МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П.КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

В.П.Калядин

Алгебраические структуры

Электронное учебное пособие

САМАРА

2011

Автор: КАЛЯДИН Владимир Петрович

Учебное пособие «Алгебраические структуры» знакомит с основами теории алгебраических структур, включая вопросы мировоззренческого характера (группы, кольца, поля, решетки), в объеме, необходимом для понимания современного уровня работ по теоретическому программированию, теории кодирования. Пособие призвано обучить студентов фундаментальным понятиям алгебраических структур; умению применять основные методы алгебраических структур в других разделах математики и ее приложений. Учебное пособие содержит основные определения и теоремы курса, приведены примеры групп, разобраны некоторые задачи.

Пособие предназначено для студентов направления 010400 «Прикладная математика и информатика».

Глава 1. ГРУППЫ.

§ 1. Алгебраические структуры.

Пусть дано некоторое множество X, тогда бинарной операцией, заданной на этом множестве, называется отображение $\tau : X \times X \to X$.

Бинарная операция называется коммутативной, если $\forall x, y \in X : \tau(x, y) = \tau(y, x)$.

Бинарная операция называется ассоциативной, если $\forall x, y, z \in X : \tau(\tau(x, y), z) = \tau(x, \tau(y, z))$.

Множество X с введенной бинарной операцией τ называется алгебраической структурой. Алгебраическая структура обозначается следующим образом: (X, τ).

Алгебраическая структура называется коммутативной (ассоциативной), если бинарная операция коммутативна (ассоциативна).

В дальнейшем считаем, что $\tau(x, y) = x * y$.

Пример.

Определить тип алгебраических структур:

1) $(N,\ x * y = x^y)$;
2) $(Z,\ x * y = x \cdot y)$;
3) $(N,\ x * y = НОД\ (x, y))$;
4) $(Z,\ x * y = x - y)$;
5) $(Z,\ x * y = x^2 + y^2)$;
6) $\left(R,\ x * y = x \cdot y^{\frac{x}{|x|}}\right)$.

Решение.

1) $(N,\ x * y = x^y)$ является некоммутативной и неассоциативной алгебраической структурой, так как $x * y = x^y,\ y * x = y^x \Rightarrow x * y \neq y * x$ и $(x * y) * z = x^y * z = (x^y)^z = x^{yz},\ x * (y * z) = x * y^z = x^{y^z} \Rightarrow (x * y) * z \neq x * (y * z)$;

2) $(Z,\ x * y = x \cdot y)$ – коммутативная и ассоциативная алгебраическая структура, так как $x * y = x \cdot y = y \cdot x = y * x$ и $(x * y) * z = (x \cdot y) * z = x \cdot y \cdot z = x * (y \cdot z) = x * (y * z)$.

Аналогичным образом, проверяя выполнение определений коммутативности и ассоциативности алгебраических структур, получим, что

$(N,\ x * y = НОД\ (x, y))$ – коммутативная, но неассоциативная алгебраическая структура.

$(Z,\ x * y = x - y)$ – некоммутативная и неассоциативная алгебраическая структура.

$(Z,\ x * y = x^2 + y^2)$ – коммутативная, неассоциативная алгебраическая структура.

$\left(R,\ x * y = x \cdot y^{\frac{x}{|x|}} \right)$ – некоммутативная и ассоциативная алгебраическая структура.

Элемент $e_l \in X$ называется единицей слева, если $\forall\, x \in X\ \ e_l * x = x$.

Элемент $e_r \in X$ называется единицей справа, если $\forall\, x \in X\ \ x * e_r = x$.

Элемент $e \in X$ называется единичным элементом, если $\forall\, x \in X\ \ e * x = x * e = x$, т.е. если он является левой и правой единицей одновременно.

Пример.

Пусть задано множество элементов вида $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$, где $x, y \in R$. Найти все единицы.

Решение.

1.

$$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{cases} ax + cy = x \\ bx + dy = y \end{cases} \Rightarrow \begin{cases} (a-1)x + cy = 0 \\ bx + (d-1)y = 0 \end{cases} \Rightarrow a = 1,\ b = 0,\ c = 0,\ d = 1 \Rightarrow e_r = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

.

2. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{cases} ax = x,\ ay = y \\ cx = 0,\ cy = 0 \end{cases} \Rightarrow a = 1,\ c = 0,\ b,\ d \in R \Rightarrow e_l = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$,

т.е. левых единиц в заданном множестве бесконечно много.

3. $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Множество X с ассоциативной бинарной операцией называется полугруппой. Таким образом, ассоциативная алгебраическая структура является полугруппой. Полугруппа с единицей называется моноидом.

Пример.

Доказать, что алгебраическая структура $(X,\ x * y = x)$ является полугруппой.

Доказательство.

$\forall x, y, z \in X\ \ (x * y) * z = x * z = x,\ x * (y * z) = x * y = x \ \Rightarrow\ (x * y) * z = x * (y * z)$, значит, согласно определению, рассматриваемая алгебраическая структура ассоциативна, следовательно, она является полугруппой.

Пример.

Доказать, что алгебраическая структура $(Z,\ x * y = x \cdot y + x + y)$ является моноидом.

Доказательство.

1) $\forall x, y, z \in X \quad (x * y) * z = (x \cdot y + x + y) * z = xyz + xz + yz + xy + x + y + z$ и $x * (y * z) = x * (y \cdot z + y + z) = xyz + xy + yz + xz = x + y + z \Rightarrow (x * y) * z = x * (y * z)$, значит, рассматриваемая алгебраическая структура является полугруппой.

2) Проверим, что $e = 0$.

$0 * x = 0 \cdot x + 0 + x = x = x \cdot 0 + x + 0 = x * 0$, следовательно, рассматриваемая полугруппа является полугруппой с единицей, а значит моноидом.

§ 2. Группы

Элемент a называется обратимым, если существует элемент a^{-1} такой, что $a * a^{-1} = a^{-1} * a = e$. Элемент a^{-1} называется обратным элементом к элементу a.

Моноид, у которого все элементы обратимы называется группой.

Однако чаще применяют другое определение.

Алгебраическая структура $(X, *)$ называется группой, если выполнены три аксиомы:

1. $\forall a, b \in X \quad a * (b * c) = (a * b) * c$ **– аксиома ассоциативности**

2. $\exists e \in X : \forall a \in X \quad a * e = e * a = a$ **– аксиома существования единицы**

3. $\forall a \in X \ \exists a^{-1} \in X : a * a^{-1} = a^{-1} * a = e$ **– аксиома существования элемента обратного данному.**

Группа, в которой выполнена аксиома $\forall a, b \in X \quad a * b = b * a$, называется абелевой группой.

Примеры.

1. Множество целых чисел с операцией сложения, т.е. $(Z, +)$ – абелева группа.

2. $(Q, +)$, $(R, +)$, $(C, +)$ – абелевы группы.

$(N, +)$ – не является группой, так как отсутствует единичный элемент.

3. $(R, \cdot)$ – не является группой, так как у элемента 0 нет обратного.

4. $(N^*, \cdot) = (N / \{0\}, \cdot)$ – не группа, так как не выполняется аксиома существования обратного элемента.

5. $(Z^*, \cdot)$ – не группа, так как не выполняется аксиома существования обратного

элемента.

6. $(Q^*,\cdot), (R^*,\cdot), (C^*,\cdot)$ являются абелевыми группами.

7. $(nZ,+)$, где n – фиксированное натуральное число, – абелева группа.

8. $(\{-1;1\},\cdot)$ – абелева группа.

9. Множество степеней фиксированного числа $a \neq 0$ с целыми показателями с заданной операцией умножения, т.е. $(a^n,\cdot)$ – абелева группа.

10. Множество всех комплексных корней n-ой степени из единицы и операция умножения, т.е. $(\sqrt[n]{1},\cdot)$ – группа.

11. Множество комплексных чисел с фиксированным модулем и операция умножения:

а) если модуль равен единице, то получим абелеву группу;

б) если модуль равен нулю, то абелева группа будет состоять из одного элемента 0;

в) если модуль не равен ни нулю, ни единице, то данное множество не является группой.

12. Множество всех комплексных корней целых степеней из единицы с заданной операцией умножения является абелевой группой.

13. Множество всех подмножеств данного множества и операция симметрическая разность – абелева группа.

14. Множество симметрических матриц и операция сложения матриц – абелева группа.

15. Множество кососимметрических матриц с введенной операцией сложения является абелевой группой.

16. Множество симметрических матриц с операцией умножения не является группой, так как не выполняется аксиома существования элемента обратного данному.

17. Множество невырожденных матриц и операция умножения – не абелева группа.

18. Множество матриц с фиксированным определителем и операция умножения: если определитель равен единице – получим не абелеву группу, иначе данное множество группой являться не будет.

19. Множество матриц вида $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, где $x, y \in R,\ x^2 + y^2 \neq 0$, и операция умножения – абелева группа.

20. $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ с операцией умножение

$i^2 = j^2 = k^2 = -1,\ ij = -jk = k,\ jk = -kj = i,\ ki = -ik = j$, является неабелевой группой и называется группой кватернионов.

21. $(Z_p, +)$, результатом операции $+$ является остаток от деления на p, является абелевой группой.

22. $(Z_p^*, \cdot)$, где p – простое число, а результатом операции $+$ является остаток от деления на p, является абелевой группой.

23. S_n – группа перестановок, операцией здесь является операция умножения перестановок.

Пример.

$S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$.

$S_4 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3), (1\ 4\ 3), (1\ 3\ 4), (1\ 2\ 3\ 4),$

$(1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

Если количество инверсий в перестановке четное, то перестановка называется *четной*, если нечетное – то *нечетной*.

24. A_n – группа четных перестановок.

Пример.

$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$.

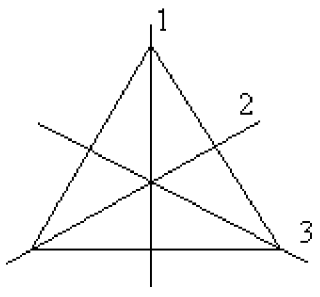
$A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (2\ 3\ 4), (2\ 4\ 3), (1\ 4\ 3), (1\ 3\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$.

25. $V_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ – группа Клейна, является абелевой группой.

26. D_n – группа Диэдра. Берется правильный n-угольник, рассматриваются все повороты и осевые симметрии, переводящие n-угольник в себя. Операция – композиция.

Группа D_n состоит из n поворотов и n осевых симметрий.

Пример.



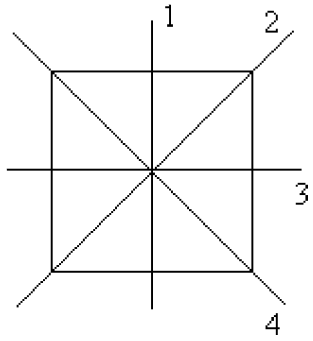
D_3:

Отображения 1, 2, 3 – осевые симметрии.

Отображение 4 – поворот на угол 0°.

Отображение 5 – поворот на угол 120° по часовой стрелке.

Отображение 6 – поворот на угол 240° по часовой стрелке.



D_4:

Отображения 1, 2, 3, 4 – осевые симметрии

Отображение 5 – поворот на угол 0^0 по часовой стрелке,

Отображение 6 – поворот на угол 90^0 по часовой стрелке,

Отображение 7 – поворот на угол 180^0 по часовой стрелке,

Отображение 8 – поворот на угол 270^0 по часовой стрелке.

$Card\ 1 = Card\ 2 = Card\ 3 = Card\ 4 = Card\ 7 = 2$,

$Card\ 6 = Card\ 8 = 4$ и $Card\ 5 = Card\ e = 1$.

Пусть G – группа, группа $H \subset G$, тогда говорят, что H является подгруппой группы G.

Пример.

1. У любой группы есть две простейшие подгруппы – это сама группа и группа, состоящая только из единичного элемента.

2. A_n – подгруппа группы S_n.

3. $(Q,+), (R,+)$ – подгруппы группы $(C,+)$.

4. Множество матриц с определителем равным нулю является подгруппой множества невырожденных матриц.

5. Множество всех поворотов является подгруппой группы Диэдра.

Подгруппа, не являющаяся всей группой и единичным элементом, называется собственной подгруппой.

Число элементов группы называется порядком группы.

Обозначение: $|G|$ или $card\ G$ или $(G:e)$.

Для фиксированного a минимальное натуральное число n такое, что $a^n = e$, называется порядком элемента ($Card\ a$). Если такое n не существует, то порядок элемента считают равным бесконечности.

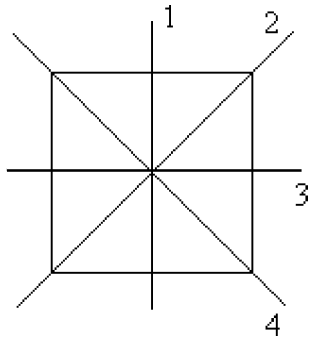
Пример.
Найти порядок группы S_3 и порядки всех ее элементов.

Группа S_3 содержит шесть элементов $\Rightarrow |S_3| = 6$.

Пусть $a = (1\ 2\ 3) \Rightarrow a^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2);\ a^3 = (1\ 3\ 2)(1\ 2\ 3) = e \Rightarrow Card\ (1\ 2\ 3) = 3$.

$Card\ (1\ 2) = Card\ (1\ 3) = Card\ (2\ 3) = 2,\ Card\ (1\ 3\ 2) = Card\ (1\ 2\ 3) = 3,\ Card\ e = 1$.

Пример.
Найти порядки всех элементов группы D_4.



Отображения 1, 2, 3, 4 – осевые симметрии.

Отображение 5 – поворот на угол 0^0 по часовой стрелке,

Отображение 6 – поворот на угол 90^0 по часовой стрелке,

Отображение 7 – поворот на угол 180^0 по часовой стрелке,

Отображение 8 – поворот на угол 270^0 по часовой стрелке.

$Card\ 1 = Card\ 2 = Card\ 3 = Card\ 4 = Card\ 7 = 2$,

$Card\ 6 = Card\ 8 = 4$ и $Card\ 5 = Card\ e = 1$.

Пример.
Найти порядки всех элементов группы $(Z_6, +)$.

$Z_6 = \{0,1,2,3,4,5\} \Rightarrow Card\ 0 = 1,\ Card\ 1 = Card\ 5 = 6,\ Card\ 2 = Card\ 4 = 3,\ Card\ 3 = 2$.

§ 3. Свойства групп

1. *В группе имеется ровно одна единица.*

Доказательство. Допустим, в группе существуют две единицы $e_1 \neq e_2$, значит $e_1 = e_1 * e_2 = e_2$ согласно второй аксиоме из определения группы, следовательно,

получено противоречие с предположением. Таким образом, в группе имеется только одна единица.

2. *У любого элемента группы существует ровно один обратный.*

Доказательство. Существование обратного элемента следует из определения группы. Единственность такого элемента докажем от противного. Пусть $\exists x_1^{-1} \neq x_2^{-1} \Rightarrow$ по определению обратного элемента $xx_1^{-1} = e = xx_2^{-1} \Rightarrow x_1^{-1}xx_1^{-1} = x_1^{-1}xx_2^{-1} \Rightarrow ex_1^{-1} = ex_2^{-1} \Rightarrow x_1^{-1} = x_2^{-1}$. Таким образом, получено противоречие с предположением, значит у любого элемента группы существует ровно один обратный.

3. *Если* $ax = ay \Rightarrow x = y$ *и* $xa = ya \Rightarrow x = y$.

Доказательство. $ax = ay \ (*a^{-1}) \Rightarrow a^{-1}ax = a^{-1}ay \Rightarrow ex = ey \Rightarrow x = y$,

$xa = ya \ (*a^{-1}) \Rightarrow xa^{-1}a = ya^{-1}a \Rightarrow xe = ye \Rightarrow x = y$.

4. $\forall x, y \in G$ *уравнение* $ax = b$ *имеет единственное решение вида* $x = a^{-1}b$.

Доказательство.

а) Пусть $x = a^{-1}b$ является решением заданного уравнения, тогда $aa^{-1}b = b \Rightarrow eb = b$, получено верное равенство, значит $x = a^{-1}b$ – решение $ax = b$;

б) Единственность решения докажем от противного. Предположим, что существует еще одно решение x^*, причем $x^* \neq x$, тогда $ax^* = b \ (*a^{-1}) \Rightarrow a^{-1}ax^* = a^{-1}b \Rightarrow ex^* = a^{-1}b \Rightarrow x^* = x$, получено противоречие с предположением, значит решение $x = a^{-1}b$ единственно.

Следствие. Зафиксируем элемент $a \in G$. Если каждый элемент группы G умножить на a слева, т.е. $g_1 \to ag_1$, $g_2 \to ag_2$ и т.д., следовательно, получена биекция – отображение группы на себя. Значит, если $g \in G$, то $ag \in G$.

5. Пусть $a \in G$, $m, n \notin Z \Rightarrow$ выполнены следующие формулы $\begin{matrix} a^m a^n = a^{m+n} \\ (a^m)^n = a^{mn} \end{matrix}$

Доказательство.

1) Докажем вспомогательное утверждение: $\forall m, n \in \square \quad \prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{n} a_{m+j} = \prod_{j=1}^{m+n} a_j$, т.е. произведение двух сложных произведений является сложным произведением всех участвующих сомножителей в прежнем порядке. Для $n = 1$ утверждение верно, так как $\prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{1} a_{m+j} = \prod_{j=1}^{m} a_j \cdot a_{m+1} = \prod_{j=1}^{m+1} a_j$, пусть оно выполняется для некоторого n, тогда

для $n+1$ получим: $\prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{n+1} a_{m+j} = \prod_{i=1}^{m} a_i \cdot \left(\prod_{j=1}^{n} a_{m+j} \cdot a_{m+n+1} \right) = \left(\prod_{i=1}^{m} a_i \cdot \prod_{j=1}^{n} a_{m+j} \right) \cdot a_{m+n+1} =$

$= \left(\prod_{i=1}^{m+n} a_i \right) \cdot a_{m+n+1} = \prod_{i=1}^{m+n+1} a_i$.

Так как $a^n = \prod_{i=1}^{n} a$, то $a^m a^n = a^{m+n}$.

2) Пусть $m < 0,\ n < 0$, тогда $m' = -m > 0,\ n' = -n > 0 \ \Rightarrow \ a^m a^n = \left(a^{-1}\right)^{m'} \left(a^{-1}\right)^{n'} =$

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

3) При $m' = -m > 0,\ n > 0$ имеем $a^m a^n = \left(a^{-1}\right)^{m'} a^n = \left(\underbrace{a^{-1} \ldots a^{-1}}_{m'} \right) \left(\underbrace{a \ldots a}_{n} \right) = a^{n-m'} = a^{m+n}$.

