения $f(x)=\sum a_\nu x^\nu$ и $g(x)=\sum b_\nu x^\nu$ как

$$h(x)=f(x)+g(x)=\sum (a_\nu+b_\nu)x^\nu.$$

Получаем абелеву аддитивную группу вследствие того, что коэффициенты принадлежат кольцу.

Умножение связано со сложением законами дистрибутивности и определяется обычным способом, при этом остаются в силе правила $a_\nu x^\nu a_\mu x^\mu = a_\nu a_\mu x^{\nu+\mu}$.

Таким образом, по определению $K[x]$ — это кольцо.

Теорема доказана.

Замечание. $K[x]$ — расширение кольца K.

Пример расширений: R — кольцо вещественных чисел. Тогда с помощью символа i, ($i^2=-1$) получается кольцо комплексных чисел C, т.е. $C=R[i]$ (в дальнейшем выяснится, что это, на самом деле, является полем).

Определение многочленов, сравнимых по модулю. Два многочлена $h(x)$, $f(x)$ называются сравнимыми по модулю $d(x)$ (пишем $h(x)\equiv f(x)(\mathrm{mod}\, d(x))$), где $d(x)$ — многочлен, если $h(x)-f(x)=g(x)d(x)$ для некоторого многочлена $g(x)$. Другими словами $h(x)$, $f(x)$ при делении на $d(x)$ дают одинаковые остатки.

Пример. Пусть $h(x)=x^7+x^4+x^3+1$, $f_1(x)=x^7+x^3+1$, $f_2(x)=x^7+x+1$ — многочлены из кольца $R[x]$. Тогда $h(x)\equiv x^4(\mathrm{mod}\, f_1(x))$, $h(x)\equiv(x^4+x^3-x)(\mathrm{mod}\, f_2(x))$ так как $h(x)=f_1(x)+x^4$ и $h(x)=f_2(x)+x^4+x^3-x$.

Рассмотрим эти же многочлены как многочлены из кольца $Z_2[x]$, т.е. коэффициенты принимают только два значения: $\{0,1\}$, при этом сумма двух одинаковых выражений равна нулю. Тогда по-прежнему $h(x)\equiv x^4(\mathrm{mod}\, f_1(x))$, но $h(x)\equiv(x^4+x^3+x)(\mathrm{mod}\, f_2(x))$, так как $x^4+x^3+x-(x^4+x^3-x)=2x\equiv 0(\mathrm{mod}\, 2)$.

Теорема 10.2 (китайская теорема об остатках). Пусть $b_1,b_2,...,b_n$ — попарно взаимно простые многочлены (целые числа), а $a_1,a_2,...,a_n$ — произвольные многочлены (целые числа). Тогда существует многочлен (целое число) a такой, что $a \equiv a_i (\mathrm{mod}\, b_i)$ для всех $1 \le i \le n$. Если найдутся два таких a и $\tilde{a}$, то $a \equiv \tilde{a}_i (\mathrm{mod}\, \Pi_{i=1}^{n} b_i)$.

Доказательство. Так как $b_1, b_2, ..., b_n$ попарно взаимно просты, то b_i взаимно прост с $\Pi_{j \ne i} b_j$. Поэтому по теореме 3.2 для всякого $1 \le i \le n$ можно выбрать такие u_i и v_i, что $u_i b_i + v_i \Pi_{j \ne i} b_j = 1$. Отсюда $a_i u_i b_i + a_i v_i \Pi_{j \ne i} b_j = a_i$, т.е.

$$a_i v_i \Pi_{j \ne i} b_j = a_i (\mathrm{mod}\, b_i). \tag{11.1}$$

Тогда достаточно положить $a = \sum_{i=1}^{n} a_i v_i \Pi_{j \ne i} b_j$. Для всякого i все слагаемые, кроме i -го, делятся на b_i, а i -е сравнимо с a_i по модулю b_i в силу (11.1). Существование доказано.