Аналогично рассматривается случай $m > 0,\ n < 0$, а также доказывается равенство $\left(a^m\right)^n = a^{mn}$.

§ 4. Изоморфизм групп

Пусть даны две группы $(G,*)$ и $(H,\circ)$. Эти группы называются *изоморфными*, если существует отображение $f : G \to H$ такое, что выполнены два условия:

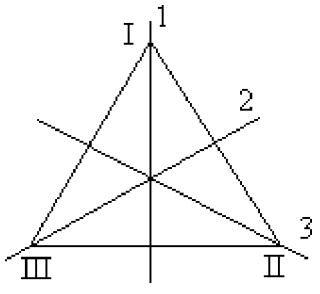
1. $\forall\ a,b \in G \quad f(a*b) = f(a) \circ f(b)$**, *2.*** f ***– биекция.***

Обозначение: $G \cong H$.

Пример.

Доказать, что $D_3 \cong S_3$.

Доказательство.



$4 - 0^\circ$,

$5 - 120^\circ$,

$6 - 240^\circ$.

$$\left.\begin{array}{lll} 1 \to (\text{II III}) & 3 \to (\text{I III}) & 5 \to (\text{I II III}) \\ 2 \to (\text{I II}) & 4 \to \text{e} & 6 \to (\text{I III II}) \end{array}\right\} \Rightarrow$$

получена группа $S_3 \Rightarrow D_3 \cong S_3$.

Свойства изоморфных групп:

1. *При изоморфизме единица переходит в единицу.*

Доказательство.

$f(a) = f(a * e_G) = f(a) \circ f(e_G) \circ \left(f\left(a^{-1}\right)\right) \Rightarrow f\left(a^{-1}\right) \circ f(a) = f\left(a^{-1}\right) \circ f(a) \circ f(e_G) \Rightarrow$
$e_H = f(e_G)$.

2. $\forall\ a \in G \quad f\left(a^{-1}\right) = (f(a))^{-1}$.

Доказательство. $e_H = f(e_G) = f\left(a * a^{-1}\right) = f(a) \circ f\left(a^{-1}\right) \Rightarrow$ согласно определению, элемент $(f(a))^{-1}$ является обратным к элементу $f\left(a^{-1}\right)$.

3. *Если* $G \cong H$, *то* $|G| = |H|$. Это свойство справедливо, так как отображение f является биекцией.

4. *При изоморфизме порядок элемента остается неизменным, т.е. если* $a \in G$ *и* $|a| = n$, *то* $|f(a)| = n$.

Доказательство.

Возьмем некоторое минимальное n такое, что $a^n = e_G \Rightarrow f\left(a^n\right) = f(e_G) = e_H$, значит по первому свойству $f\left(a^n\right) = (f(a))^n$.

Пусть существует $k < n$ такое, что $(f(a))^k = e_H \Rightarrow f\left(a^k\right) = e_H = f(e_G) \Rightarrow a^k = e_G \Rightarrow k = n$.

Таким образом, при изоморфизме порядок элементов сохраняется.

Теорема (Кэли).

Любая конечная группа порядка n *изоморфна некоторой подгруппе группы* S_n.

Доказательство.

Рассмотрим некоторую группу $G = \{e, a_1, a_2, ..., a_{n-1}\}$, а так же отображение вида $f_g : a_i \to g a_i$, где $g \in G$. Если $g = e$, то каждый элемент группы G переходит в себя. Если $g \neq e$, то согласно следствию из четвертого свойства групп отображение f_g будет ставить в соответствие элементу $g \in G$ некоторую перестановку элементов этой же группы, т.е группа G будет изоморфна группе перестановок. Известно, что $|S_n| = n!$, а по условию $[G[= n$, значит изоморфизма между G и S_n нет, следовательно группа G может быть изоморфна лишь некоторой подгруппе группы S_n.

§ 5. Циклические группы

Группа, образованная степенями одного фиксированного элемента, называется *циклической группой*, а этот элемент называется *образующим*.

Если $(G,*)$ – циклическая группа, то $G=\{a, a^2,\dots, a^n=e\}$, где a – образующий элемент.

Рассмотрим примеры циклических групп:

1) $(Z,+)$, образующими элементами являются 1 и –1.

2) $(\{-1;1\},\cdot)$, образующим элементом является элемент –1.

3) $(\sqrt[n]{1},\cdot)$, образующий элемент – корень из 1 с наименьшим ненулевым аргументом.

Пример.

Найти все циклические подгруппы группы S_3.

Решение.

а) $\{e\}$ – циклическая подгруппа;

б) $a=(1\ 2),\ a^2=e,\ a^3=a,\dots \Rightarrow \{e,(1\ 2)\}$ – циклическая подгруппа;

в) $\{e,(1\ 3)\}$, $\{e,(2\ 3)\}$ – циклические подгруппы;

г) $a=(1\ 2\ 3),\ a^2=(1\ 3\ 2),\ a^3=3,\dots \Rightarrow \{e,(1\ 2\ 3),(1\ 3\ 2)\}$ – циклическая подгруппа.

Свойства циклических групп:

1. *Циклические группы могут быть конечного или бесконечного порядков, причем порядок образующего элемента равен порядку группы.*

Доказательство.

Рассмотрим последовательность элементов $a, a^2, a^3,\dots, a^n,\dots, a^m,\dots$. Возможны следующие случаи:

а) Все степени элемента a различны, т.е. $n\neq m \Rightarrow a^n\neq a^m$, в этом случае группа, образованная данной последовательностью элементов будет иметь бесконечный порядок.

б) Пусть существуют совпадения $a^n=a^m$ при $n\neq m$. Если, например, $m>n$, то $a^{m-n}=e$, т.е. существуют положительные степени элемента $a\in G$, равные единичному элементу. Пусть q - наименьший положительный показатель, для которого $a^q=e$, тогда группа G будет состоять из q различных элементов, т.е. иметь конечный

порядок $|G| = q$.

2. *В циклической группе может быть несколько образующих элементов.*

Например, рассмотрим группу $(Z_5^*, \cdot)$, где $Z_5^* = Z_5 / \{0\} = \{1, 2, 3, 4\}$:

а) $2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1 = e \Rightarrow$ 2 – образующий элемент;

б) $3^1 = 3,\ 3^2 = 4,\ 3^3 = 2,\ 3^4 = 1 = e \Rightarrow$ 3 – образующий элемент;

в) $4^1 = 4,\ 4^2 = 1 = e,\ 4^3 = 4,\ 4^4 = 1 = e,... \Rightarrow$ 4 образующим элементом не является.

3. *Любая подгруппа циклической группы сама является циклической группой.*

Доказательство.

Рассмотрим произвольную циклическую группу $G = \{a, a^2, ..., a^n = e\}$, каждый ее элемент имеет вид a^k, где $k = \overline{1, n}$. Пусть H - ненулевая подгруппа группы G. Если $a^k \in H$ для некоторого $k \neq 0$, то и $a^{-k} \in H$. Среди всех элементов $a^k \in H$ с положительным k выберем элемент a^m, где m наименьшее. Записав любое $k > 0$ в виде $k = lm + r,\ 0 \leq r < m$, видим, что из $a^k \in H$ следует $a^r = a^k a^{-lm} \in H$, т.е. $r = 0$. Значит, H - циклическая группа.

4. *Любая циклическая группа является абелевой группой.*

Доказательство.

$a^k a^l = a^{k+l}$ по пятому свойству групп, аналогично получим, что $a^l a^k = a^{k+l}$, следовательно, по определению циклическая группа является абелевой.

5. *Все циклические группы одного порядка изоморфны.*

Доказательство.

1) Рассмотрим сначала группы конечного порядка, т.е. $|G| = |H| = n$, $G \subset \{a^k\}$, $H \subset \{b^k\}$. Организуем отображение вида $f : a^k \to b^k$, докажем, что оно является изоморфизмом, проверив два условия из определения:

а) $f(a^k * a^l) = f(a^{k+l}) = b^{k+l} = b^k \circ b^l = f(a^k) \circ f(a^l)$,

б) f – биективное отображение.

2) Теперь рассмотрим группы бесконечных порядков, т.е. $|G| = |H| = \infty$, $G \subset \{a^k\}$. Докажем, что любая группа $(G, *)$ изоморфна группе $(Z, +)$, тем самым получим, что все группы бесконечных порядков изоморфны между собой. Для этого проверим два условия из определения изоморфизма:

а) $f(a^k * a^l) = f(a^{k+l}) = k + l == f(a^k) \circ f(a^l)$

б) f – биективное отображение.

§ 6. Автоморфизмы групп

Отображение $f : G \to G$ группы в себя называется *автоморфизмом*.

Множество всех автоморфизмов называется *группой автоморфизмов* $(\mathrm{Aut}\ G)$.

Операцией в группе $\mathrm{Aut}\ G$ является *композиция*, так как элементы этой группы – отображения.

Теорема.

$\mathrm{Aut}\, G$ *является группой.*

Доказательство:

Проверим три аксиомы из определения группы:

1) Среди композиции трех отображений не имеет значения, как расставлять скобки, значит, аксиома ассоциативности выполняется.

2) Аксиома существования единичного элемента также верна: e – тождественное преобразование.

3) Согласно третьей аксиоме из определения группы, у каждого элемента группы должен существовать обратный элемент, т.е. у каждого отображения из $\mathrm{Aut}\ G$ должно существовать обратное. Отображение f является биекцией по определению, значит, для него существует обратное отображение.

Таким образом, согласно определению $\mathrm{Aut}\ G$ является группой.

Пример.

Определить, является ли $Aut\ Z_9$ циклической группой. Найти $|Aut\ Z_9|$.

Решение.

$Z_9 = \{0,1,2,3,4,5,6,7,8\}$. Найдем порядки элементов группы Z_9:

$|0| = |e| = 1,\ \ |1| = 9,\ \ |2| = 9,\ \ |3| = 3,\ \ |4| = 9,\ \ |5| = 9,\ \ |6| = 3,\ \ |7| = 9,\ \ |8| = 9 \Rightarrow$ группа Z_9 является циклической, причем у нее существует шесть образующих элементов: 1, 2, 4, 5, 7, 8. Рассмотрим отображение $f : Z_9 \to Z_9$, следовательно, по четвертому свойству изоморфных групп образующие элементы при отображении должны перейти в образующие элементы, в результате получим:

f_1	f_2	f_3	f_4	f_5	f_6
$0 \to 0$	$0 \to 0$	$0 \to 0$	$0 \to 0$	$0 \to 0$	$0 \to 0$
$1 \to 1$	$1 \to 2$	$1 \to 4$	$1 \to 5$	$1 \to 7$	$1 \to 8$
$2 \to 2$	$2 \to 4$	$2 \to 8$	$2 \to 1$	$2 \to 5$	$2 \to 7$
$3 \to 3$	$3 \to 6$	$3 \to 3$	$3 \to 6$	$3 \to 3$	$3 \to 6$
$4 \to 4$	$4 \to 8$	$4 \to 7$	$4 \to 2$	$4 \to 1$	$4 \to 5$
$5 \to 5$	$5 \to 1$	$5 \to 2$	$5 \to 7$	$5 \to 8$	$5 \to 4$
$6 \to 6$	$6 \to 3$	$6 \to 6$	$6 \to 3$	$6 \to 6$	$6 \to 3$
$7 \to 7$	$7 \to 5$	$7 \to 1$	$7 \to 8$	$7 \to 4$	$7 \to 2$
$8 \to 8$	$8 \to 7$	$8 \to 5$	$8 \to 4$	$8 \to 2$	$8 \to 1$

Таким образом, $\mathrm{Aut}\, Z_9 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, $|\mathrm{Aut}\, Z_9| = 6$.

Проверим, является ли $\mathrm{Aut}\, Z_9$ циклической группой:

$f_1^2 = f_1 \Rightarrow Card\ f_1 = 1$.

$f_2^2 = f_3,\ f_2^3 = f_6,\ f_2^4 = f_3,\ f_2^5 = f_4,\ f_2^6 = f_1 \Rightarrow Card\ f_2 = 6 \Rightarrow$ элемент f_2 является образующим элементом, значит группа $Aut\ Z_9$ – циклическая.

Группой *внутренних автоморфизмов* группы G называются множество автоморфизмов вида: $\mathrm{Inn}\ G = \{L_a : g \to aga^{-1}\}$.

Свойства групп внутренних автоморфизмов:

1. $\mathrm{Inn}\ G \subset \mathrm{Aut}\ G$.

2. *Если группа G абелева, тогда группа внутренних автоморфизмов состоит из одного элемента, являющегося тождественным, т.е.* $\mathrm{Inn}\, G = \{ g \to g \}$.

§ 7. Гомоморфизмы групп

Группа $(G, *)$ *гомоморфно отображается* в группу $(H, \circ)$, если существует отображение $f : G \to H$ такое, что выполнено условие $f(a * b) = f(a) \circ f(b)$.

Множество $\ker f = \{a : f(a) = e\}$ **называется *ядром гомоморфизма*.**

$\ker f = e$ тогда и только тогда, когда гомоморфное отображение f является изоморфным, это утверждение основано на свойствах изоморфных групп.

Пример.

Определить какие из отображений $f: C/\{0\} \to C/\{0\}$ являются гомоморфными:

1) $f(z)=|z|$; 2) $f(z)=2|z|$; 3) $f(z)=1+|z|$; 4) $f(z)=1$.

Решение.

1) $f(z_1 \cdot z_2)=|z_1 \cdot z_2|=|z_1|\cdot|z_2|=f(z_1)\cdot f(z_2)$, следовательно, согласно определению отображение f является гомоморфизмом.

2) $f(z_1 \cdot z_2)=2|z_1 \cdot z_2|=2|z_1|\cdot|z_2|$ и $f(z_1)\cdot f(z_2)=2|z_1|\cdot 2|z_2|$, значит $f(z_1 \cdot z_2)\neq f(z_1)\cdot f(z_2)$, т.е. отображение f не является гомоморфным.

3) $f(z_1 \cdot z_2)=1+|z_1 \cdot z_2|=1+|z_1|\cdot|z_2|$ и $f(z_1)\cdot f(z_2)=(1+|z_1|)\cdot(1+|z_2|)$, следовательно, $f(z_1 \cdot z_2)\neq f(z_1)\cdot f(z_2)$, значит f – не гомоморфизм.

4) $f(z_1 \cdot z_2)=1=1\cdot 1=f(z_1)\cdot f(z_2)$, значит, f является гомоморфизмом.

Теорема.

Ядро гомоморфизма является подгруппой.

Доказательство.

Для доказательства данной теоремы необходимо проверить замкнутость ядра гомоморфизма относительно операции $*$ и выполнение трех аксиом из определения группы:

1) так как все элементы, принадлежащие ядру гомоморфизма, принадлежат также и группе G, то для них выполняется свойство ассоциативности из определения группы;

2) по первому свойству изоморфных групп $f(e_G)=e_H$, значит согласно определению ядра гомоморфизма $e_G \in \ker f$;

3) если $a \in \ker f$, то $e_H=f(e_G)=f\left(a*a^{-1}\right)=f(a)\circ f\left(a^{-1}\right)=e_H \circ f\left(a^{-1}\right)=f\left(a^{-1}\right)$, значит $a^{-1} \in \ker f$;

4) пусть $a_1, a_2 \in \ker f$, тогда $a_1 * a_2 \in \ker f$, так как $f(a_1 * a_2)=f(a_1)\circ f(a_2)=e_H$.

Пусть $\ker f = H$, тогда $\forall g \in G \quad f\left(g*H*g^{-1}\right)=f(g)\circ f(H)\circ f\left(g^{-1}\right)=$

$=f(g)\circ e\circ f\left(g^{-1}\right)=f(g)\circ f\left(g^{-1}\right)=e \Rightarrow gHg^{-1}=H$. Подгруппа H, для которой выполнено данное свойство, называется *нормальной подгруппой* группы G $(H \lhd G)$.

§ 8. Смежные классы

Пусть задан гомоморфизм $G \to H$, ядром этого гомоморфизма является множество $\ker f$, рассмотрим множество $a \ker f = \{ab,\ b \in \ker f\}$, для него выполняются следующие свойства:

1. *все элементы этого множества отображаются в* $f(a)$, *так как* $f(a \ker f) = f(a) \circ f(\ker f) = f(a) \circ e = f(a)$;

2. если $f(c) = f(a)$, следовательно, $f(a^{-1}c) = f(a^{-1}) f(c) = e_H \Rightarrow a^{-1}c = b \in \ker f$ и $c = ab \in a \ker f \Rightarrow c \in a \ker f$. Этот факт указывает на целесообразность разбиения группы G на подмножества вида $a \ker f$.

Пусть G – группа, H – ее подгруппа, тогда множество $gH = \{gh,\ h \in H\},\ g \in G,$ называется *левым смежным классом* группы G по подгруппе H $(\{G/H\}_l)$, а множество $Hg = \{hg,\ h \in H\},\ g \in G,$ *– правым смежным классом* $(\{G/H\}_r)$.

Пример.

Пусть $G = S_3 = \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$, $H = \{e, (1\ 2)\}$. Найти все левые и правые смежные классы группы G по подгруппе H.

Решение.

Найдем все левые смежные классы: $eH = \{e, (1\ 2)\} = H$.

$(1\ 2)H = \{(1\ 2), (1\ 2)(1\ 2)\} = \{(1\ 2), e\} = H$.

$(1\ 3)H = \{(1\ 3), (1\ 3)(1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$. $(2\ 3)H = \{(2\ 3), (2\ 3)(1\ 2)\} = \{(2\ 3), (1\ 3\ 2)\}$.

$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\}$.

$(1\ 3\ 2)H = \{(1\ 3\ 2), (1\ 3\ 2)(1\ 2)\} = \{(1\ 3\ 2), (2\ 3)\}$.

$S_3 = H \cup \{(1\ 3), (1\ 2\ 3)\} \cup \{(2\ 3), (1\ 3\ 2)\}$.