Единственность следует из того, что если $a \equiv \tilde{a} \equiv a_i (\mathrm{mod}\, b_i)$ для всех $1 \le i \le n$, то $a \equiv \tilde{a}_i (\mathrm{mod}\, \Pi_{i=1}^{n} b_i)$, так как $b_1, b_2, ..., b_n$ попарно взаимно просты.

Теорема доказана.

Пример. Рассмотрим пример идеала в кольце многочленов $R[x]$. Все многочлены вида $(x^2+1)Q(x)$, где $Q(x) \in R[x]$ — произвольный многочлен образуют главный идеал (см. предложение 8.1).

Доказательства последующих двух теорем приводятся в расширенных курсах общей алгебры.

Теорема 10.3 (китайская теорема об остатках для произвольных идеалов). Пусть K — кольцо и пусть $I_1, ..., I_n$ — такие идеалы, что $I_i + I_j = K$ при всех $i \ne j$. Для любого семейства элементов $x_1, ..., x_n$ кольца K существует такой элемент $x \in K$, что $x = x_i (\mathrm{mod}\, I_i)$ при всех i.

Теорема 10.4 (основная теорема алгебры). Всякий многочлен с любыми числовыми коэффициентами, степень которого не меньше единицы, имеет хотя бы один корень, в общем случае комплексный.

Предложение 10.1 (о корнях многочлена). Если комплексное (но не действительное) число α служит корнем многочлена $f(x)$ с действительными коэффициентами, то корнем для $f(x)$ будет и сопряженное число $\overline{\alpha}$.

Доказательство. Пусть α служит корнем многочлена

$$f(x) = x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n,$$

т.е. $f(\alpha) = \alpha^n + a_1 \alpha^{n-1} + ... + a_{n-1}\alpha + a_n = 0 \Rightarrow \overline{f(\alpha)} = f(\overline{\alpha}) = 0$.

Предложение доказано.

Замечание. Всякий многочлен $f(x)$ степени n, $n \ge 1$, с любыми числовыми коэффициентами имеет n корней, если каждый из корней считать столько раз, какова его кратность.

Определение разложения многочлена. Пусть дан многочлен $f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n$ и пусть $\alpha_1, \alpha_2, ..., \alpha_n$ — его корни. Тогда $f(x) = a_0 (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$ — разложение многочлена $f(x)$ n-й степени в произведение n линейных множителей.

Определение равных многочленов. Два многочлена $f(x)$ и $g(x)$ равны, если равны их коэффициенты при одинаковых степенях неизвестного.

Замечание. Многочлен нулевой степени – отличное от нуля комплексное число. Число 0 – единственный многочлен, степень которого не определена.

Определение поля. Кольцо F называется полем, если существует единичный элемент e относительно операции умножения, т.е. оно состоит не только из одного нуля и если в нем деление выполнимо, притом однозначным образом, во всех случаях, кроме деления на нуль.

Пример. Множество всех действительных чисел R образует поле. Существует также поле комплексных чисел C, поле рациональных чисел Q, но не может быть поля целых чисел, поскольку обратные элементы по умножению, кроме единицы, не являлись бы целыми.

Пусть F — поле. Рассмотрим кольцо многочленов $F[x]$.

Определение приводимого и неприводимого многочлена над полем. Многочлен $f(x)$ степени n приводим в F, если он может быть разложен над этим полем в произведение двух множителей, степени которых меньше n: $f(x)=\varphi(x)\psi(x)$ и $f(x)$ – неприводим в поле F, если в любом его разложении один из множителей имеет степень 0, другой степень n.

Примеры.

а) многочлен x^2-2 неприводим в поле рациональных чисел, но в поле действительных чисел он приводим: $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$.

б) многочлен x^2+1 неприводим в поле рациональных и действительных чисел, но приводим в поле комплексных чисел: $x^2+1=(x-i)(x+i)$.

Задачи

10.1. Образует ли кольцо множество вещественных чисел вида $x+y\sqrt{2}$, где $x,y\in Q$ (Q – множество рациональных чисел)?

Решение. Q – множество рациональных чисел образует поле и, в частности, кольцо, так как Q замкнуто относительно операций сложения и умножения, и все свойства из определения кольца выполнены. Множество чисел вида $x+y\sqrt{2}$, где $x,y\in Q$, также замкнуто относительно операции сложения. Так как $\sqrt{2}\ \sqrt{2}\ =2$ (рациональное число), то это множество также замкнуто относительно операции умножения. Поэтому это кольцо $Q[\sqrt{2}]$.

10.2. Разложить на линейные и квадратные множители над полем вещественных чисел многочлен: x^6+8.

Решение: Имеем $x^6+8=(x^2+2)(x^4-2x^2+4)$. Поскольку оба сомножителя не имеют вещественных корней, запишем для второго сомножителя представление с неопределенными коэффициентами:

$$(x^4-2x^2+4)=(x^2+ax+b)(x^2+dx+m).$$

Следовательно,

$$(x^4-2x^2+4)=(x^2+ax+b)(x^2+dx+m)=x^4+(d+a)x^3+(b+m+ad)x^2+(bd+am)x+bm.$$

Получим систему уравнений:

$$d+a=0,\ b+m+ad=-2,\ bd+am=0,\ bm=4,$$

вещественные решения которой определяются однозначно

$$d=-a=-\sqrt{6},\ b=m=2.$$

Ответ: $x^6+8=(x^2+2)(x^2+\sqrt{6}x+2)(x^2-\sqrt{6}x+2)$.

10.3. Образует ли кольцо множество многочленов с целочисленными коэффициентами?

Решение. В силу определения операции сложения многочленов множество многочленов с целочисленными коэффициентами образует абелеву группу по сложению и замкнуто относительно умножения. Поэтому данное множество образует кольцо.

10.4. Пусть $x, y, a, b\in Q$. Образует ли кольцо множество вещественных чисел вида а) $x+y\sqrt[3]{2}+a\sqrt[3]{4}$, б) $x+y\sqrt[3]{2}+a\sqrt{3}$; в) $x+y\sqrt{2}+a\sqrt{3}+b\sqrt{6}$; г) $x+y\sqrt[3]{3}+a\sqrt[3]{4}$?

Решение. Во всех случаях достаточно проверить замкнутость относительно умножения: а) образует кольцо, так как по умножению замкнуто:

$$(x+y\sqrt[3]{2}+a\sqrt[3]{4})(x_1+y_1\sqrt[3]{2}+a_1\sqrt[3]{4})=xx_1+2ya_1+2y_1a+(xy_1+x_1y+2aa_1)\sqrt[3]{2}+(ax_1+yy_1+a_1x)\sqrt[3]{4}.$$

б) не образует кольцо, так как по умножению не замкнуто:

$$(x+y\sqrt[3]{2}+a\sqrt{3})(x_1+y_1\sqrt[3]{2}+a_1\sqrt{3})=xx_1+3aa_1+(xy_1+x_1y)\sqrt[3]{2}+yy_1\sqrt[3]{4}+(ya_1+y_1a)\sqrt{3}\sqrt[3]{2}.$$

в) образует кольцо, так как по умножению замкнуто:

$$(x+y\sqrt{2}+a\sqrt{3}+b\sqrt{6})(x_1+y_1\sqrt{2}+a_1\sqrt{3}+b_1\sqrt{6})=xx_1+3aa_1+2yy_1+bb_1+$$
$$+(x_1y+xy_1+3ab_1+3a_1b)\sqrt{2}+(xa_1+x_1a+2by_1+2b_1y)\sqrt{3}+(b_1)\sqrt{6}$$
$$+(xb_1+x_1b+x_1a+ya_1+y_1a)\sqrt{6}.$$

г) не образует кольцо, так как по умножению не замкнуто:

$$(x+y\sqrt[3]{3}+a\sqrt[3]{4})(x_1+y_1\sqrt[3]{3}+a_1\sqrt[3]{4})=xx_1+(xy_1+x_1y)\sqrt[3]{3}+(xa_1+x_1a)\sqrt[3]{4}+$$
$$+(ya_1+y_1a)\sqrt[3]{12}+yy_1\sqrt[3]{9}+2aa_1\sqrt[3]{2}.$$

10.5. Построить многочлен наименьшей степени с комплексными коэффициентами, имеющий:

а) двойной корень 1, простые корни 2, 3 и $1+i$;

б) двойной корень i, простой корень $-1-i$.