Найдем все правые смежные классы: $He = \{e, (1\ 2)\} = H$;

$H(1\ 2) = \{(1\ 2), (1\ 2)(1\ 2)\} = \{(1\ 2), e\} = H$;

$H(1\ 3) = \{(1\ 3), (1\ 2)(1\ 3)\} = \{(1\ 3), (1\ 3\ 2)\}$; $H(2\ 3) = \{(2\ 3), (1\ 2)(2\ 3)\} = \{(2\ 3), (1\ 2\ 3)\}$;

$H(1\ 2\ 3) = \{(1\ 2\ 3), (1\ 2)(1\ 2\ 3)\} = \{(1\ 2\ 3), (2\ 3)\}$;

$H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 2)(1\ 3\ 2)\} = \{(1\ 3\ 2), (1\ 3)\}$;

$S_3 = H \cup \{(1\ 3), (1\ 3\ 2)\} \cup \{(2\ 3), (1\ 2\ 3)\}$.

Пример.

Смежные классы группы C по подгруппе R – прямые, параллельные вещественной

оси.

Пример.

Смежные классы группы C^* по подгруппе R_+ – лучи, исходящие из начала координат.

Пример.

Смежные классы группы C^* по подгруппе $\{z \in C^* : |z| = 1\}$ – окружности с центром в начале координат.

Свойства смежных классов:

1. *Левый и правый смежные классы, вообще говоря, не совпадают.*

2. *Если* G *– абелева группа, то левый и правый смежные классы совпадают, это утверждение вытекает из определения абелевой группы.*

3. *Среди всех левых (правых) смежных классов имеется ровно одна подгруппа, так как в любой подгруппе существует единица, а такой класс один.*

4. *Левые (правые) смежные классы либо не пересекаются, либо совпадают.*

Доказательство.

Предположим, что $g_1H \cap g_2H \neq \varnothing$, тогда $g_1h_1 = g_2h_2,\ h_1, h_2 \in H$, следовательно,

$g_1 = g_2h_2h_1^{-1} \Rightarrow g_1b = g_2h_2h_1^{-1}b,\ b \in H \Rightarrow h_2h_1^{-1}b \in H \Rightarrow g_2h_2h_1^{-1}b \in g_2H \Rightarrow g_1H \subset g_2H$.

Аналогичным образом доказывается обратное включение $g_2H \subset g_1H$.

Получено противоречие, значит, $g_1H = g_2H$.

Доказательство для правых смежных классов проводится аналогичным образом.

5. *Группа* G *является объединением левых (правых) смежных классов*, т.е. $G = \bigcup_i g_iH$

$\left(G = \bigcup_i H\, g_i\right)$, так как подгруппа H обязательно имеет единичный элемент, значит

$\forall g \in G \quad g \in gH$.

6. *Между правым и левым смежными классами имеется взаимнооднозначное соответствие*, так как количество левых и правых смежных классов одинаковое.

7. *Разбиение на множество левых (правых) смежных классов порождает отношение эквивалентности:* $a \sim b \Leftrightarrow a^{-1}b \in H$.

Доказательство.

Убедимся в рефлективности, симметричности и транзитивности представленного отношения:

1) $a \sim a$, так как $a^{-1}a = e \in H$;

2) $a \sim b \Leftrightarrow a^{-1}b = h \in H \Leftrightarrow b^{-1}a = h^{-1} \in H \Leftrightarrow b \sim a$;

3) $a \square b, b \square c \Rightarrow b^{-1}a = h_1, c^{-1}b = h_2 \Rightarrow c^{-1}a = c^{-1}bh_1 = h_2h_1 \in H \Rightarrow a \square c$.

Количество левых (правых) смежных классов *называется индексом группы* G по подгруппе H. Обозначение: $(G : H)$. Очевидно, что $(G : e) = |G|$.

Теорема (Лагранж).

Порядок группы делится на порядок ее подгруппы.

Доказательство.

Рассмотрим левые смежные классы группы G по подгруппе H: $\{G / H\}_l$. В каждом из этих классов ровно столько элементов, сколь в подгруппе H. Следовательно, $(G : e) = (G : H) \cdot (H : e) \Rightarrow |G| = (G : H) \cdot |H|$. Так как каждое из чисел $|G|$, $(G : H)$, $|H|$ является натуральным, значит, порядок группы делится на порядок любой ее подгруппы.

Следствия:

1. *Порядок любого элемента группы делит порядок этой группы.*

Доказательство.

Пусть g - это произвольный элемент, принадлежащий группе H. Рассмотрим циклическую группу, порожденную данным элементом: $\langle g \rangle = \{g, g^2, \ldots, g^k = e\}$. По теореме Лагранжа порядок группы G делится на порядок подгруппы $\langle g \rangle$, т.е. на k, где k является еще и порядком элемента g.

2. *Любая группа порядка p, где p - простое число, является циклической.*

Доказательство.

Согласно первому следствию из теоремы Лагранжа порядок любого элемента группы должен делить p, значит, элементы могут иметь либо порядок 1, либо p. Порядок 1 имеет лишь единичный элемент, т.е. e. Следовательно, существует элемент порядка p. Таким образом, по первому свойству циклических групп рассматриваемая группа

является циклической.

Подгруппа H группы G называется *нормальной*, если левые и правые смежные классы группы G по подгруппе H одинаковы.

§ 9. Факторгруппы

Пусть дана группа S_3 и ее подгруппа $H = \{e, (1\ 2)\}$. Найдем произведение левых смежных классов $eH = H$ и $(1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}$: $eH \cdot (1\ 3)H = \{e, (1\ 2)\} \cdot \{(1\ 3), (1\ 2\ 3)\} = \{(1\ 3), (1\ 2\ 3), (1\ 3\ 2), (2\ 3)\}$ $\Rightarrow$ произведение левых смежных классов не является левым смежным классом.

Пусть H - некоторая нормальная подгруппа группы G, проверим выполнение утверждения: $a \sim b,\ c \sim d \Rightarrow ac \sim bd$. Действительно, по определению эквивалентности и седьмому свойству смежных классов: если $a \sim b \Rightarrow a^{-1}b = h_1 \in H$ и если $c \sim d \Rightarrow c^{-1}d = h_2 \in H$. Значит, $(ac)^{-1}bd = c^{-1}a^{-1}bd = c^{-1}\left(a^{-1}b\right)d = c^{-1}h_1 d = c^{-1}h_1 cc^{-1}d =$

$= c^{-1}h_1 c\left(c^{-1}d\right) = \underbrace{c^{-1}h_1 c}_{\in H} h_2 = h'h_2 \in H \Rightarrow ac \sim bd$. Фактически это означает, что операцию умножения на смежных классах можно ввести следующим образом: $aH \cdot bH = (ab)H$.

Рассмотрим смежные классы группы G по нормальной подгруппе H и заданную операцию умножения и докажем, что это группа, для этого проверим выполнение трех аксиом из определения группы:

1) $aH \cdot (bH \cdot cH) = aH \cdot (bc)H = (abc)H = (ab)H \cdot cH = (aH \cdot bH) \cdot cH$;

2) Существует единичный элемент $eH = H$: $aH \cdot eH = (ae)H = aH$ и $eH \cdot aH = (ea)H = aH$;

3) $aH \cdot a^{-1}H = (aa^{-1})H = eH = H$, следовательно, у каждого элемента группы существует обратный элемент.

Пример.

$Z/nZ \cong Z_n$.

Пример.

$C/R \cong R$.

Факторгруппа **группы** G **по нормальной подгруппе** H **– это множество смежных классов** $\{G/H\}$ **с операцией умножения, введенной следующим образом:** $aH \cdot bH = (ab)H$ **.**

§ 10. Действия групп на множествах

Пусть даны группа G **, множество** Ω **и** $S(\Omega)$ **– группа всех взаимно однозначных отображений множества** Ω **на себя. Гомоморфизм** $\Phi: G \to S(\Omega)$ **элементу** $g \in G$ **ставит в соответствие некоторое преобразование** Φ_g **из** $S(\Omega)$ **(причем образ** $\Phi_g(x)$ **точки** $x \in \Omega$ **относительно преобразования** Φ_g **часто обозначается символом** gx**) и задает** ***действие (слева) группы*** G ***на множестве*** Ω **, если выполняются две аксиомы:**

1) $ex = x$ **, где** e **– единица группы** G **,** $x \in \Omega$ **;**

2) $f(g(x)) = (fg)x$ **, где** $f \in G, g \in G, x \in \Omega$ **.**

Можно дать другое определение *действия группы* G *на множестве* Ω, например, как отображение декартова произведения $G \times \Omega \to \Omega$, причем также с выполнением указанных аксиом.

Две точки (два элемента) $x, x' \in \Omega$ *эквивалентны относительно действия группы* G *на* Ω, если $\exists g \in G: gx = x'$. Указанное отношение является отношением эквивалентности $a \sim b$, так как выполняются три необходимых свойства:

1. $a \sim a$ *(рефлексивность);*

2. $a \sim b \Rightarrow b \sim a$ *(симметричность);*

3. $a \sim b, b \sim c \Rightarrow a \sim c$ *(транзитивность).*

Их выполнение легко показать, исходя из определения действия группы на множестве. Свойство рефлексивности: $\forall x \in \Omega: ex = x \Rightarrow x \sim x$; свойство симметричности: $\exists g \in G: gx = x' \Rightarrow \exists g^{-1}: g^{-1}x' = x \Rightarrow x' \sim x$; свойство транзитивности: $\exists g_1: g_1 x = x'; \exists g_2: g_2 x' = x'' \Rightarrow x = g_1^{-1}x', x' = g_2^{-1}x'' \Rightarrow \exists g_1^{-1}g_2^{-1}: x = \left(g_1^{-1}g_2^{-1}\right)x'' \Rightarrow x \sim x''$.

Полученное отношение эквивалентности разбивает множество Ω на непересекающиеся классы эквивалентности. Каждый такой класс эквивалентности

называется *орбитой*. Если орбита содержит элемент $x \in \Omega$, то ее можно обозначить символом $G(x)$.

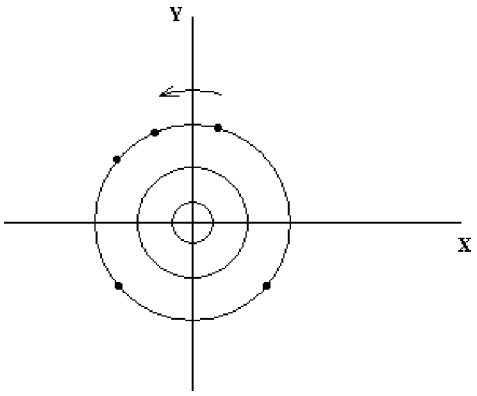
Пример 1.
Найти все орбиты.

1) G – группа вращений вокруг начала координат, Ω – плоскость $\mathbb{R}^2$.

2) G – группа невырожденных линейных операторов, Ω – n-мерное евклидово пространство.

3) G – группа ортогональных операторов; Ω – n-мерное евклидово пространство.

4) G – циклическая подгруппа группы S_{10}, образованная элементом $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 9 & 4 & 10 & 6 & 2 & 1 & 7 \end{pmatrix}$ и всеми его натуральными степенями: $G = \{g, g^2, \ldots\}$; $\Omega = \{1,2,3,4,5,6,7,8,9,10\}$.



Решение.
1) Одна из орбит – окружность с центром в начале координат (так как любую точку x', принадлежащую ей можно получить вращением некоторой другой точки x, то есть действием элемента $g \in G$ на $x \in \Omega$). В данном случае орбит бесконечно много, и все они – непересекающиеся окружности с центрами в начале координат (см. рисунок).

2) Орбиты всего две. Первая образована нулевым вектором (у нулевого вектора не существует ни одного эквивалентного элемента относительно действия G на Ω), вторая – все пространство без нулевого вектора.

3) Так как ортогональный оператор не меняет длины вектора, то каждая орбита образована множеством векторов одинаковой длины. В данном случае орбит бесконечно много.

4) Чтобы найти все орбиты удобнее элемент g представить в циклическом виде: $g = (1\ \ 5\ \ 4\ \ 9)(2\ \ 8)(6\ \ 10\ \ 7)$. Можно заметить, что элемент g определяет четыре орбиты: $G(1) = \{1,4,5,9\}, G(2) = \{2,8\}, G(3) = \{3\}, G(6) = \{6,7,10\}$, где $G(1), G(2), G(3), G(6)$ – орбиты, содержащие элементы $1,2,3,6$ соответственно. Остальные элементы

группы G не будут определять новых орбит, и полученные четыре орбиты не перейдут в одну большую, так как при возведении элемента g в любую степень элементы $1,2,3,6$ никогда не войдут в один цикл (это видно из циклического представления элемента), а, значит, и в одну орбиту.

Количество элементов в орбите называют *длиной орбиты*, и обозначается $CardG(x)$**.**

Множество вида: $St(x) = \{g \in G \mid gx = x\}$ **называют *стабилизатором*.**

Теорема 1.

Стабилизатор – подгруппа группы G .

Доказательство.

Множество $St(x)$ является подгруппой, так как выполняются необходимые условия:

1) $e \in St(x)$ по первой аксиоме действия групп на множестве($ex = x \ \forall x \in \Omega$);

2) Если $g_1, g_2 \in St(x)$, то элемент $(g_1 g_2)$ тоже принадлежит $St(x)$ (в самом деле: $(g_1 g_2)x = g_1(g_2 x)$ по второй аксиоме действия групп на множестве, тогда $g_1(g_2 x) = g_1 x = x \Rightarrow (g_1 g_2) \in St(x)$);

3) Если $g \in St(x)$, то и $g^{-1} \in St(x)$ (так как $e \in St(x)$, тогда можно записать следующую цепочку: $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x \Rightarrow g^{-1} \in St(x)$). Теорема доказана.

Стабилизатор часто называют *стационарной подгруппой*.

Две подгруппы H, H_1 группы G называются *сопряженными*, если $H_1 = gHg^{-1}$ для некоторого $g \in G$.

Пример 2.

G – подгруппа группы S_{10}, образованная элементом $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 9 & 4 & 10 & 6 & 2 & 1 & 7 \end{pmatrix}$ и всеми его натуральными степенями: $G = \{g, g^2, \ldots\}$; $\Omega = \{1,2,3,4,5,6,7,8,9,10\}$. Найти стабилизатор каждого элемента $x \in \Omega$.

Решение.

Элемент g удобнее записать так: $g = (1 \ 5 \ 4 \ 9)(2 \ 8)(6 \ 10 \ 7)$. Остальные

элементы группы G имеют вид: $g^2 = (1\ \ 4)(5\ \ 9)(6\ \ 7\ \ 10)$, $g^3 = (1\ \ 9\ \ 4\ \ 5)(2\ \ 8)$, $g^4 = (6\ \ 10\ \ 7)$, $g^5 = (1\ \ 5\ \ 4\ \ 9)(2\ \ 8)(6\ \ 7\ \ 10)$, $g^6 = (1\ \ 4)(5\ \ 9)$, $g^7 = (1\ \ 9\ \ 4\ \ 5)(2\ \ 8)(6\ \ 10\ \ 7)$, $g^8 = (6\ \ 7\ \ 10)$, $g^9 = (1\ \ 5\ \ 4\ \ 9)(2\ \ 8)$, $g^{10} = (1\ \ 4)(5\ \ 9)(6\ \ 10\ \ 7)$, $g^{11} = (1\ \ 9\ \ 4\ \ 5)(2\ \ 8)(6\ \ 7\ \ 10)$, $g^{12} = e$. Из полученных данных легко найти стабилизатор каждого элемента: $St(1) = St(4) = St(5) = St(9) = \{g^4, g^8, g^{12}\}$, $St(2) = St(8) = \{g^2, g^4, g^6, g^8, g^{10}, g^{12}\}$, $St(3) = G$, $St(6) = St(7) = St(10) = \{g^3, g^6, g^9, g^{12}\}$.

Стабилизаторы обладают такими свойствами:

1. *Порядок стабилизатора делит порядок группы* G.

Доказательство. По теореме 1 стабилизатор – подгруппа группы G, значит, по теореме Лагранжа его порядок делит порядок группы G.

2. Пусть x_0 – некоторая фиксированная точка в Ω, элемент $g \in St(x_0)$. Тогда *левые смежные классы вида* $gSt(x_0)$ *по подгруппе* $St(x_0)$ *находятся во взаимнооднозначном соответствии с элементами орбиты* $G(x_0)$.

Доказательство. Рассмотрим некоторый элемент $h \in St(x_0)$, тогда $gx_0 = hx_0$. Умножим равенство на g^{-1}: $g^{-1}hx_0 = x_0$, получим, что $g^{-1}h \in St(x_0) \Rightarrow h \in gSt(x_0)$, тогда $gSt(x_0)$ – левый смежный класс группы G по стабилизатору $St(x_0)$. Получено, что левые смежные классы $gSt(x_0)$ группы G по подгруппе $St(x_0)$ находятся во взаимнооднозначном соответствии с элементами орбиты $G(x_0)$.

3. *Длина орбиты делит порядок группы* G.

Доказательство. Число элементов орбиты совпадает с порядком левых классов, следовательно, по теореме Лагранжа длина орбиты делит порядок группы, ч. т. д.

4. *Пусть группа* G *действует на множестве* Ω. *Если две точки* $x_0, x_1 \in \Omega$ *лежат на одной орбите, то их стабилизаторы сопряжены.*

Доказательство. Так как точки, то лежат на одной орбите, то $x_1 = gx_0$. По определению стабилизатора: $St(x_1)x_1 = x_1 \Rightarrow St(x_1)x_1 = gx_0$, тогда $g^{-1}St(x_1)x_1 = x_0$. Полученное равенство преобразуем следующим образом: $g^{-1}St(x_1)gx_0 = x_0$

следовательно $g^{-1}St(x_1)g \subset St(x_0)$. Рассмотрим аналогичное действие для $x_0 = g^{-1}x_1$:

$St(x_0)x_0 = x_0 \Rightarrow$

$St(x_0)x_0 = g^{-1}x_1 \Rightarrow St(x_0)g^{-1}x_1 = g^{-1}x_1 \Rightarrow gSt(x_0)g^{-1}x_1 = x_1 \Rightarrow gSt(x_0)g^{-1} \subset St(x_1)$.

Полученное включение умножим слева на g^{-1}, а справа на g: $St(x_0) \subset g^{-1}St(x_1)g$. С одной стороны $St(x_0) \subset g^{-1}St(x_1)g$, с другой $g^{-1}St(x_1)g \subset St(x_0)$. Значит, имеет место равенство $g^{-1}St(x_1)g = St(x_0) \Rightarrow St(x_1) = gSt(x_0)g^{-1} \Rightarrow$ по определению стабилизаторы являются сопряженными подгруппами, ч. т. д.