Решение. а) $(z-1)^2(z-2)(z-3)(z-1-i)$. б) $(z-i)^2(z+1+i)$.

11. Поле

Напомним, что кольцо F называется полем, если существует единичный элемент e относительно операции умножения, т.е. оно состоит не только из одного нуля и если в нем деление выполнимо, притом однозначным образом, во всех случаях, кроме деления на нуль.

Определение поля Галуа. Конечные поля называются полями Галуа (Galois Field) и обозначаются $GF(q)$, где q - число элементов поля.

Пример. Примером поля Галуа служит Z_p (кольцо вычетов по модулю простого числа p). Это множество чисел $\{0,1...,p-1\}$ образует конечное поле, в котором сложение и умножение производятся по модулю p:

а) Z_2 состоит из двух элементов, сложение: $\begin{array}{ccc} + & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$, умножение: $\begin{array}{ccc} \cdot & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$.

б) Z_3 состоит из трех элементов, сложение: $\begin{array}{cccc} + & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 2 & 0 \\ 2 & 2 & 0 & 1 \end{array}$, умножение: $\begin{array}{cccc} \cdot & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 \\ 2 & 0 & 2 & 1 \end{array}$.

Определение подполя. Подмножество $\tilde{F}$ поля F называется подполем, если F_1 само является полем.

Пример. Поле рациональных чисел Q – подполе поля вещественных чисел R.

Определение изоморфных полей. Поля F и F_1 называются изоморфными, если они изоморфны как кольца.

Замечание. Пусть f - изоморфное отображение F и F_1. По определению $f(0)=0_1$ и $f(e)=e_1$.

Определение простого поля. Поле, не обладающее никаким собственным подполем, называется простым.

Теорема 11.1 (о поле из классов вычетов). Кольцо классов вычетов Z_m является полем тогда и только тогда, когда $m=p$ — простое число.

Доказательство. Пусть p — простое число. Обозначим $\{s\}_p$ — произвольный класс вычетов по модулю p с представителем s, где s взаимно простое с p число. Рассмотрим элементы $s, 2s, ..., (p-1)s$. Все они являются представителями разных классов вычетов, т.к. p — простое число. Действительно, предположив, что $ks - ms = pl$ при $k \neq m$ ($k<p$, $m<p$, $0<k-m<p$) и некоторого целого числа l, получим $(k-m)s = pl$. Отсюда $\frac{(k-m)s}{p} = l$ целое число, что невозможно. Поэтому среди классов $s+pZ$ $2s+pZ$,…, $(p-1)s+pZ$ найдется класс $1+pZ$, т.е. $\{s\}_p$ обратим. Если p не является простым числом, то классы вычетов с представителями, являющимися делителями p, будут не обратимы.

Теорема доказана.

Пример. Рассмотрим кольцо вычетов по модулю 4, т.е. фактор-кольцо Z_4, с двумя операциями: $\begin{array}{c|cccc} + & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{array}$, $\begin{array}{c|cccc} \cdot & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 0 & 2 \\ 3 & 0 & 3 & 2 & 1 \end{array}$.

Заметим, что класс вычетов с представителем 2 не обратим. Поэтому Z_4 не является полем.

Замечание. Утверждение, аналогичное теореме 11.1, имеет место и для многочленов. Фактор-кольцо $F[x]/\langle g(x)\rangle$ является полем тогда и только тогда, когда $g(x)$ — неприводимый многочлен над полем F.

Пример. Построить кольцо классов вычетов по модулю полинома $g(x) = x^2 + x + 1$ над полем Z_2.