На $\Omega = G$ действие любого элемента $g \in G$ можно определить посредством формулы: $gx = gxg^{-1} \; \forall x \in G$. Такое действие группы на множестве называется *действие сопряжением*. **Множество элементов, не меняющихся при сопряжении (значит, являющееся ядром данного преобразования), называется *центром группы* и обозначается $Z(G)$, то есть $Z(G) = \{x \in G \mid \forall g \in G \Rightarrow x = gxg^{-1}\}$. Можно заметить, что элементы центра являются перестановочными со всеми элементами группы:** $x = gxg^{-1} \Rightarrow xg = gx$.

Множество элементов $\{gxg^{-1}, g \in G\}$образуют *класс сопряженных элементов* с элементом $x \in H$. Если подгруппа H нормальна, то если элемент $x \in H$, то весь класс сопряженных элементов будет принадлежать этой подгруппе.

Пример 3.
Найти центр группы S_3.

Решение.
$S_3 = \{e, (1\ 3), (1\ 2), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Проверим, какие элементы являются перестановочными: $(1\ 2)(1\ 3) = (1\ 2\ 3) \neq (1\ 3)(1\ 2) = (1\ 3\ 2)$,

$(1\ 2\ 3)(2\ 3) = (1\ 3) \neq (2\ 3)(1\ 2\ 3) = (1\ 2)$,

$(1\ 3\ 2)(2\ 3) = (1\ 2) \neq (1\ 3) = (2\ 3)(1\ 3\ 2)$. Значит, элементы $(1\ 3), (1\ 2), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)$ не принадлежат центру $\Rightarrow Z(S_3) = \{e\}$.

Теорема.

Центр группы G является нормальной подгруппой.

Доказательство.

Множество $Z(G)$ является подгруппой, так как выполняются необходимые условия:

1) $e \in Z(G)$, так как $geg^{-1} = e \ \forall g \in G$.

2) Если $x_1, x_2 \in Z(G)$, то элемент $x_1 x_2$ тоже принадлежит $Z(G)$. В самом деле: $gx_1g^{-1} = x_1,\ gx_2g^{-1} = x_2 \ \forall g \in G \Rightarrow \forall g \in G \ x_1x_2 = gx_1g^{-1}gx_2g^{-1} = gx_1x_2g^{-1} \Rightarrow x_1x_2 \in Z(G)$.

3) Если $x \in Z(G)$, то и $x^{-1} \in Z(G)$, что видно из такой цепочки: $e \in Z(G) \Rightarrow$ $geg^{-1} = e \ \forall g \in G \Rightarrow e = gxx^{-1}g^{-1} = gxex^{-1}g^{-1} = \underbrace{gxg^{-1}}_{x} gx^{-1}g^{-1} = xgx^{-1}g^{-1} \Rightarrow gx^{-1}g^{-1} = x^{-1} \Rightarrow$

$x^{-1} \in Z(G)$.

Так как центр – подгруппа, построенная следующим образом: $Z(G) = \{x \in G \mid \forall g \in G \Rightarrow x = gxg^{-1}\}$, то из определения нормальной подгруппы следует, что центр – нормальная подгруппа. Теорема доказана.

Замечание. Чем больше центр, то есть чем больше элементов являются перестановочными, и тем больше группа похожа на абелеву.

§ 11. Разрешимые группы

Выражение $[a,b] = aba^{-1}b^{-1}$ называется *коммутатором элементов* a,b группы G.

Коммутатор имеет следующие свойства:

1. *Коммутатор служит корректирующим членом, необходимым для того, чтобы поменять местами элементы.* Это можно заметить, домножив его определение слева на ba: $ab = [a,b]ba$. Значит, если $[a,b] = e$, то элементы a,b перестановочны.

2. *Группа G является абелевой, когда $\forall a,b \in G$ выполняется равенство $[a,b] = e$.*

3. *Элемент, обратный коммутатору – коммутатор.* В самом деле: $[a,b]^{-1} = \left(aba^{-1}b^{-1}\right)^{-1} = bab^{-1}a^{-1} = [b,a]$.

4. *Произведение двух коммутаторов не всегда является коммутатором.*

Коммутантом **группы G называют подгруппу G', образованную множеством коммутаторов и всех их произведений.** Обозначение: G'.

Теорема.

G' – подгруппа G .

1) $e \in G'$ (так как коммутатор $[x,x] = e \quad x \in G$).

2) Если $x_1, x_2 \in G'$, то элемент $x_1 x_2$ тоже принадлежит G', так как коммутант включает в себя множество произведений коммутаторов.

3) Если $x \in G'$, то и $x^{-1} \in G'$ (пусть коммутатор $x = [a,b] \Rightarrow \; x^{-1} = [a,b]^{-1} \Rightarrow \; x^{-1} \in G'$).

Пример 1.
Найти коммутант группы: 1) S_3; 2) S_n.

Решение.

1) Группа $S_3 = \{e, (1\ \ 3), (1\ \ 2), (2\ \ 3), (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$. Найдем все коммутаторы. Очевидно, что $[x,x] = \left[x, x^{-1}\right] = \left[x^{-1}, x\right] = [e,x] = [x,e] = e \ \forall x \in G$.

$\left[(1\ \ 2), (2\ \ 3)\right] = \left[(1\ \ 2), (1\ \ 2\ \ 3)\right] = \left[(1\ \ 3)\ (1\ \ 2\ \ 3)\right] = \left[(2\ \ 3)\ (1\ \ 2)\right] = (1\ \ 2\ \ 3)$;

$\left[(1\ \ 2), (1\ \ 3)\right] = \left[(1\ \ 2), (1\ \ 3\ \ 2)\right] = \left[(1\ \ 3), (2\ \ 3)\right] = \left[(1\ \ 3), (1\ \ 3\ \ 2)\right] =$

$= \left[(2\ \ 3), (1\ \ 3\ \ 2)\right] = (1\ \ 3\ \ 2)$. Учитывая, что $[a,b]^{-1} = [b,a] \ \forall a,b \in G$, получим: $S_3' = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\} = A_3$.

2) Так как $[a,b] = aba^{-1}b^{-1}$, то могут представиться такие случаи: $[ч,ч] = ч \cdot ч \cdot ч \cdot ч =$ $= ч$, $[ч,н] = ч \cdot н \cdot ч \cdot н = ч$, $[н,ч] = н \cdot ч \cdot н \cdot ч = ч$, $[н,н] = н \cdot н \cdot н \cdot н = н$, где $н$ – нечетная перестановка $ч$ – четная перестановка. Значит, в коммутанте не может быть нечетных перестановок $\Rightarrow S_n' \subset A_n$. Найдем коммутатор двух перестановок: $\left[(i\ \ j), (i\ \ k)\right] = (i\ \ j)(i\ \ k)(i\ \ j)(i\ \ k) = (i\ \ j\ \ k)$, где i, j, k – числа $\Rightarrow$ в коммутанте имеются все такие циклы: $(i\ \ j\ \ k) \in S_n'$, а так как любую четную перестановку можно представить в виде произведения тройных циклов, то все четные перестановки имеются в коммутанте. Значит, $S_n' = A_n$.

Теорема 1.

Пусть G – некоторая группа, H – подгруппа группы G. Если $G' \subset H$, то H – нормальная подгруппа.

Доказательство.

Рассмотрим произведение вида gxg^{-1}, где $x \in H$, g – произвольный элемент из G .

Домножив произведение на e, получим $gxg^{-1} = gxg^{-1}e = \ = gxg^{-1}x^{-1}x = [g,x]x$. Так как $[g,x] \in G' \subset H, x \in H \Rightarrow [g,x]x \in G'H = H \Rightarrow gxg^{-1} \in H$. При таком действии любого элемента группы G на все элементы подгруппы H получим снова подгруппу H, а не меньшую подгруппу. Покажем это. Предположим обратное: пусть получаются не все элементы H. Тогда выберем в качестве g элемент e (причем $exe^{-1} = x$), и получим всю подгруппу $H \Rightarrow$ предположение неверно. Тогда H – по определению нормальная подгруппа G, ч. т. д.

Следствие. Коммутант является нормальной подгруппой группы G.

Группу G, для которой выполнено $G \triangleright G' \triangleright G'' \triangleright \ldots \triangleright G^{(n)} = \{e\}$, называют *разрешимой группой*.

Группу, не имеющую нетривиальных нормальных подгрупп, называют *простой*.

Пример 2.

Определить, является ли группа разрешимой: а) S_3; б) S_4; в) S_5.

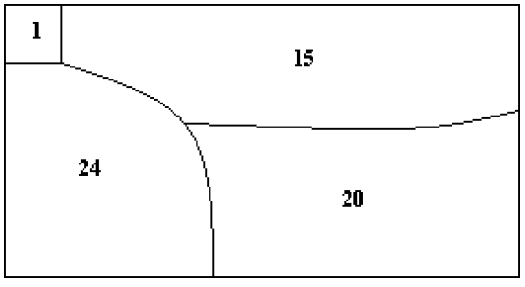
Решение.

а) Составим цепочку: $S_3' = A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$. Коммутатор любых двух элементов $a, b \in A_3$ равен e, значит, $A_3' = \{e\} \Rightarrow S_3 \triangleright A_3 \triangleright \{e\} \Rightarrow$ группа S_3 разрешима.

б) Так как $S_4' = A_4 = \{e, (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 2), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3), (1\ 2)(3\ 4), (1\ 3)(2\ 3), (1\ 4)(2\ 3)\}$,

$A_4' = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ ($A_4' = V_4$, где V_4' – группа Клейна), $V_4' = \{e\}$, значит, $S_4 \triangleright A_4 \triangleright V_4 \triangleright \{e\} \Rightarrow$ группа S_4 разрешима.

в) $S_5' = A_5$. Так как коммутант принадлежит нормальной подгруппе, определим, какие нормальные подгруппы имеет группа A_5. Для этого найдем все классы сопряженных элементов в этой группе ($i, j, k, l, m = \overline{1,5}$): 1) $\{e\}$ (один элемент); 2) класс элементов вида $\{(ijk)\}$ (20 элементов); 3) класс элементов вида $\{(ij)(kl)\}$ (15 элементов); 4) два класса



элементов вида $\{(ijklm)\}$ (2 по 12 элементов). То есть вся группа A_5 может быть разделена на классы сопряженных элементов, не пересекающиеся между собой. Схематично это представление показано на рисунке. Полученные кусочки нельзя составить вместе так, чтобы получилась нетривиальная подгруппа. Покажем это. Для того чтобы класс являлся подгруппой, необходима принадлежность единичного элемента данному классу. То есть, одним из условий получения подгруппы является объединение этого класса с классом $\{e\}$. Но при этом порядок полученной новой части не будет делить порядок группы. Значит, подгрупп у группы A_5 может быть лишь две: $\{e\}$ и A_5 (то есть A_5 – простая группа). Следовательно, коммутантом в A_5 может быть одна из тривиальных подгрупп. Рассмотрим такой коммутатор: $[(1\,2\,3),(1\,2\,4)] = (1\,2)(3\,4)$. Коммутант A_5 не может состоять из одного единичного элемента, значит $A_5' = A_5$. Получено, что группа S_5 неразрешима.

§12. Произведение групп

Пусть имеется пара групп: $(A,*),(B,\circ)$, тогда множество упорядоченных пар вида $\{(a,b), a \in A, b \in B\}$ с заданной операцией $(a_1,b_1)\Diamond(a_2,b_2) = (a_1 * a_2, b_1 \circ b_2)$ называют *прямым внешним произведением групп* и обозначают $A \times B$.

Лемма 1.

Дана группа G и две её нормальные подгруппы A,B, причем $A \cap B = e$. Тогда, если элемент $g \in G$ представляется в виде $g = ab, a \in A, b \in B$, то это представление единственно.

Доказательство.

Предположим обратное. Пусть имеется другое представление: $g = a_1 b_1, a_1 \in A, b_1 \in B$, тогда $ab = a_1 b_1 \Rightarrow a_1^{-1} a = b_1 b^{-1}$, но $A \cap B = e$, следовательно $a_1^{-1} a = b_1 b^{-1} = e \Rightarrow a_1 = a,\ b_1 = b$. Значит представление $g = ab, a \in A, b \in B$ единственно. Лемма доказана.

Лемма 2.

Дана группа G и две её нормальные подгруппы A,B, причем $A \cap B = e$. Тогда

$\forall a \in A, \forall b \in B$ *выполнено:* $ab = ba$.

Доказательство.
Рассмотрим коммутатор элементов a и b:

$[a,b] = aba^{-1}b^{-1} = aa_1 \in A$, $[a,b] = aba^{-1}b^{-1} = b_1 b^{-1} \in B$.

Так как $A \cap B = e$, то $[a,b] = e$ или $ab = ba$. Лемма доказана.

Пусть дана группа G и две её нормальные подгруппы A, B, причем $A \cap B = e$ и $AB = G$, тогда G разлагается в произведение подгрупп A, B : $G = A \times B$. То есть любому элементу g соответствует пара (a,b) по закону: $g = ab$ (причем с учетом леммы 2 $g = ab = ba$). Такое разложение группы называют *прямым внутренним произведением*. Если условие $B \lhd G$ не выполняется, то такое разложение называют *полупрямым внутренним произведением*. Например, группы S_4 и S_n раскладываются в полупрямое внутреннее произведение следующим образом: $S_4 = V_4 \times S_3$, $S_n = A_n \times \langle (1\ \ 2) \rangle$.

Пример.
Найти:

1) Прямое внешнее произведение групп V_4 и циклической группы, порожденной элементом $(1\ \ 2\ \ 3)$.

2) Разложить в прямое внутреннее произведение группу V_4.

Решение.
1) Группа $V_4 = \{e, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$. Циклическая группа, порожденная элементом $(1\ \ 2\ \ 3)$, имеет вид: $G = \{e, (1\ \ 2\ \ 3), (1\ \ 3\ \ 2)\}$. Тогда прямое внешнее произведение данных групп такое: $V_4 \times \langle (1\ \ 2\ \ 3) \rangle = \{e, (1\ \ 2\ \ 3),$ $(1\ \ 2\ \ 4), (1\ \ 3\ \ 2), (1\ \ 4\ \ 2), (1\ \ 3\ \ 4), (1\ \ 4\ \ 3), (2\ \ 3\ \ 4), (2\ \ 4\ \ 3), (1\ \ 2)(3\ \ 4),$ $(1\ \ 3)(2\ \ 3), (1\ \ 4)(2\ \ 3)\} = A_4$. Так как группа $\langle (1\ \ 2\ \ 3) \rangle$ – циклическая, то она изоморфна циклической группе порядка три: Z_3, то есть $A_4 = V_4 \times \langle (1\ \ 2\ \ 3) \rangle \cong V_4 \times Z_3$.

2) Рассмотрим нормальные подгруппы группы V_4: $\langle (1\ \ 2)(3\ \ 4) \rangle = \{e, (1\ \ 2)(3\ \ 4)\}$ и $\langle (1\ \ 3)(2\ \ 4) \rangle = \{e, (1\ \ 3)(2\ \ 4)\}$. Группа V_4 раскладывается в прямое внутреннее

произведение данных групп: $V_4 = \langle (1\ \ 2)(3\ \ 4) \rangle \times \langle (1\ \ 3)(2\ \ 4) \rangle$. Но $\langle (1\ \ 2)(3\ \ 4) \rangle \cong Z_2$, $\langle (1\ \ 3)(2\ \ 4) \rangle \cong Z_2$, тогда $V_4 \cong Z_2 \times Z_2$. Так же можно заметить, что группа $A_4 \cong V_4 \times Z_3 \cong$ $\cong (Z_2 \times Z_2) \times Z_3$.

§ 13. Образующий элемент. Определяющие соотношения

Рассмотрим множество элементов следующего вида: $\{a^k,\ a^n = e\}$. Можно заметить, что данное множество является записью циклической группой порядка n. Рассмотрим произвольную группу и возьмем элементы, например a, b, c, через которые получаются остальные элементы группы. Тогда элементы a, b, c – *образующие элементы*, а выражение $a^n = e$ *– определяющее соотношение.*

Рассмотрим примеры записи групп с помощью образующих элементов и определяющих соотношений.

1) Группа вида $\{\langle a\ \ b \rangle | a^3 = b^2 = e,\ abab = e\}$ состоит из таких элементов: e, a, b, a^2, $a^2 b, ab$, и является группой шестого порядка. Группа Диэдра D_3 является группой шестого порядка. Рассмотрим ее. Пусть элемент a – поворот на угол $120°$, b – любая осевая симметрия. Тогда, группу Диэдра можно записать с помощью образующих элементов и определяющих соотношений: $\{\langle a\ \ b \rangle | a^3 = b^2 = e,\ abab = e\}$. Группа S_3 так же является группой шестого порядка. Ее так же можно представить в указанном виде: в качестве a можно выбрать любой тройной цикл, например $(1\ \ 2\ \ 3)$, а в качестве b – любой двойной цикл, например $(1\ \ 2)$.

2) Группу Диэдра n-ого порядка, учитывая предыдущий пример, можно представить так: $\{\langle a\ \ b \rangle | a^n = b^2 = e,\ abab = e\}$, где a – поворот на угол $\frac{2\pi}{n}$, b – любая осевая симметрия.

3) Группу Q_8 можно представить таким образом: $Q_8 = \{\langle a\ \ b \rangle, a^4 = e, a^2 = b^2,$ $bab^{-1} = a^{-1}\}$. Но так как легче работать с буквенным представлением, чем с матрицами, то Q_8 записывают еще и так: $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, причем $i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,$ $jk = i,\ kj = -i$.

Теорема (основная теорема о гомоморфизмах).

Пусть имеется отображение (гомоморфизм) $f: G \to H$. *Тогда* $G/K \cong \operatorname{Im} f$, *где* $K = \ker f$ – *ядро гомоморфизма.*

Глава 2. КОЛЬЦА

§ 1. Определение и примеры

Непустое множество K **с заданными двумя бинарными операциями, обозначаемых + и ×, и удовлетворяющее аксиомам:**

1) $(K,+)$ **– абелева группа;**

2) $(K,\times)$ **– полугруппа;**

3) $\forall x,y,z \in K\ (x+y)\times z = x\times z + y\times z,\ x\times(y+z) = x\times y + x\times z$.

называется *кольцом*.

Обозначение: $(K,+,\times)$.

Если вторую аксиому изменить на: $(K,\times)$ **– моноид, то** $(K,+,\times)$ **будет называться *кольцом с единицей*.**

Рассмотрим примеры колец.