Решение. Многочлены вида $a(x) = g(x)Q(x) + r(x)$, где $r(x)$ – произвольный многочлен, степень которого меньше 2, при фиксированном $r(x)$ образуют класс вычетов по модулю $x^2 + x + 1$. Так как всего имеется $2^2 = 4$ разных многочлена $r(x)$ степени меньше 2 над Z_2, то возможны 4 следующие класса вычетов (табл. 11.1):

Таблица 11.1

$r(x) = 0$	$\leftrightarrow$	$a(x) = Q(x)(x^2 + x + 1)$
$r(x) = 1$	$\leftrightarrow$	$a(x) = Q(x)(x^2 + x + 1) + 1$
$r(x) = x$	$\leftrightarrow$	$a(x) = Q(x)(x^2 + x + 1) + x$
$r(x) = x + 1$	$\leftrightarrow$	$a(x) = Q(x)(x^2 + x + 1) + x + 1$

Здесь $Q(x)$ – произвольный многочлен. В качестве представителей классов обычно выбирают вычеты наименьшей степени, которые совпадают с многочленами $r(x)$ и образуют кольцо классов вычетов по модулю многочлена $x^2 + x + 1$, т.е. множество $(0,1, x, x + 1)$.

Пример. Найдем все многочлены степени 2, неприводимые над полем Z_2. Для этого рассмотрим всевозможные произведения $x, x+1,$ многочленов степени 1 над Z_2 в табл. 11.2.

Таблица 11.2

$\cdot$	x	$x+1$
x	x^2	$x^2 + x$
$x+1$	$x^2 + x$	$x^2 + 1$

Заметим, что $(x+1)(x+1) = x^2 + 2x + 1 = x^2 + 1$ над полем Z_2. Число различных многочленов второй степени над полем Z_2 равно $1 \cdot 2 \cdot 2 = 4$, из них, как следует из табл. 11.2, приводимыми являются x^2, $x^2 + x$, $x^2 + 1$. Поэтому $x^2 + x + 1$ неприводим над Z_3.

Определение характеристики поля (кольца). Пусть F — произвольное кольцо или поле. Если существует такое целое положительное число n, что для каждого элемента $r \in F$ выполняется равенство $nr = \underbrace{r + ... + r}_{n} = 0$, то наименьшее из таких чисел n называется характеристикой поля (кольца) F и обозначается символом $char\, F$. При этом поле (кольцо) называется полем (кольцом) положительной характеристики.

Если же таких чисел n не существует, то полагают $char\, F = 0$ и называют F полем (кольцом) характеристики нуль.

Пример. Для полей Q, C, R равенство $n1=0$ означает, что $n=0$. Поэтому говорят, поля Q, C, R имеют характеристику 0.

Замечание. Существуют поля, в которых $n1=0$ возможно при $n \neq 0$. Поле Z_p имеет характеристику p, так как $p\{s\}_p = \{0\}_p$.

Пример. В кольце $Z_2[x]$ многочленов над полем Z_2 выполнены равенства:

$$(1+x+x^2)+(x+x^3)=1+x^2+x^3;\ (1+x+x^2)\cdot(x+x^3)=x+x^2+x^4+x^5,$$

т.е. $char\, Z_2[x]=2$.

Замечание. Деление в кольце многочленов не всегда возможно даже на ненулевой многочлен. Например, деление невозможно, если степень делимого меньше степени делителя.

Пример. Рассмотрим поле Галуа $GF(2^2)=Z_2[x]/\langle g(x)\rangle$ из многочленов над двоичным полем, где $g(x)=x^2+x+1$ неприводимый над полем Z_2 многочлен второй степени. Остатки от деления на многочлен второй степени имеют степень, не превышающую 1. Число различных многочленов первой степени над полем Z_2 равно 2^2. Поэтому число различных элементов в фактор-кольце $Z_2[x]/\langle g(x)\rangle$ или число различных классов вычетов по модулю $g(x)$ также равно 2^2. Выполняя действия в табл. 11.3, следует помнить, что все коэффициенты рассматриваются по модулю 2. Z_2 является подполем $Z_2[x]/\langle g(x)\rangle$.

Таблица 11.3

$+$	0	1	x	$x+1$		$\cdot$	0	1	x	$x+1$
0	0	1	x	$x+1$		0	0	0	0	0
1	1	0	$x+1$	x		1	0	1	x	$x+1$
x	x	$x+1$	0	1		x	0	x	$x+1$	1
$x+1$	$x+1$	x	1	0		$x+1$	0	$x+1$	1	x

Заметим, что обратный элемент к классу вычетов с представителем $x+1$ будет класс вычетов с представителем x.

Замечание. Поле Галуа $GF(p^n)=Z_p[x]/\langle g(x)\rangle$ состоит из классов вычетов в кольце многочленов над Z_p по модулю неприводимого над Z_p многочлена n-й степени $g(x)$. Остатки от деления на многочлен второй степени имеют степень, не превышающую $n-1$. Число различных многочленов $n-1$-степени над полем Z_p равно p^n. Поэтому число различных элементов в фактор-кольце $Z_p[x]/\langle g(x)\rangle$ или число различных классов вычетов по модулю $g(x)$ также равно p^n. Выполняя действия, следует помнить, что все коэффициенты рассматриваются по модулю p. Z_p является подполем $Z_p[x]/\langle g(x)\rangle$. Поле Галуа $GF(p^n)=Z_p[x]/\langle g(x)\rangle$ имеет характеристику p. Если вместо $g(x)$ рассмотреть другой неприводимый над Z_p многочлен n-й степени, то получится поле $GF(p^n)$, изоморфное первоначальному полю.

Задачи

11.1. Доказать, что если f — гомоморфизм полей F и F_1 с $Kerf \neq \{0\}$, то $Kerf = F$.

Решение. Пусть

$$Kerf \neq \{0\} \Rightarrow \exists a : f(a) = 0_1,\ a \neq 0 \Rightarrow f(e) = f(aa^{-1}) = f(a) f(a^{-1}) = 0_1.$$

Следовательно,

$\forall b\ f(b) = f(eb) = f(e) f(b) = 0_1$. Отсюда $Kerf = F$.

11.2. Найдем все многочлены степени 2, неприводимые над полем Z_3. Для этого рассмотрим всевозможные произведения $x, 2x, x+1, x+2, 2x+1, 2x+2$ многочленов степени 1 над Z_3 в табл. 11.4.

Таблица 11.4

$\cdot$	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
x	x^2	$2x^2$	x^2+x	x^2+2x	$2x^2+x$	$2x^2+2x$
$2x$	$2x^2$	x^2	$2x^2+2x$	$2x^2+x$	x^2+2x	x^2+x
$x+1$	x^2+x	$2x^2+2x$	x^2+2x+1	x^2+2	$2x^2+1$	$2x^2+x+2$
$x+2$	x^2+2x	$2x^2+x$	x^2+2	x^2+x+1	$2x^2+2x+2$	$2x^2+1$
$2x+1$	$2x^2+x$	x^2+2x	$2x^2+1$	$2x^2+2x+2$	x^2+x+1	x^2+2
$2x+2$	$2x^2+2x$	x^2+x	$2x^2+x+2$	$2x^2+1$	x^2+2	x^2+2x+1

Заметим, что $2x(2x+1) = 2x^2 + 4x = 2x^2 + x$ над полем Z_3 и т.д. Число различных многочленов второй степени над полем Z_3 равно 18, из них, как следует из табл. 11.4, приводимыми являются x^2, $2x^2$, x^2+x, x^2+2x, $2x^2+x$, $2x^2+2x$, x^2+2x+1, x^2+2, $2x^2+1$, $2x^2+x+2$, x^2+x+1, $2x^2+2x+2$, x^2+2x+1. Поэтому x^2+1, x^2+x+2, x^2+2x+2, $2x^2+2$, $2x^2+x+1$, $2x^2+2x+1$ неприводимы над Z_3.