1) $(\square,+,\times)$ – кольцо с единицей;

2) $(n\square,+,\times), n \in \square$, $n = 1$ – кольцо с единицей, $n \neq 1$ – кольцо;

3) $(\square,+,\times)$, $(\square,+,\times)$, $(\square,+,\times)$ – кольцо с единицей;

4) $\left(\left\{x + y\sqrt{2}\right\},+,\times\right)$, $x, y \in \square$ – кольцо с единицей;

5) $\left(\left\{x + y\sqrt[3]{2}\right\},+,\times\right)$ – не является кольцом, т.к. множество не замкнуто относительно второй операции;

6) $\left(\left\{x + iy\right\},+,\times\right)$, $x, y \in \square$ – кольцо гауссовых чисел (кольцо с единицей);

7) $\left(\left\{\text{âåù åñòâåí íû å ñèì àòðè÷åñêèå àòðèöû ï î ðÿäêà } n\right\},+,\times\right)$ – не является кольцом;

8) $\left(\left\{\begin{pmatrix} x & y \\ \alpha y & x \end{pmatrix}\right\},+,\times\right)$, $x, y \in \square, \alpha = \text{const} \in \square$ – кольцо с единицей;

9) $\left(\left\{\text{í åï ðåðû âí û å ô óí êöèè í à } [a,b]\right\},+,\times\right)$ – кольцо с единицей;

10) $\left(\left\{\text{ô óí êöèè, èì åþ ù èå âîò ðóþ ï ðî èçâî äí óþ í à } [a,b]\right\},+,\times\right)$ – кольцо с единицей;

11) $\left(\left\{\text{ô óí êöèè, î áðàù àþ ù èåñÿ â í óëü í à í åêî òî ì ï î äì í î æåñòâå } [a,b]\right\},+,\times\right)$ – кольцо с единицей;

12) $\left(2^A,\Delta,\cap\right)$ – кольцо с единицей (здесь A – множество, 2^A – множество всех его подмножеств);

13) $(Z_p, +, \times)$ – кольцо классов вычетов;

14) $(\{$âåù åñòâåí í û å ñèì ì åòðè÷åñêè å ì àòðèöû ï î ðÿäêà $n\}, +, \times)$.

Замечание. Здесь единственное конечное кольцо – кольцо классов вычетов, все остальные – бесконечные.

§ 2. Кольцо классов вычетов

Построим кольцо вычетов. Пусть n – фиксированное натуральное число. Рассмотрим в множестве $\mathbb{Z}$ целых чисел следующее *отношение сравнимости по модулю* n: a *сравнимо с* b *по модулю* n (обозначение $a \equiv b \pmod{n}$), если $a - b$ делится на n или, что равносильно, если a и b дают одинаковые остатки при делении на n.

Очевидно, что это отношение эквивалентности, причем классы эквивалентности могут быть занумерованы числами $0, 1, 2, \ldots, n-1$ таким образом, что r-ый класс состоит их всех целых чисел, дающих при делении на n остаток r.

Класс эквивалентности, содержащий целое число a, называется *вычетом числа* a по модулю n и обозначается через $[a]_n$ или просто через $[a]$, если ясно, какое n имеется в виду. Также для упрощения записи квадратные скобки иногда опускают.

Фактормножество множества $\mathbb{Z}$ по отношению сравнимости по модулю n обозначается через Z_n. Мы можем написать, что $Z_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, но следует понимать, что каждый элемент множества Z_n может быть обозначен по-разному. Так, элемент $[1]_n$ может быть с таким же успехом обозначен, как $[2n+1]_n, [-(n-1)]_n$ и т.д.

Докажем теперь, что отношение сравнимости по модулю n согласовано с операциями сложения и умножения в $\mathbb{Z}$. Пусть $a \equiv a' \pmod{n}$, $b \equiv b' \pmod{n}$. Тогда $a + b \equiv a' + b \equiv a' + b' \pmod{n}$ и, аналогично, $ab \equiv a'b = a'b' \pmod{n}$.

Таким образом, мы можем определить в множестве Z_n операции сложения и умножения по формулам $[a]_n + [b]_n = [a+b]_n, [a]_n [b]_n = [ab]_n$ (справедливым для любых $a, b \in \mathbb{Z}$). Тем самым Z_n превращается в коммутативное ассоциативное кольцо с единицей. Оно называется кольцом вычетов по модулю n.

Пример.

Вычислим $[2]^{100}$ в кольце Z_{125}.

Решение.

$[2]^7 = [128] = [3],\ [2]^{35} = \left([2]^7\right)^5 = [3]^5 = [243] = [-7],\ [2]^{50} = [2]^{35}\left([2]^7\right)^2[2] = [-7][3]^2[2] =$

$= [-126] = [-1],\ [2]^{100} = \left([2]^{50}\right)^2 = [1].$

Полученный результат означает, что $2^{100} \equiv 1 (\mathrm{mod}\ 125)$.

§ 3. Гомоморфизм и идеалы колец

Даны два кольца $(K_1, \square, \times)$, $(K_2, \Diamond, \bullet)$.

Операция $f : (K_1, \square, \times) \to (K_2, \Diamond, \bullet)$ **называется** ***гомоморфизмом*** **кольца** $K_1 \to K_2$, **если выполнено:**

1) $\forall x, y \in K_1\ f(x \square y) = f(x) \Diamond f(y)$;
2) $\forall x, y \in K_1\ f(x * y) = f(x) \bullet f(y)$.

$\ker f = \{x \in K_1 \mid f(x) = 0\}$ – ***ядро гомоморфизма***, **где 0 – единичный элемент по сложению** $\in K_2$

Если $\ker f = 0$, **то** f **называется** ***мономорфизмом*** **(**$0 \in K_1$**).**

Если $\mathrm{Im}\ f = K_2$, **то** f **называется** ***эпиморфизмом*.**

Мономорфизм + эпиморфизм = изоморфизм.

Подмножество L **кольца** K – ***подкольцо***, **если** $\forall x, y \in L : x - y \in L,\ xy \in L$.

Пример 1.

$(n\square, +, \times), n \in \square$ подкольцо $(\square, +, \times)$.

Если выполнено: L **– подкольцо кольца** K **и** $LK \subset L$, $KL \subset L$, **то** L – ***двусторонний идеал*** **кольца** K.

Способ построения идеала:

Берем элемент a, перемножаем на все элементы из K: aK, Ka. Затем получившиеся элементы складываем и перемножаем. Таким образом, получаем *главный идеал элемента* a.

Пример 2.

Найти все идеалы Z_{12}.

Решение.

1) Найдем главные идеалы элементов:
   а) $\{0\}$;
   б) $1 \in L \Rightarrow L = Z_{12}$;
   в) $2 \in L \Rightarrow L = \{0,2,4,6,8,10\}$;
   г) $3 \in L \Rightarrow L = \{0,3,6,9\}$;
   д) $4 \in L \Rightarrow L = \{0,4,8\}$;
   е) $5 \in L \Rightarrow L = Z_{12}$, дальше идеалы совпадают с ранее полученными.
2) $\{2,3\} \in L \Rightarrow L = \{0,2,4,6,8,10,3,6,9,5,11,7,1\} = Z_{12}$ и т.д.

§ 4. Факторкольцо

Рассмотрим кольцо K и его идеал L. Множество смежных классов $\{a+L\}$ с введенными операциями:

1) $(a+L)+(b+L)=(a+b)+L$;

2) $(a+L)(b+L)=ab+L$

называется *факторкольцо* кольца K по идеалу L. Обозначение: K/L.

Пример.
Дано: Z_{12}, $L=\{0,4,8\}$. Найти: K/L,

Решение.
$K/L=\{a+L\}-?$.

$0+L=L=L_1,\ 1+L=\{1,5,9\}=L_2,\ 2+L=\{2,6,10\}=L_3,\ 3+L=\{3,7,11\}$.

$Z_{12}/\{0,4,8\}=\{L_1,L_2,L_3,L_4\}$.

Полученные смежные классы называются *классами вычетов по модулю* L.

§ 5. Делители нуля. Поле

Элемент кольца a называется *левым делителем нуля*, а b – *правым*, если выполнено: $a,b \in K, a \neq 0, b \neq 0, ab = 0$.

Замечание. Если кольцо коммутативно по умножению, то левый и правый делители совпадают, в этом случае их называют *делители нуля*.

Пример 1.
Поле Z_4, $2 \cdot 2 = 0 \pmod 4 \Rightarrow 2$ является левым и правым делителем нуля.

Пример 2.

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

Коммутативное кольцо с единицей без делителей нуля называется *целостным кольцом*.

Теорема 1.

Коммутативное кольцо является целостным тогда и только тогда, когда имеет место закон сокращения: $ac = bc, c \neq 0 \Rightarrow a = b$.

Доказательство.

1) Необходимость.

$ac - bc = 0 \Rightarrow (a-b)c = 0, c \neq 0 \Rightarrow a - b = 0 \Rightarrow a = b$.

2) Достаточность.

Пусть $ab = 0, a \neq 0, b \neq 0 \Rightarrow ab = 0 \cdot b$ $\Rightarrow$ по закону сокращения $a = 0 \Rightarrow$ получено противоречие.

Множество $U(K) = \{a \in K : \exists a^{-1} \in K\}$ называется множеством обратимых элементов кольца K.

Теорема 2.

$U(K)$ – группа по умножению, если K – коммутативное кольцо с единицей.

Доказательство.

1) $\forall a, b, c \in K \Rightarrow (ab)c = a(bc)$ – из определению кольца;

2) $\exists 1$,т.к. кольцо K является коммутативным кольцом с единицей по условию;

3) $\exists\ a^{-1} \in U(K) : a^{-1}a = 1$ – по определению $U(K)$.

Теперь докажем замкнутость группы $U(K)$ относительно операции умножения:

$a, b \in U(K), (ab)\cdot\left(b^{-1}a^{-1}\right) = aa^{-1} = 1 \Rightarrow$ у ab есть обратный элемент $b^{-1}a^{-1}$.

Пример 3.

1) $U(\square) = \{1; -1\}$;

2) $U(\square) = \square / \{0\}$;

3) $U(Z_6) = \{1; 5\}$.

***Поле* – коммутативное кольцо с единицей, у которого все ненулевые элементы обратимы.**

Замечание. Кольцо, состоящее из одного нуля не считается полем.

Примерами полей служит поле рациональных чисел Q, поле действительных чисел R и поле комплексных чисел C. Кольцо Z не является полем: в нем обратимы только ± 1. Отсутствие делителей нуля в поле означает, что произведение любых двух ненулевых элементов также является ненулевым элементом. Ненулевые элементы поля P образуют абелеву группу относительно умножения. Она называется *мультипликативной группой поля* P и обозначается через P^*. Можно записать: $P^* = P / \{0\}$.

Теорема 4.

Кольцо Z_n *является полем тогда и только тогда, когда* n *– простое число.*

Доказательство.

1) Пусть n составное, т.е. $n = kl$, где $1 < k, l < n$. Тогда $[k]_n, [l]_n \neq 0$, но $[k]_n [l]_n = [kl]_n = [n]_n = 0$. Таким образом, в кольце Z_n имеются делители нуля и, значит, оно не является полем.

2) Пусть, напротив, n – простое число и $[a]_n \neq 0$, т.е. a не делится на n. Будем искать элемент, обратный к $[a]_n$ подбором, т.е. умножая $[a]_n$ по очереди на все элементы кольца. Получим элементы $[0]_n, [a]_n, [2a]_n, \ldots, [(n-1)a]_n$ (*).

Докажем, что все они различны. В самом деле если $[ka]_n = [la]_n (0 \le k < l \le n-1)$, то $[(l-k)a]_n = 0$, т.е. $(l-k)a$ делится на n, что невозможно, так как ни $l-k$, ни a на n не делятся. (Здесь мы использовали то, что n простое.) Следовательно, в ряду элементов (*) встречаются все элементы кольца Z_n, в том числе $[1]_n$, а это и означает,

что элемент $[a]_n$ обратим.

Кольцо Z_n обладает всеми свойствами поля, кроме, быть может обратимости ненулевых элементов. Очевидно, что Z_2 – поле из двух элементов.

Теорема 5 (малая теорема Ферма).

p – простое число $\Rightarrow \forall a \neq 0 \pmod p$ *выполнено:* $a^{p-1} = 1 \pmod p$.

Доказательство.

p – простое число, следовательно Z_p – поле. Рассмотрим мультипликативную группу этого поля:

$Z_p^* = \{1, 2, ..., p-1\}, \left|Z_p^*\right| = p-1$. По теореме Лагранжа $\forall a \in Z_p^*, a^{p-1} = 1 \pmod p$

Конечные поля могут быть с количеством элементов p^n, где p – простое число и $n \in N$.

Например, существует поле с четырьмя и с восемью элементами, но не существует поля с шестью элементами.

P_1 – подполем поля P, если P_1 является подкольцом кольца P и само является полем. В этом случае поле P называется расширением поля P_1.

Пример 4.

1) □ – подполе □, а □ – расширение □;

2) $\square\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \middle| a, b \in \square\right\}$ – расширение □.

§ 6. Характеристика поля

***Простое поле* – поле, не имеющее нетривиального подполя.**

Теорема.

У любого поля существует и единственное простое подполе, причем оно изоморфно либо Z_p, либо Q.

Доказательство.

1) Рассмотрим поле P и найдем его подполя: $P_1, P_2, ..., P_n$. Причем $P_1 \cap P_2 \cap ... \cap P_n = P_0$ – простое подполе.

2) В любом поле существуют элементы 0 и 1, т.е. $\{0,1\} \subset P_0$.

Т.к. $1 \in P_0 \Rightarrow 1+1 \in P_0$ (в виду замкнутости), $1+1+1 \in P_0$ и т.д. Если этот процесс оборвется, т.е $\underbrace{1+1+...+1}_{p} = 0$, то $P_0 \cong Z_p$. Если этот процесс не оборвется, то все $\underbrace{1+1+...+1}_{n} \in P_0$, т.е. все натурные числа находятся в поле P_0 ($\square \subset P_0$).

Рассмотрим обратные элементы: $-(1+1+...+1) \in P_0 \Rightarrow \square \subset P_0$. Аналогично обратные элементы по умножению: $(1+1+...+1)^{-1} \in P_0$, причем в виду замкнутости $\underbrace{(1+1+...+1)}_{n}\underbrace{(1+1+...+1)}_{k} \in P_0$. Следовательно, $P_0 \cong Q$. Теорема доказана.

Поле, простое подполе которого изоморфно *Q*, называется *полем характеристики ноль* ($\mathrm{char}\, P = 0$). **Поле, у которого простое подполе изоморфно Z_p, называется *полем характеристики*** p ($\mathrm{char}\, P = p$).

§ 7. Поле комплексных чисел

Подобно тому как невозможность деления в кольце целых чисел приводит к необходимости расширить его до поля рациональных чисел, невозможность извлечения квадратных корней из отрицательных чисел в поле действительных чисел приводит к необходимости расширить его до большего поля, называемого полем комплексных чисел.

Для того чтобы лучше понять, что такое поле комплексных чисел, нужно прежде всего подумать над тем, что такое поле действительных чисел. Строгое построение поля действительных чисел обычно приводится в курсе анализа. Мы не будем входить в его детали. Однако заметим, что имеется несколько определений действительных чисел: как бесконечных десятичных дробей, как сечений Дедекинда множества рациональных чисел и т.д. Формально говоря, при этом получаются различные поля. Какое из них является «настоящим» полем действительных чисел? Ответ на этот вопрос состоит в том, что все они изоморфны и их следует рассматривать просто как различные модели одного и того же объекта, называемого полем действительных чисел.

Наиболее удовлетворительных в подобной ситуации всегда является аксиоматический подход, при котором сначала формулируются в виде аксиом свойства, которыми должен обладать искомый объект, а затем доказывается, что этими свойствами он определяется однозначно с точностью до изоморфизма, и с помощью какой-либо конструкции доказывается его существование. В случае поля действительных чисел такими аксиомами (помимо аксиом поля) могут быть аксиомы порядка, аксиома Архимеда и аксиома непрерывности.

Нетрудно доказать, что любые две модели поля действительных чисел не просто изоморфны, но между ними имеется единственный изоморфизм. (Доказательство сводится к тому, что всякий изоморфизм поля $\mathbb{R}$ на себя тождествен, и основано на соображении, что неотрицательные числа при любом изоморфизме должны переходить в неотрицательные, так как они и только они являются квадратами в поле $\mathbb{R}$.) Это означает, что каждый элемент поля $\mathbb{R}$ имеет свою индивидуальность, т.е. в любой модели могут быть идентифицированы числа 10, $\sqrt{2}$, π и т.д.

Дадим теперь аксиоматическое определение поля комплексных чисел.

Полем комплексных чисел называется всякое такое поле $\mathbb{C}$, обладающее следующими свойствами:

1. *оно содержит в качестве подполя поле* $\mathbb{R}$ *действительных чисел;*

2. *оно содержит такой элемент* i, *что* $i^2 = -1$;

3. *оно содержит минимально среди полей с этими свойствами*, т.е. если $K \subset \mathbb{C}$ – какое-либо подполе, содержащее $\mathbb{R}$ и i, то $K = \mathbb{C}$.

Теорема.

Поле комплексных чисел существует и единственно с точностью до изоморфизма, переводящего все действительные числа в себя. Каждое комплексное число однозначно представляется в виде $a + bi$, *где* $a, b \in \mathbb{R}$, *а* i *– (фиксированный) элемент, квадрат которого равен* -1.

Поле комплексных чисел можно определить и другими способами:

1) множество матриц вида: $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$;

2) упорядоченная пара двух чисел;

3) $\mathbb{R}(i)$ – расширение поля $\mathbb{R}$.

§ 8. Кольцо многочленов

Пусть K кольцо с единицей 1, A – некоторое его подкольцо, содержащее 1. Если $t \in K$, то наименьшее подкольцо в K содержащее A и t, будет, очевидно, состоять из элементов вида

$$a(t) = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n,$$

где $a_s \in A$, $n \in \mathbf{Z}$, $n \geq 0$. Обозначим его $A[t]$.

A –коммутативное кольцо с 1, множество наборов $\{(a_0, a_1, \ldots, a_n, \ldots), a_i \in A\}$, где все a_i кроме конечного числа равны 0, с введенными операциями

$$(a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$$
$$(a_0, a_1, \ldots, a_n, \ldots)(b_0, b_1, \ldots, b_n, \ldots) = (c_0, c_1, \ldots, c_n, \ldots),$$

где $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$, называется *кольцом многочленов над* A (обозначается $A[x]$), а его элементы *многочленами*.

Нулевым элементом в кольце многочленов является $(0, 0, \ldots, 0, \ldots)$, единицей – $(1, 0, \ldots, 0, \ldots)$. Обозначим $(0, 1, 0, \ldots, 0, \ldots)$ через X. Используя введенную операцию умножения, находим, что $X^2 = (0, 0, 1, 0, \ldots, 0, \ldots)$. Также введем обозначение $(a, 0, 0, \ldots, 0, \ldots) = a(1, 0, \ldots, 0, \ldots)$. Тогда в новых обозначениях можно выполнить разложение

$$(a_0, a_1, \ldots, a_n, \ldots) = (a_0, 0, \ldots, 0, \ldots) + (0, a_1, 0, \ldots, 0, \ldots) + \ldots = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots .$$

Порядком элемента $(a_0, a_1, \ldots, a_n, \ldots)$ называется номер самого правого отличного от нуля a_i (обозначение $\deg(a_0, a_1, \ldots, a_n, \ldots)$). Или $\deg(a_0, a_1, \ldots, a_n, \ldots) = \max_{a_i \neq 0} i$.

Пусть $\deg(a_0, a_1, \ldots, a_n, \ldots) = n$ и $\deg(b_0, b_1, \ldots, b_n, \ldots) = k$. Тогда из операций сложения и умножения следует, что $\deg\left((a_0, a_1, \ldots, a_n, \ldots) + (b_0, b_1, \ldots, b_n, \ldots)\right) \leq \max\{n, k\}$ и $\deg\left((a_0, a_1, \ldots, a_n, \ldots)(b_0, b_1, \ldots, b_n, \ldots)\right) = n + k$.

Теорема 1.

Если A – целостное кольцо с 1, то и кольцо $A[x]$ $A[x]$ является целостным.

Доказательство.

Рассмотрим многочлены $a = a_0 + a_1 x + \ldots + a_n x^n$ и $b = b_0 + b_1 x + \ldots + b_m x^m$ степеней n и m

соответственно. По условию A не содержит делителей нуля, значит $a_i b_j \neq 0$ для $i = \overline{1, n},\ j = \overline{1, m}$. Из этого справедливо

$$a\ ab = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + (a_n b_m)x^{n+m}.$$

Отсюда следует, что и $A[x]$ не содержит делителей нуля.

Теорема 2.

Пусть коммутативное кольцо K содержит A в качестве подкольца. Для каждого элемента $t \in K$ существует единственный гомоморфизм $\varphi : A[x] \to K$ такой, что $\forall a \in A\ \ \varphi(a) = a\ \ \varphi(x) = t$.

Доказательство.

Предположим, что такой гомоморфизм φ существует. Т. к. $\varphi(a_i) = a_i$ для каждого коэффициента многочлена a, записанного в виде $a = a_0 + a_1 x + \ldots + a_n x^n$, и $\varphi\left(x^k\right) = \left(\varphi\left(x\right)\right) = t^k$ (по свойству гомоморфизма и условию теоремы), то

$$\varphi\left(a\right) = \varphi\left(a_0 + a_1 x + \ldots + a_n x^n\right) = t_0 + t_1 x + \ldots + t_n x^n$$

Т. е. $\varphi\left(a\right)$ определен однозначно и выражается указанной выше формулой. Обратно: задав отображение φ этой же формулой, мы, очевидно, удовлетворим условию и получим гомоморфизм колец. Это ясно для отображения аддитивных групп колец, а что касается умножения, то применение φ к произведению $ab = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + (a_n b_m)x^{n+m}$, а затем использование (общего) закона дистрибутивности даёт

$$\varphi\left(ab\right) = \varphi\left(a_0 b_0\right) + \varphi\left(a_0 b_1 + a_1 b_0\right)t + \ldots + \varphi\left(a_n b_m\right)t^{n+m} = \left(\sum_{i=0}^{n} a_i t^i\right)\left(\sum_{j=0}^{m} b_j t^j\right) = \varphi\left(a\right)\varphi\left(b\right).$$

Элемент t называется *алгебраическим над кольцом* A, если $\varphi(t) = 0$, т. е. найдется многочлен $a_0 + a_1 t + \ldots + a_n t^n = 0$. Если $\varphi(t) \neq 0$, то t – *трансцендентный над* A элемент.

Пример.

Для $\mathbf{Z}[t]$ числа $\sqrt{2}$ и π являются трансцендентными, а число 2 является алгебраическим.

§ 9. Делитель

Элемент a *делит* элемент b (b *делится* на a), если $\exists c : ac = b$. Обозначения: $a \mid b$ – a делит b, $b \vdots a$ – b делится на a.

Если $a \mid b$ и $b \mid a$, то a и b называются *ассоциированными*.

Элемент a называется *простым*, если он необратим и не разлагается в произведение необратимых элементов.

Пример 1.
В поле Q все числа, кроме 0, являются ассоциированными между собой.

Пример 2.
В кольце $\square$ ассоциированными являются противоположные элементы.

Основные свойства отношения делимости в целостном кольце K:

1. *Если* $a \mid b$, $b \mid c$, *то* $a \mid c$.

Доказательство.

Действительно, мы имеем $b = ab'$, $c = bc'$, где $b', c' \in K$. Поэтому $c = (ab')c' = a(b'c')$.

2. *Если* $a \mid b$, $a \mid c$, *то* $a \mid (b \pm c)$.

Доказательство.

В самом деле, по условию $a = ca'$, $b = cb'$ для некоторых $a', b' \in K$, и ввиду дистрибутивности $a \pm b = c(a' + b')$.

3. *Если* $a \mid b$, *то* $a \mid bc$.

Доказательство.

Ясно, что $b = ab' \Rightarrow bc = (ab')c = a(b'c)$.

Кольцо K обладает свойством *факториальности*, если любой элемент $a \neq 0$ из кольца K раскладывается в произведение $a = up_1 p_2 \dots p_r$,

где u – обратимый элемент, а $p_1, p_2, \dots, p_r$ – простые элементы (не обязательно попарно различные), причем из существования другого такого разложения $a = uq_1 q_2 \dots q_s$ следует, что $r = s$ и при надлежащей нумерации элементов p_i и q_j будет $q_1 = u_1 p_1, \dots, q_r = u_r p_r$,

где $u_1, u_2, \dots, u_r$ – обратимые элементы.

Пример.
Кольцо $\square$ и $\square[x]$ факториально.

Не во всех кольцах есть единственность разложения.

Пример.
Рассмотрим $\square\left[\sqrt{5}\right]$. $\left(7+\sqrt{5}\right)\left(7-\sqrt{5}\right)=44=4\cdot 11$

$$\forall a,b\in K\ \exists! c,r\in K: a=bc+r$$
$$\forall P(x),Q(x)\ \exists! R(x),S(x): P(x)=Q(x)S(x)+R(x), \deg R(x)<\deg Q(x)$$

§ 10. НОД и НОК

Пусть K – целостное кольцо. Под *наибольшим общим делителем* понимают двух элементов $a,b\in K$ будем понимать элемент $d\in K$, обозначаемый $\text{НОД}(a,b)$ и обладающий следующими двумя свойствами:

1. $d\mid a, d\mid b$**;**

2. $c\mid a, c\mid b\Rightarrow c\mid d$**.**

Введем понятие *наименьшего общего кратного* $m=\text{НОК}(a,b)$ элементов $a,b\in K$, определенного двумя свойствами:

1. $a\mid m, b\mid m$**;**

2. $a\mid c, b\mid c\Rightarrow m\mid c$**.**

Теорема 1.

Пусть $a=up_1^{k_1}\ldots p_r^{k_r}$, $b=vp_1^{l_1}\ldots p_r^{l_r}$ *– элементы факториального кольца* K*. Тогда:*

$$\text{НОД}(a,b)=w_1p_1^{s_1}\ldots p_r^{s_r}, \text{ где } s_i=\min\{k_i,l_i\}, i=\overline{1,r};$$
$$\text{НОК}(a,b)=w_2p_1^{t_1}\ldots p_r^{t_r}, \text{ где } t_i=\max\{k_i,l_i\}, i=\overline{1,r}.$$

Следствие. $ab=\text{НОД}(a,b)\cdot\text{НОК}(a,b)$.

Алгоритм Евклида нахождения $\text{НОД}(a,b)$:

Пусть даны ненулевые элементы $a,b \in K$. Применяя последовательность действий:

$$a = b \cdot s_1 + r_1$$
$$b = r_1 \cdot s_2 + r_2$$
$$r_1 = r_2 \cdot s_3 + r_3$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-1} = r_n s_{n+1} + r_{n+1}$$
$$r_n = r_{n+1} s_{n+2}$$

Таким образом за конечное число шагов получим нулевой остаток от деления, а последний не нулевой остаток и будет $\text{НОД}(a,b) = r_{n+1}$.

Пример.

Найти НОД $P(x) = x^4 + x^3 - 3x^2 - 4x - 1$ и $Q(x) = x^3 + x^2 - x - 1$.

$$P(x) = xQ(x) + (-2x^2 - 3x - 1)$$

$$Q(x) = \left(-\frac{1}{2}x + \frac{1}{4}\right)\left(-2x^2 - 3x - 1\right) + \left(-\frac{3}{4}x - \frac{3}{4}\right)$$

$$-2x^2 - 3x - 1 = \left(\frac{8}{3}x + \frac{4}{3}\right)\left(-\frac{3}{4}x - \frac{3}{4}\right)$$

Т. о. $\text{НОД}\left(P(x), Q(x)\right) = x + 1$.

Теорема 2.

Любые два многочлена $P(x)$ *и* $Q(x)$ *имеют* НОД, *причем можно найти такие* $u(x)$ *и* $v(x)$, *что будет выполнено соотношение* $\text{НОД}\left(P(x), Q(x)\right) = u(x)P(x) + v(x)Q(x)$.

Доказательство.

Это следует из алгоритма Евклида.

§ 11. Евклидовы кольца

Кольцо K называется *евклидовым*, если существует отображение

$$\delta\left(K / \{0\}\right) \to \square \cup \{0\}$$

такое, что выполнены условия:

1. $\delta(a) \le \delta(ab), \forall a,b \ne 0$;

2. $\forall a,b \exists q,r : a = bq + r$, *где* $\delta(a) < \delta(b)$ *или* $r = 0$.

Пример 1.

$\mathbf{Z}$ – евклидово кольцо. $\delta(x) = |x|$.

Пример 2.
Для $\square[x]$ $\delta(P(x)) = \deg P(x)$.

Теорема 1.

Всякое евклидово кольцо K является кольцом с разложением, т. е. любой элемент $a \neq 0$ из K записывается в виде $a = up_1p_2 \dots p_r$, где u – обратимый элемент, а $p_1, p_2, \dots, p_r$ – простые элементы.

Доказательство.

Пусть элемент $a \in K$ обладает собственным делителем b: $a = bc$, где b и c – необратимые элементы (другими словами, a и b не ассоциированы). Докажем, что $\delta(b) < \delta(a)$.

Согласно первой аксиоме евклидовых колец $\delta(b) \leq \delta(bc) = \delta(a)$. Предположив выполнение равенства $\delta(b) = \delta(a)$, воспользуемся второй аксиомой евклидовых колец и найдем q, r с $b = qa + r$, где $\delta(r) < \delta(a)$ или же $r = 0$. Случай $r = 0$ отпадает ввиду неассоциированности a и b. По той же причине $1 - qc \neq 0$. Отсюда по второй аксиоме (поменять a и b местами)

$$\delta(a) = \delta(b) \leq \delta\left(b\left(1 - qc\right)\right) = \delta(b - qa) = \delta(r) < \delta(a)$$

– противоречие. Значит, $\delta(b) < \delta(a)$.

Если теперь $a = a_1a_2 \dots a_n$, где все a_i необратимы, то $a_{m+1}a_{m+2} \dots a_n$ – собственный делитель $a_m a_{m+1}a_{m+2} \dots a_n$, и по доказанному

$$\delta(a) = \delta(a_1a_2 \dots a_n) > \delta(a_2 \dots a_n) > \dots > \delta(a_n) > \delta(1)$$

Эта строго убывающая цепочка неотрицательных целых чисел имеет длину $n \leq \delta(a)$. Значит, для элемента $a \in K$ имеется разложение максимальной длины, которое и будет разложением на простые множители.

Теорема 2 (критерий факториальности колец).

Целостное кольцо K факториально тогда и только тогда, когда из условия $p \mid ab$, где p – простое, следует, что $p \mid a$ или $p \mid b$.

Доказательство.

1. Пусть K факториально, и пусть $ab = pc$. Если $a = u\prod a_i$, $b = v\prod b_i$, $c = w\prod c_i$ –

разложения a, b и c. Тогда из $uv\prod a_i \prod b_i = pw\prod c_i$, следует что элемент p ассоциирован с одним из a_i или b_j, т.е. p делит a или b.

2. Пусть выполнено условие $p \mid ab \Rightarrow p \mid a$ или $p \mid b$. Рассуждая по индукции, допустим, что разложение всех элементов из K с числом $\le n$ простых множителей единственно(с точностью до порядка множителей и их ассоциированности). Докажем теперь это для любого $a \neq 0$, который может быть разложен на $n+1$ простых множителей. Пусть

$$a = \prod_{i=1}^{n+1} p_i = \prod_{j=1}^{m+1} r_i$$

– два разложения элемента a с $m \ge n$. Условие теоремы примененное к $p = p_{n+1}$, дает, что p_{n+1} должен делить один из элементов $r_{1,\dots,}r_{m+1}$. Без ограничения общности считаем, что $p_{n+1} \mid r_{m+1}$. Но r_{m+1} – простой элемент, поэтому $r_{m+1} = up_{n+1}$, где u – обратимый элемент. Получаем равенство $\prod_{i=1}^{n} p_i = u\prod_{j=1}^{m} r_i$. В правой части стоит произведение n простых множителей. По предположению индукции $m = n$, и оба разложения отличаются лишь порядком простых элементов, снабженных, возможно, какими-то обратимыми множителями.

Теорема 3.

Всякое евклидово кольцо K факториально (т. е. обладает свойством однозначности разложения на простые множители).

Доказательство.

С учетом доказанных выше двух теорем, необходимо показать, что если p – простой элемент кольца K, делящий произведение bc каких-то элементов $b, c \in K$, то $p \mid b$ или $p \mid c$.

При $b = 0$ или $c = 0$ доказывать нечего. Если же $bc \neq 0$,тогда найдем $d = \text{НОД}(b, p)$. Т. к. d делитель простого элемента p, то он либо равен 1 (точнее, является делителем 1), либо ассоциирован с p. В первом случае b и p взаимно простые, значит существуют $u, v \in K : ub + vp = 1$. Значит $ubc + vpc = c$. vpc делится на p, а ubc делится на bc, которое делится на p, следовательно $p \mid c$. Во втором случае $d = up$, $u \mid 1$, значит $p \mid b$.

Теорема 4 (основная теорема арифметики).

Кольца Z и C[x] факториальны.

Доказательство.

Оба этих кольца евклидовы, тога по предыдущей теореме они факториальны.

***Неприводимым* многочленом в кольце $K[x]$ называется простой элемент этого кольца.**

Пример 1.
В любом кольце многочлены первой степени неприводимы.

Пример 2.
x^2+1 является неприводимым в $R[x]$ и является приводимым в $C[x]$, т. к. $x^2+1=(x-i)(x+i)$.

Пример 3.
В $\mathbf{Z}_3[x]$ x^3+2x+1 неприводим.

Пример 4.
В $\mathbf{Z}[x]$ x^5+x+1 неприводим.

Теорема 5.

В любом кольце многочленов существует бесконечно много неприводимых многочленов.

Доказательство.

1) Пусть $K[x]$ бесконечное кольцо, в этом случае достаточно рассмотреть неприводимые многочлены вида $x-a$.

2) Пусть $K[x]$ конечное кольцо. Докажем от противного. Пусть неприводимых многочленов конечное число: $p_1,\dots,p_n$. Составим из них многочлен $f=p_1p_2\dots p_n+1$. Этот многочлен не делится ни одним из p_i, значит, либо f неприводим, тогда противоречие, либо есть делитель из неприводимых, что тоже приводит к противоречию.

Критерий неприводимости (Эйзенштейн).

Пусть $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ *– многочлен в* $Z[x]$*, все коэффициенты* $a_1, \ldots, a_n$ *которого делятся на некоторое простое число* p*, но* a_n *не делится на* p^2*. Тогда* $f(x)$ *не приводим.*

Доказательство.

Предположим обратное, что многочлен приводим. Значит, он раскладывается на множители: $f(x) = \left(x^k + b_1 x^{k-1} + \ldots + b_k\right)\left(x^s + c_1 x^{s-1} + \ldots + c_s\right)$. Рассмотрим это разложение в $\mathbf{Z}_p$. $x^n = x^k x^s$, все $b_i, c_i \vdots p$, значит $a_n = b_k c_s \vdots p^2$. Получили противоречие.

Пример.

$x^5 + 3x^4 + 3x^2 - 6x + 12$ неприводим в $\mathbf{Z}[x]$.

§ 12. Корни многочленов

Элемент a называется *корнем* многочлена $P(x)$, если $P(a) = 0$.

Теорема 1 (теорема Безу).

Элемент a *является корнем многочлена* $P(a)$ *тогда и только тогда, когда* $P(x) \vdots (x-a)$.

Доказательство.

Из алгоритма деления с остатком: $P(x) = (x-c)Q(x) + r(x)$, где $\deg r(x) < \deg(x-c) = 1$. Значит $r(x)$ – константа. Подставляя c вместо x,получим $P(c) = r$, значит $P(x) = (x-c)Q(x) + P(c)$. В частности $P(c) = 0 \Leftrightarrow P(x) = (x-c)Q(x)$.

Элемент a называется *корнем кратности* k многочлена $P(x)$, если $P(x)$ делится на $(x-a)^k$ и не делится на $(x-a)^{k+1}$. Или $P(x) = (x-a)^k Q(x)$, где $Q(a) \neq 0$.

Операция дифференцирования – операция, которая многочлену вида $x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ ставит в соответствие многочлен $nx^{n-1} + (n-1)a_1 x^{n-2} + \ldots + a_{n-1}$.

Теорема 2.