11.3. Построить кольцо классов вычетов по модулю полинома $g(x) = x^2 + 1$ над полем Z_3.

Решение. Многочлены вида $a(x) = g(x)Q(x) + r(x)$, где $r(x)$ – произвольный многочлен, степень которого меньше 2, при фиксированном $r(x)$ образуют класс вычетов по модулю x^2+1. Так как всего имеется $3^2 = 9$ разных многочленов $r(x)$ степени меньше 2 над Z_3, то возможны 9 следующих классов вычетов (табл. 11.5). Здесь $Q(x)$ – произвольный многочлен. В качестве представителей классов обычно выбирают вычеты наименьшей степени, которые совпадают с многочленами $r(x)$ и образуют кольцо классов вычетов по модулю многочлена x^2+1, т.е. множество $(0, 1, 2, x, 2x, x+1, x+2, 2x+1, 2x+2)$.

Таблица 11.5

$r(x)=0$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)$
$r(x)=1$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+1$
$r(x)=2$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+2$
$r(x)=x$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+x$
$r(x)=2x$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+2x$
$r(x)=x+1$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+x+1$
$r(x)=x+2$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+x+2$
$r(x)=2x+1$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+2x+1$
$r(x)=2x+2$	$\leftrightarrow$	$a(x)=Q(x)(x^2+1)+2x+2$

11.3. Построить поле $GF(9)$.

Решение. Искомое поле есть $GF(9)=Z_3[x]/\langle x^2+1\rangle$ (см. табл.11.6 и табл.11.7).

Таблица 11.6

+	**0**	**1**	**2**	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Таблица 11.7

×	**0**	**1**	**2**	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Заметим, что $9=3^2$. Поэтому необходимо найти многочлен степени 2, неприводимый над полем Z_3. Таким многочленом является, например, x^2+1.

Если вместо x^2+1 взять другой многочлен, то получится новое поле, изоморфное старому.

Заключение

Поле Галуа $GF(p^n)$ содержит всегда p^n элементов, где p - простое число, n - натуральное число. Элементы $GF(p^n)$ — классы вычетов по модулю $f(x)$, неприводимого над Z_p многочлена n-й степени. Для построения поля из q элементов необходимо представить q в виде p^n, где p - простое число, n - натуральное число. Далее следует выбрать $f(x)$, где $f(x)$ — неприводимый над Z_p многочлен n степени.

Предупреждение возможных угроз безопасности информации и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами.

Арифметика поля Галуа широко используется в криптографии. В ней работает вся теория чисел, поле содержит числа только конечного размера, при делении отсутствуют ошибки округления. Многие криптосистемы основаны на $GF(p)$, где p — это большое простое число.

Чтобы еще более усложнить вопрос, криптографы также используют арифметику по модулю неприводимых многочленов степени n, коэффициентами которых являются целые числа по модулю p, где p — это по-прежнему простое число, т.е. рассматривают $GF(p^n)$. Используется арифметика по модулю $f(x)$, где $f(x)$ — неприводимый над Z_p многочлен n степени.

Литература

1. Курош А.Г. Курс высшей алгебры. - М.: Наука: Изд-во физ.-мат. литературы, 1971.

2. Курош А.Г. Лекции по общей алгебре. - М.: Наука: Изд-во физ.-мат. литературы, 1973.

3. Ван дер Варден. Алгебра. - М.: Наука: Изд-во физ.-мат. литературы, 1979.

4. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. - М.: Наука, 1972.

5. Сборник задач по алгебре / под ред. А.И. Кострикина. - М.: Физ. мат.лит., 2001.

6. Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры. - М.: Физ.мат.лит., 2004.

7. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. - М.: Наука: Изд-во физ.-мат. литературы, 1976.

8. Pilz G. Near-Rings. The Theory and its Applications. North-Holland, Amsterdam, 1983.

9. Ленг С. Алгебра. - М.: Мир, 1968.