Пусть элемент a *является корнем кратности* k *многочлена* $P(a)$*, тогда* a *будет*

$(k-1)$ *-кратным корнем многочлена* $P'(x)$.

Доказательство.

Рассмотрим $k=1$, значит $P(x)=(x-a)Q(x)$, где $Q(a)\neq 0$. Дифференцируя $P(x)$ получим $P'(x)=Q(x)+(x-a)Q'(x)$. Следовательно $P'(a)\neq 0$.

Теперь пусть a корень кратности $k>1$, значит $P(x0=(x-a)^kQ(x)$, где $Q(a)\neq 0$. Тогда

$$P'(x)=k(x-a)^{k-1}Q(x)+(x-a)^kQ'(x)=(x-a)^{k-1}\left(kQ(x)+(x-a)Q'(x)\right)=(x-a)^{k-1}Q_1(x),$$

где $Q_1(x)=kQ(x)+(x-a)Q'(x)$, причем $Q_1(a)\neq 0$. Значит a корень кратности $k-1$ многочлена $P'(x)$.

Теорема 3.

Пусть $P(x)$ *любой многочлен, тогда многочлен*

$$\frac{P(x)}{\text{НОД}\left(P(x),P'(x)\right)}$$

имеет те же корни, что $P(x)$*, но с единичной кратностью.*

Доказательство.

1) Пусть a корень единичной кратности, тогда $P'(a)\neq 0$. Следовательно, $\text{НОД}\left(P(x),P'(x)\right)$ не делится на $x-a$.

2) Пусть теперь a корень кратности k, тогда $P'(x)=(x-a)^{k-1}Q_1(x)$. Значит $\text{НОД}\left(P(x),P'(x)\right)$ делится на $(x-a)^{k-1}$.

Из этого следует утверждение теоремы.

§ 13. Формулы Виета

Найдем многочлен, корнями которого являются $c_1,c_2,\ldots,c_n$, среди которых, возможно, есть и одинаковые.

$$(x-c_1)(x-c_2)\ldots(x-c_n)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$$

Тогда для коэффициентов $a_1,\ldots,a_n$ получаться выражения через $c_1,\ldots,c_n$:

$$a_1=-(c_1+c_2+\ldots+c_n),$$

$$a_2=\sum_{1\le i<j\le n}c_ic_j,$$

$$a_3=-\sum_{1\le i<j<k\le n}c_ic_jc_k,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_k=(-1)^k\sum_{1\le i_1<i_2<\ldots<i_k\le n}c_{i_1}c_{i_2}\ldots c_{i_k},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$a_n = (-1)^n c_1 c_2 \dots c_n .$$

Эти формулы называются *формулами Виета.*

Многочлен $P(x_1, x_2, \dots, x_n)$ называется *симметрическим,* если:

$$\pi\left(P(x_1, \dots, x_n)\right) = P\left(\pi(x_1), \dots, \pi(x_n)\right),$$

где π - любая перестановка.

Пример.

Многочлен $P(x_1, x_2, x_3) = x_1^{\,2} + x_2 - x_3^{\,2}$, перестановка $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Тогда $\pi\left(P(x_1, x_2, x_3)\right) = x_2^{\,2} + x_3 = x_1^{\,2}$. Значит, $P(x_1, x_2, x_3)$ не является симметрическим.

Простейшие симметрические многочлены

$$s_1 = x_1 + x_2 + \dots + x_n ,$$

$$s_2 = \sum_{1 \le i < j \le n} x_i x_j ,$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots ,$$

$$s_n = x_1 x_2 \dots x_n$$

С их помощью формулы Виета примут вид: $a_k = (-1)^k s_k(c_1, \dots, c_n)$.

§ 14. Симметрические многочлены

Сумма степеней в многочлене вида $x_1^{\alpha_1} \dots x_k^{\alpha_k}$ называется *весом* многочлена. Если в многочлене несколько таких элементов, то вес этом максимум из весом.

Пример.

Для многочлена $x_1^{\,2} x_3 + x_2^{\,3} x_4 + x_2^{\,2} x_3^{\,2}$ вес 4.

Теорема (о представлении симметрических многочленов).

Пусть $P(x_1, \dots, x_n)$ – симметрический многочлен веса m. Тогда существует, и притом единственный, многочлен g веса m такой, что $P(x_1, \dots, x_n) = g(s_1, \dots, s_n)$.

Пример.

Рассмотрим многочлен $x_1^{\,4} + x_2^{\,4} + x_3^{\,4}$. Его вес 4.

$$x_1^4 + x_2^4 + x_3^4 = \alpha s_1^4 + \beta s_1 s_3 + \gamma s_2^2 + \delta s_1^2 s_2 ,$$

где $s_1 = x_1 + x_2 + x_3$, $s_2 = x_1x_2 + x_1x_3 + x_2x_3$, $s_3 = x_1x_2x_3$.

Пусть $x_1 = 1$, $x_2 = 0$, $x_3 = 0$. Тогда $\alpha = 1$.

Пусть $x_1 = 1$, $x_2 = -1$, $x_3 = 0$. Тогда $\gamma = 2$.

Пусть $x_1 = 1$, $x_2 = 1$, $x_3 = 0$. Тогда $2 = 16\alpha + \gamma + 4\delta$. Отсюда $\delta = -4$.

Пусть $x_1 = x_2 = x_3 = 1$. Тогда $3 = 81\alpha + 3\beta + 9\gamma + 27\delta$. Отсюда $\beta = 4$.

В результате получили, что

$$x_1^4 + x_2^4 + x_3^4 = s_1^4 + 4s_1s_3 + 4s_2^2 - 4s_1^2s_2$$

§ 15. Дискриминант

Определителем Вандермонда называется определитель, построенный таким образом:

$$\Delta_n = \begin{vmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ \dots & \dots & \dots & \dots \\ x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \end{vmatrix}.$$

Чтобы найти его значение, последовательно умножим $(n-1)$-ую строку на $-x_1$ и прибавим к n-ой строке, затем $(n-2)$-ую строку на $-x_1$ и прибавим к $(n-1)$-ой строке, и так далее, в конце первую строку умножим на -1 и прибавим ко второй. Получим

$$\Delta_n = \begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & x_2 - x_1 & \dots & x_n - x_1 \\ \dots & \dots & \dots & \dots \\ 0 & x_2^{n-1} - x_2^{n-2}x_1 & \dots & x_n^{n-1} - x_n^{n-2}x_1 \end{vmatrix}.$$

Разложим определитель по первому столбцу:

$$\Delta_n = \begin{vmatrix} x_2 - x_1 & \dots & x_n - x_1 \\ \dots & \dots & \dots \\ x_2^{n-1} - x_2^{n-2}x_1 & \dots & x_n^{n-1} - x_n^{n-2}x_1 \end{vmatrix} = \begin{vmatrix} x_2 - x_1 & \dots & x_n - x_1 \\ \dots & \dots & \dots \\ x_2^{n-2}(x_2 - x_1) & \dots & x_n^{n-2}(x_n - x_1) \end{vmatrix} =$$

$$= (x_2 - x_1)(x_3 - x_1)\cdot\ldots\cdot(x_n - x_1)\begin{vmatrix} 1 & \dots & 1 \\ \dots & \dots & \dots \\ x_2^{n-2} & \dots & x_n^{n-2} \end{vmatrix} = (x_2 - x_1)(x_3 - x_1)\cdot\ldots\cdot(x_n - x_1)\cdot\Delta_{n-1}.$$

Далее аналогично преобразуем определитель $(n-1)$-ого порядка, $(n-2)$-ого порядка и

так далее. В результате получим: $\Delta_n = \prod_{1 \le j < i \le n} (x_i - x_j)$. Можно заметить, если все x_i, x_j различны, то $\Delta_n \neq 0$, иначе определитель равен нулю.

Рассмотрим многочлены $P(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ и $\Delta_n^2 = \prod_{1 \le j < i \le n} (X_i - X_j)^2$, где $X_1, \ldots, X_n$ – корни многочлена $P(x)$, и найдем значение Δ_n^2. Так как $\Delta_n^2 = \Delta_n \Delta_n^T$, то преобразуем многочлен следующим образом:

$$\Delta_n^2 = \begin{vmatrix} 1 & \ldots & 1 \\ \ldots & \ldots & \ldots \\ X_1^{n-1} & \ldots & X_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & \ldots & X_1^{n-1} \\ \ldots & \ldots & \ldots \\ 1 & \ldots & X_n^{n-1} \end{vmatrix} = \begin{vmatrix} n & p_1 & p_2 & \ldots & p_{n-1} \\ p_1 & p_2 & p_3 & \ldots & p_n \\ p_2 & p_3 & p_4 & \ldots & p_{n+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ p_{n-1} & p_n & \ldots & \ldots & p_{2n-1} \end{vmatrix},$$

где $p_1 = \sum_{i=1}^{n} X_i, p_2 = \sum_{i=1}^{n} X_i^2, \ldots, p_k = \sum_{i=1}^{n} X_i^k$. Причем p_k могут быть выражены через $S_k = (-1)^k a_k$ с помощью *формул Ньютона*: $p_k - p_{k-1}S_1 + \ + p_{k-2}S_2 - \ldots + + (-1)^k k S_k = 0$ при $0 < k \le n$; $p_k - p_{k-1}S_1 + p_{k-2}S_2 - \ldots + (-1)^n p_{k-n}S_k = 0$ при $k > n$. То есть многочлен Δ_n^2 зависит от $S_1, \ldots, S_n$.

Величина $Dis(S_1, \ldots, S_n) = \Delta_n^2$ называется *дискриминантом многочлена* $P(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$.

Теорема.

Дискриминант многочлена равен нулю тогда и только тогда, когда многочлен имеет кратные корни.

Пример.
Определить, при каком λ многочлен $P(x) = x^3 - 3x + \lambda$ имеет кратные корни.

Решение.
Данную задачу возможно решить двумя способами.

1) $Dis(S_1, S_2, S_3) = \begin{vmatrix} 3 & p_1 & p_2 \\ p_1 & p_2 & p_3 \\ p_2 & p_3 & p_4 \end{vmatrix}$, $S_1 = -a_1 = 0,\ S_2 = a_2 = -3,\ S_3 = -a_3 = \lambda$. $p_1 - S_1 = 0$

$\Rightarrow p_1 = S_1 = 0;\ p_2 - p_1 S_1 + 2S_2 = 0 \Rightarrow p_2 = 6;\ p_3 - p_2 S_1 + p_1 S_2 - 3S_3 = 0 \Rightarrow p_3 = -3\lambda;$ $p_4 - p_3 S_1 +$

$+p_2S_2 - p_1S_3 = 0 \Rightarrow p_4 = 18$. Многочлен имеет кратные корни, если $Dis(S_1, S_2, S_3) = 0 \Rightarrow$ $3(36 - 9\lambda^2) = 0$. То есть при $\lambda = \pm 2$.

2) $P'(x) = 3x^2 - 3 = 3(x-1)(x+1)$. Если исходный многочлен имеет кратные корни, то многочлен $P'(x)$ такие же корни, но все единичной кратности. Значит, либо корень $x_1 = 1$ – кратный многочлена $P(x)$, либо $x_1 = -1$. В первом случае при $x_1 = 1$ получаем $\lambda = 2$, во втором случае при $x_1 = -1,\ \lambda = -2$. То есть $\lambda = \pm 2$.

§ 16. Результант

Результантом двух многочленов $P(x) = a_0x^n + a_1x^{n-1} \ldots + a_{n-1}x^1 + a_n$ и $Q(x) = b_0x^k + +b_1x^{k-1} \ldots + b_{k-1}x^1 + b_k$ называется определитель:

$$\mathrm{Re}\, z(P(x), Q(x)) = \begin{vmatrix} a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & a_{n-1} & a_n & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & \ldots & \ldots & a_n \\ b_0 & b_1 & \ldots & b_k & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & b_{k-1} & b_k & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & b_0 & b_1 & \ldots & b_k \end{vmatrix}.$$

Результант можно схематично разделить на две части: первая образована коэффициентами многочлена $P(x)$ и содержит k строк, вторая – коэффициентами многочлена $Q(x)$ и содержит n строк.

Теорема.

Результант двух многочленов $P(x) = a_0x^n + \ldots + a_n$ *и* $Q(x) = b_0x^k + \ldots + b_k$ *равен нулю тогда и только тогда, когда – либо* $a_0 = b_0 = 0$, *либо многочлены имеют общий корень.*

Пример.

При каком λ многочлены $P(x) = x^3 - \lambda x + 2$ и $Q(x) = x^2 + \lambda x + 2$ имеют общий корень.

Решение.

Составим результант данных многочленов: $\mathrm{Re}\, z(P(x), Q(x)) =$

$$= \begin{vmatrix} 1 & 0 & -\lambda & 2 & 0 \\ 0 & 1 & 0 & -\lambda & 2 \\ 1 & \lambda & 2 & 0 & 0 \\ 0 & 1 & \lambda & 2 & 0 \\ 0 & 0 & 1 & \lambda & 2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -\lambda & 2 & 0 \\ 0 & 1 & 0 & -\lambda & 2 \\ 0 & \lambda & 2+\lambda & -2 & 0 \\ 0 & 1 & \lambda & 2 & 0 \\ 0 & 0 & 1 & \lambda & 2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -\lambda & 2 \\ \lambda & 2+\lambda & -2 & 0 \\ 1 & \lambda & 2 & 0 \\ 0 & 1 & \lambda & 2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -\lambda & 2 \\ 0 & 2+\lambda & -2+\lambda^2 & -2\lambda \\ 0 & \lambda & 2+\lambda & -2 \\ 0 & 1 & \lambda & 2 \end{vmatrix}.$$

Разложим снова определитель по первому столбцу, тогда: $\operatorname{Re} z\left(P(x), Q(x)\right) =$

$$= \begin{vmatrix} 2+\lambda & -2+\lambda^2 & -2\lambda \\ \lambda & 2+\lambda & -2 \\ 1 & \lambda & 2 \end{vmatrix} = 2(2+\lambda)^2 - 2\lambda^3 - 2\left(-2+\lambda^2\right) + 2\lambda(2+\lambda) + 2\lambda(2+\lambda) - 2\lambda\left(-2+\lambda^2\right) =$$

$$= 2\left(4+4\lambda+\lambda^2\right) - 2\lambda^3 + 4 - 2\lambda^2 + 8\lambda + 4\lambda^2 + 4\lambda - 2\lambda^3 = 12 + 20\lambda + 4\lambda^2 - 4\lambda^3 = 12 + 16\lambda +$$

$$+4\lambda^2 - 4\lambda^3 + 4\lambda = -4\lambda(\lambda+1)(\lambda-1) + 4\left(\lambda^2+4\lambda+3\right) = (\lambda+1)\left(-4\lambda^2+4\lambda+4\lambda+12\right) =$$

$= -4(\lambda+1)^2(\lambda-3)$. Многочлен имеет кратные корни, если $\operatorname{Re} z\left(P(x), Q(x)\right) = 0 \Rightarrow$

$-4(\lambda+1)^2(\lambda-3) = 0$, значит $\lambda_1 = -1,\ \lambda_2 = 3$.

Рассмотрим многочлен $P(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$, тогда его дискриминант можно найти таким образом: $Dis = (-1)^{\frac{n(n-1)}{2}} \dfrac{\operatorname{Re} z\left(P(x), P'(x)\right)}{a_0}$.

§ 17. Алгебраическая замкнутость поля

Можно дать несколько определений алгебраической замкнутости поля. Поле P *алгебраически замкнуто*, если кольцо многочленов $P[x]$ над этим полем содержит неприводимые многочлены только первого порядка.

Поле P *алгебраически замкнуто*, если у любого многочлена из $P[x]$ существует хотя бы один корень.

Поле P *алгебраически замкнуто*, если любой многочлен из $P[x]$ n-ого порядка имеет ровно n корней с учетом кратности.

Например, поля Q, R не являются алгебраически замкнутыми, так как многочлен x^2+1 в этих полях не имеет корней.

Лемма 1 (о модуле старшего члена).

Пусть дан многочлен $P(z)$ *с комплексными коэффициентами* $P_n(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n, a_i \in \mathbb{C}$. *Существует* $r \in \mathbb{R}$ *такое, что* $\forall z \in \mathbb{C}$, $|z| > r$ *выполнено* $|a_0 z^n| > |a_1 z^{n-1} + \ldots + a_n|$.

Доказательство.

Пусть $A = \max_i \{|a_i|\}$, выберем $r = \frac{A}{|a_0|} + 1$. $|z| > \frac{A}{|a_0|} + 1 \Rightarrow |z| - 1 > \frac{A}{|a_0|} \Rightarrow |a_0| > \frac{A}{|z| - 1}$.

Тогда

$$|a_0 z^n| > \frac{A}{|z|-1}|z^n| > \frac{A\left(|z|^n - 1\right)}{|z|-1} = A\left(|z|^{n-1} + |z|^{n-2} + \ldots + |z| + 1\right) = A\left(|z|^{n-1}\right) +$$

$$+ A\left(|z|^{n-2}\right) + \ldots + A\left(|z|\right) + A \geq |a_1|\left(|z|^{n-1}\right) + |a_2|\left(|z|^{n-2}\right) + \ldots + |a_{n-1}|\left(|z|\right) + |a_n| \geq \geq |a_1 z^{n-1} + \ldots + a_{n-1} z + a_n|.$$

Получено, что $|a_0 z^n| > |a_1 z^{n-1} + \ldots + a_n|$. Лемма доказана.

Лемма 2.

Любой многочлен $P(z)$ *нечетной степени с вещественными коэффициентами имеет хотя бы один вещественный корень.*

Доказательство.

По лемме 1 $\exists\, r \in \mathbb{R} : |a_0 r^n| > |a_1 r^{n-1} + \ldots + a_n| \Rightarrow$ многочлены $P(z)$ и $|a_0 r^n|$ будут иметь одинаковые знаки на концах отрезка $[-r, r]$. Функция $a_0 z^n$ на концах отрезка имеет разные знаки $\Rightarrow$ по теореме о прохождении непрерывной функции через нуль при смене знака данная функция в некоторой точке будет иметь нулевое значение $\Rightarrow$ многочлен $P(z)$ тоже будет иметь нулевую точку, то есть некоторый корень. Лемма доказана.

Пусть имеем некоторое кольцо многочленов $P[x]$. Рассмотрим такое факторкольцо: $P[x]/f(x)P[x]$, где $f(x)P[x]$ – главный идеал. Это факторкольцо состоит из элементов вида $\overline{g} = g + (f)$, где $g \in P[x]$, (f) – все элементы, принадлежащие идеалу. Данное факторкольцо будет полем в зависимости от многочлена $f(x)$.