10. http://ru.wikiversity.org

11. http://ru.wikipedia.org

Приложение 1

Список обозначений

$\tau(a,b)$ или $a\tau b$ – бинарная операция.

$z^* = x - iy$ (или $\bar{z}$) – комплексно сопряженное числу $z = x + iy$.

$|z| = \sqrt{x^2 + y^2}$ – модуль комплексного числа $z = x + iy$.

Z – множество целых чисел – это кольцо, аддитивная группа.

N – множество натуральных чисел не образуют группу.

Q – множество рациональных чисел (поле).

C – множество комплексных чисел (поле).

R – множество вещественных чисел (поле)

R_+ – множество положительных вещественных чисел (мультипликативная группа).

G – группа.

e - единица в группе G.

$G = \langle a \rangle$ - циклическая группа с образующим a.

U_n - группа комплексных корней степени n из 1.

$GL(n,F)$ – не абелева мультипликативная группа невырожденных матриц размерности $n \times n$ с элементами из поля F.

$UT(n,F)$ - множество всех матриц с нулевым углом под главной диагональю и с единицами по диагонали и элементами из F:

$$A = \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 0 & 1 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$ (унитреугольная группа).

$\det A$ — определитель матрицы.

$b = g^{-1}ag = a^g$, т.е. b получается из a трансформированием элементом g или элемент a сопряжен с элементом b посредством элемента g.

$H \le G$ — подгруппа группы G.

$|G:H|$ — индекс подгруппы H в группе G (мощность множества смежных классов группы G по подгруппе H).

$H \trianglelefteq G$ — нормальная подгруппа группы G.

G/H — фактор-группа, т.е. группа, элементами которой являются смежные классы группы G по нормальной подгруппе H.

$Z_n = Z/nZ$ - кольцо вычетов по модулю n или фактор-кольцо из целых чисел по идеалу nZ.

$[a,b] = a^{-1}b^{-1}ab$ — коммутатор элементов a,b группы G.

K — кольцо.

$\{s\}_p$ — класс вычетов по модулю p.

$char\,F$ — характеристика поля F.

$GF(q) = F_q$ - поле Галуа (Galois Field), где q - число элементов поля.

$K[x]$ — кольцо многочленов от переменной x над кольцом K.

$GF(p^n)$ — фактор-кольцо $Z_p[x]/\langle f(x)\rangle$, где p - простое число, n - натуральное число, $f(x)$ - неприводимый над Z_p многочлен n степени.

Приложение 2

Задачи для самостоятельного решения

1. Пусть $G = \langle a\rangle$ — циклическая группа порядка n и $b = a^k$. Доказать, что элемент b тогда и только тогда будет образующим группы G, когда числа n и k простые.

2. Пусть p - простое число, ε_n - первообразный корень степени p^n из 1 в поле комплексных чисел, причем $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1,2,\ldots$. Отображение, сопоставляющее p-ичной дроби $\frac{m}{p^n}$ ($Q(p)$ - абелева группа по сложению) комплексное число ε_n^m (абелева группа по умножению), является ли гомоморфизмом?

3. Найти фактор-группу аддитивной группы целых чисел, кратных 4, по подгруппе чисел, кратных 24.

4. Найти все гомоморфные отображения циклической группы $G = \langle a\rangle$ порядка 18 в циклическую группу $\langle b\rangle$ порядка 6.

5. Построить абелеву аддитивную группу из 7 элементов.

6. Доказать, что поле $GF(p^n)$ содержит в себе в качестве подполя $GF(p^k)$ тогда и только тогда, когда k является делителем n.

7. Можно ли построить поле из а) 7, б) 8, в) 14 элементов?

8. Найти все неприводимые многочлены степени 2 над полем Z_5.

9. Построить поля $Z_3[x]/\langle f(x)\rangle$ и $Z_3[x]/\langle f_1(x)\rangle$, а затем указать изоморфное отображение этих полей, где $f(x) = 2x^2 + 2x + 1$, а $f_1(x) = 2x^2 + 2$.