Теорема 1.

Факторкольцо $P[x]/f(x)P[x]$ *является полем тогда и только тогда, когда* $f(x)$ –

неприводимый многочлен над полем

Доказательство.

1) f – приводимый многочлен, то есть $f = f_1 f_2$. Рассмотрим такие элементы $\overline{f_1} = f_1 + (f)$, $\overline{f_2} = f_2 + (f)$, где f_1, f_2 – некоторые элементы кольца многочленов, $\overline{f_1}, \overline{f_2}$ – все элементы факторкольца. Перемножим их $\overline{f}_1 \overline{f_2} = f_1 f_2 + (f) f_2 + (f) f_1 + (f)(f) = (f)$, так как $f_1 f_2 = f = 0$, если рассматривать его относительно идеала, то $\overline{f}_1 \overline{f_2} = (f)$. Тогда $\overline{f}_1 \overline{f_2} = 0$ по модулю (f). Значит, в факторкольце имеются делители нуля $\Rightarrow$ факторкольцо не является полем.

2) Пусть $f(x)$ – неприводимый многочлен. Выберем любой многочлен $h(x) \in P[x]$, такой что НОД$(h(x), f(x)) = 1$. Тогда существует разложение: $u(x)h(x) + v(x) f(x) = 1$. Рассмотрим это равенство в факторкольце, то есть по модулю $\overline{f}$. Это разложение примет вид $\overline{u}\,\overline{h} = 1$, то есть все элементы (кроме нулевого) обратимы, значит, факторкольцо является полем.

Кроме того, элемент $\overline{x} = x + (f)$ является в полученном кольце корнем $f(x)$: $f(\overline{x}) = 0$, так как $\overline{a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n} = \overline{a_0 x^n} + \ldots + \overline{a_n} = a_0 \overline{x}^n + a_n$.

Можно сделать такой вывод: если $f(x)$ – неприводимый многочлен, то $P[x]/f(x)P[x]$ – поле с корнем $f(x)$.

Пусть дано поле P и многочлен $f(x) = x^n + \ldots + a_n$. Поле F, в котором многочлен раскладывается на линейные множители $f(x) = (x - c_1) \cdot \ldots \cdot (x - c_n)$ и $F = P \cup \{c_1, \ldots, c_n\} = P(c_1, \ldots, c_n)$ называется *полем разложения многочлена*.

Теорема 2.

У любого многочлена имеется свое поле разложения.

Доказательство.

Рассмотрим многочлен $f(x) = f_1(x) \cdot \ldots \cdot f_k(x)$. Рассмотрим факторкольцо $P[x]/f_1(x)P[x] = P_1$, причем в нем имеется какой-то из корней $f_1(x)$. Значит, $f(x)$ раскладывается в P_1 на такие множители: $f(x) = (x - c_1) g_1(x) f_2(x) \ldots \cdot f_k(x)$.

Рассмотрим такое факторкольцо: $P_1[x]/g_1(x)P_1[x] = P_2$. Ему принадлежит корень многочлена $g_1(x)$. Таким образом можно разложить весь многочлен $f_1(x)$. Выполним те же действия для многочленов $f_2(x),\ldots,f_k(x)$. Получим вложенную систему полей $P \subset P_1 \subset P_2 \subset \ldots \subset P_s$, причем последнее будет являться полем разложения для данного многочлена $f(x)$.

Теорема (основная теорема алгебры).

Поле С является алгебраически замкнутым.

Доказательство.

1) Пусть многочлены имеют вещественные коэффициенты. Докажем теорему методом математической индукции. Рассмотрим многочлен $f(z) = a_0 z^n + a_1 z^{n-1} + \ldots + a_{n-1}z + a_n, a_i \in \square$. Запишем его порядок так: $\deg f(z) = 2^m k$, где k – нечетное число.

Проведем индукцию по переменной m.

1. $m = 0$, тогда $\deg f(z) = k$. Согласно лемме 2 $f(z)$ имеет хотя бы один вещественный корень.

2. Предположим, что любой многочлен, порядок которого $\deg f(z) = 2^m k$, где $m \le m_0$ имеет хотя бы один комплексный корень.

3. Рассмотрим многочлен $(x^2+1)f(x)$ и его поле разложения, которое существует по теореме 2, причем поле $\square$ включено в это поле разложения. Значит, в этом поле многочлен имеет $\underbrace{2^m k}_{n} + 2$ корней. Выпишем их: $u_1, u_2, \ldots, u_n, i, -i$.

Рассмотрим такие числа $v_{ij} = u_i u_j + a(u_i + u_j)$ и такой многочлен $\prod_{1\le i,j\le n}(x - v_{ij})$. Найдем порядок многочлена: $\deg \prod_{1\le i,j\le n}(x - v_{ij}) = \frac{n(n-1)}{2} = \frac{2^m k(2^m k - 1)}{2} = 2^{m-1}k(2^m k - 1)$, причем $k(2^m k - 1)$ – нечетное число. Тогда, применяя предположение индукции можно утверждать, что данный многочлен имеет хотя бы один комплексный корень.

Многочлен $\prod_{1\le i,j\le n}(x - v_{ij})$ является симметрическим относительно u_i, u_j, а любой симметрический многочлен представляется в виде функции от элементарных

многочленов $\Rightarrow$ это многочлен с вещественными коэффициентами. Вместо коэффициента a в v_{ij} можно рассматривать любые числа, например, a_1 может соответствовать v_{12}, $a_2 \to v_{35}$ и так далее. Таких a_i бесконечное число, а чисел v_{ij} ограниченное число – $\frac{n(n-1)}{2}$. Значит, существуют такие значения a_i, что им будут соответствовать такие v_{ij}: $a_1 \to v_{12}$, $a_2 \to v_{12}'$, причем $v_{12} = u_1u_2 + a_1(u_1+u_2)$, $v_{12}' = u_1u_2 + a_2(u_1+u_2)$. Тогда $u_1u_2 = \frac{a_2v_{12} - a_1v_{12}'}{a_2 - a_1}$, $u_1 + u_2 = \frac{v_{12} - v_{12}'}{a_1 - a_2} \Rightarrow u_1, u_2$ – корни уравнения $x^2 + \underbrace{\frac{v_{12} - v_{12}'}{a_2 - a_1}}_{b} x + \underbrace{\frac{a_2v_{12} - a_1v_{12}'}{a_2 - a_1}}_{c} = 0$, значит, $u_{1,2} = \frac{-b \pm \sqrt{D}}{2a} \in \square$ и является корнем исходного многочлена. Индукционный переход доказан.

2) Пусть многочлены имеют комплексные коэффициенты, то есть $f(z) = a_0z^n + a_1z^{n-1} + \ldots + a_{n-1}z + a_n, a_i \in \square$. Рассмотрим сопряженный многочлен $\overline{f(z)}$, тогда многочлен $f(z)\overline{f(z)}$ имеет вещественные коэффициенты, так как $\overline{f(z)\overline{f(z)}} = f(z)\overline{f(z)} \Rightarrow$ по первой части теоремы у него существует хотя бы один вещественный корень: $f(c)\overline{f(c)} = 0$. Возможны случаи:

1. $f(c) = 0$, тогда получаем, что найден корень.
2. $\overline{f(c)} = 0$, тогда $f(\overline{c}) = 0$, получаем, что найден корень причем $\overline{c} \in \square$

Значит, у любого многочлена имеется хотя бы один комплексный корень. Теорема доказана.

Следствие.

Любой многочлен с вещественными коэффициентами разлагается в произведение линейных многочленов над полем $\square$ *и в произведение линейных и квадратичных с* $Dis < 0$ *над полем* $\square$.

Доказательство.

Рассмотрим многочлен $a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, a_i \in \square$. Тогда $x = u \pm v_i$ – его корни.

Получаем, что $\left(x-\left(u+v_i\right)\right)\left(x-\left(u-v_i\right)\right)=x^2+2ux+u^2+v^2$. Свойство доказано.

§ 18. Корни многочленов

Корни многочленов небольших порядков можно найти несколькими способами. Рассмотрим их.

1) Пусть дан многочлен $a_0x^3+a_1x^2+a_2x+a_3$. Тогда его корни возможно найти из уравнения $a_0x^3+a_1x^2+a_2x+a_3=0\Rightarrow x^3+\frac{a_1}{a_0}x^2+\frac{a_2}{a_0}x+\frac{a_3}{a_0}=0\Rightarrow x^3+ax^2+bx+c=0$. То есть задача нахождения корней многочлена $a_0x^3+a_1x^2+a_2x+a_3$ свелась к задаче нахождения корней многочлена x^3+ax^2+bx+c, где $a=\frac{a_1}{a_0},\ b=\frac{a_2}{a_0},\ c=\frac{a_3}{a_0}$.

Сделаем замену $x=t+\alpha$ и выберем $\alpha=-\frac{a}{3}$, тогда получим уравнение такого вида $x^3+px+q=0\Rightarrow x^3-a^3-b^3-3ab\,x=0$. По формулам Виета:

$$\begin{cases}q=-a^3-b^3\\ p=-3ab\end{cases},\ \begin{cases}q=-\left(a^3+b^3\right)\\ p^3=-27a^3b^3\end{cases}.$$

Тогда

$$\begin{cases}\left(a^3+b^3\right)=-q\\ a^3b^3=-\frac{p^3}{27}\end{cases}\Rightarrow a^3,b^3$$

– корни уравнения

$$t^2+qt-\frac{p^3}{27}=0\Rightarrow t_{1,2}=\frac{-q\pm\sqrt{q^2+\frac{4p^3}{27}}}{2}=$$

$$=-\frac{q}{2}\pm\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}\Rightarrow a=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},b=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

Решив уравнение $x^3-a^3-b^3-3ab\,x=0$, получим, что $x=a+b$. Сделав подстановку, получим $x=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}$ – *формула Кардано.*

Формула Кардано дает девять решений. Она была модифицирована Эйлером: должно выполняться условие $ab=-\frac{p}{3}$, тогда получим ровно три корня.

2) Рассмотрим многочлен $x^3 + px + q$. Его дискриминант:

$$Dis = \begin{vmatrix} 3 & p_1 & p_2 \\ p_1 & p_2 & p_3 \\ p_2 & p_3 & p_4 \end{vmatrix}.$$

Тогда

$$p_1 = 0, p_2 = -2p,\ p_3 = -3q,\ p_4 = 2p^2 \Rightarrow Dis = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} = -108\left(\frac{p^3}{27} + \frac{q^2}{4}\right).$$

Возможны следующие случаи:

1. $Dis < 0$, то есть $\frac{p^3}{27} + \frac{q^2}{4} > 0 \Rightarrow$ многочлен имеет один вещественный корень и два комплексных.

2. $Dis = 0 \Rightarrow \frac{p^3}{27} + \frac{q^2}{4} = 0 \Rightarrow$ все три корня вещественные, причем хотя бы два из них совпадают.

3. $Dis > 0 \Rightarrow \frac{p^3}{27} + \frac{q^2}{4} < 0 \Rightarrow$ многочлен имеет три различных вещественных корня.

3) Рассмотрим многочлен четвертой степени: $a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$. Приведем многочлен к виду $x^4 + ax^3 + bx^2 + cx + d = 0$. Сделаем такую замену, чтобы избавиться от x^3. Пусть $x = t + \alpha$: $(t+\alpha)^4 + a(t+\alpha)^3 + b(t+\alpha)^2 + c(t+\alpha) + d =$

$= (t^2 + 2\alpha t + \alpha^2)(t^2 + 2\alpha t + \alpha^2) + a(t^3 + 3t^2\alpha + 3t\alpha^2 + \alpha^3) + b(t^2 + 2\alpha t + \alpha^2) + c(t+\alpha) + d = 0$. То есть при $\alpha = -\frac{a}{4} \Rightarrow$ получим многочлен вида $x^4 + px^2 + qx + s = 0$. Выделим полный квадрат, где α – некоторое неизвестное число:

$$\left(x^2 + \frac{p}{2} + \alpha\right)^2 + qx + s - 2\alpha x^2 - p\alpha - \frac{p^2}{4} - \alpha^2 = 0,$$

$$\left(x^2 + \frac{p}{2} + \alpha\right)^2 - \left(2\alpha x^2 - qx + \left(p\alpha + \frac{p^2}{4} + \alpha^2 - s\right)\right) = 0.$$

Число α следует выбрать так, чтобы второе слагаемое представляло собой полный квадрат, то есть, чтобы его дискриминант равнялся нулю: $Dis = q^2 - 4 \cdot 2\alpha\left(p\alpha + \frac{p^2}{4} + \alpha^2 - s\right) = 0 \Rightarrow$ получено кубическое уравнение относительно

α, имеющее хотя бы один вещественный корень. Возьмем этот корень и свернем вторую скобку: $\left(x^2+\frac{p}{2}+\alpha_*\right)^2-\left(\sqrt{2\alpha_*}x-\frac{q}{2\sqrt{2\alpha_*}}\right)^2=0\Rightarrow$ получена разность квадратов:

$$\left(x^2+\frac{p}{2}+\alpha_*+\sqrt{2\alpha_*}x-\frac{q}{2\sqrt{2\alpha_*}}\right)\times\left(x^2+\frac{p}{2}+\alpha_*-\sqrt{2\alpha_*}x+\frac{q}{2\sqrt{2\alpha_*}}\right)=0.$$

Далее приравниваем каждую скобку к нулю, решаем два уравнения и получаем четыре корня. Данный метод решения называется методом Феррари.

4) Уравнения пятой степени и выше в общем виде решить не удается.

§ 19. Локализация корней.

Рассмотрим несколько методов определения интервалов, в которых находятся корни многочленов.

1) Пусть имеется многочлен

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

По лемме о модуле старшего члена все корни многочлена не превосходят числа

$$\frac{A}{a_0}+1\Rightarrow\ x<\frac{A}{a_0}+1.$$

Получена верхняя оценка интервала, в котором лежат его положительные корни. Рассмотрим многочлен

$$x^nP\left(\frac{1}{x}\right)=a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n.$$

Его корни:

$$\frac{1}{x}<\frac{A}{a_n}+1\Rightarrow\ x>\frac{1}{\frac{A}{a_n}+1}$$

– нижняя оценка. Аналогично строится оценка для отрицательных корней с помощью многочленов $P(-x)$ и $x^nP\left(-\frac{1}{x}\right)$.

Пример.

Оценить корни многочлена $P(x)=x^4+x^3+2x^2-x+2$.

Решение.

1. Оценка положительных корней. Сверху: $x<3$. Снизу: $x^nP\left(\frac{1}{x}\right)=1+x+2x^2-$

$-x^3+2x^4 \Rightarrow \frac{1}{x}<\frac{5}{2} \Rightarrow x>\frac{2}{5} \Rightarrow x \in \left(\frac{2}{5};3\right)$.

2. Оценка отрицательных корней. Снизу: $x>-3$. Сверху: $x^n P\left(-\frac{1}{x}\right)=1-x+2x^2+$

$+x^3+2x^4 \Rightarrow -\frac{1}{x}<\frac{5}{2} \Rightarrow x<-\frac{2}{5} \Rightarrow x \in \left(-3;-\frac{2}{5}\right)$.

2) Метод Ньютона

Пусть имеем многочлен $P(x)=x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$ и найдена такая точка $x=c$, что $P(c)>0,\ P'(c)>0,\ldots,\ P^{(n)}(c)>0$. В этом случае при $x \geq c$ многочлен не будет иметь корней.

3) Правило знаков Декарта

Пусть дан многочлен $P(x)$. Рассмотрим ненулевые коэффициенты многочленов $P(x)$ и $P(-x)$, и найдем число смен знаков в этих последовательностях. Тогда количество положительных корней $P(x)$ равно числу смен знаков коэффициентов многочлена $P(x)$, либо меньше его на четное число. Аналогично для отрицательных корней многочлена $P(x)$. Например, пусть дан многочлен $P(x)=5x^4-3x^2+2x^3-x+1$, тогда получим такую последовательность $5,-3,2,-1,1$. Число смен знаков равно четырем, значит количество положительных корней равно либо четырем, либо двум, либо нулю. $P(-x)=5x^4+3x^2+2x^3+x+1 \Rightarrow 5,3,2,1,1$. Число смен знаков равно нулю, значит, отрицательных корней многочлен не имеет.

Теорема.

Если все корни многочлена вещественные, то число положительных корней равно числу смен знака в последовательности коэффициентов рассматриваемого многочлена.

4) Оценка корней с помощью производной

Например, если $P(x)=x^5+4x^3+2x \Rightarrow \quad P'(x)=5x^4+12x^2+2$, тогда $P'(x)>0 \ \forall x$. Получено, что функция x^5+4x^3+2x возрастает. Значит, уравнение имеет ровно один

вещественный корень и четыре комплексных. Причем корень такой $P(0)=0$.

5) Метод Штурма

Этот метод применим только для многочленов, не имеющих кратных корней. Поэтому рассматриваем многочлен такого вида $\frac{P(x)}{НОД\left(P(x),P'(x)\right)}$. Он имеет те же корни, что и $P(x)$, но единичной кратности .

Система Штурма – это множество функций $f(x),\ f_1(x),\ldots,\ f_k(x)$, для которых выполняются следующие условия:

1. $f_i(x)$ и $f_{i+1}(x)$ не имеют общих корней.
2. $f_k(x)$ не имеет вещественных корней.
3. Если $f_i(\alpha)=0$, тогда $f_{i-1}(\alpha)\,f_{i+1}(\alpha)<0$.
4. Если $f(\alpha)=0$, то произведение $f(x)\,f_1(x)$ в точке $x=\alpha$ меняет знак.

Возьмем любое число α и подставим в эту систему Штурма: $f(\alpha),,\ldots,\ f_k(\alpha)$. Получим величину $w(\alpha)$ – число смен знака в точке $x=\alpha$. Тогда число корней на отрезке $[a,b]=w(a)-w(b)$.

Рассмотрим конкретный пример системы Штурма: $f(x)$ – исходный многочлен; $f_1(x)=P'(x)$. Разложим $f(x)$ таким образом: $f(x)=f_1(x)g_1(x)+r_1(x)$, тогда $f_2(x)=-r_1(x)$. Аналогично получаем $f_3(x)=-r_2(x)$, где $f_1(x)=f_2(x)g_2(x)+r_2(x)$. И так далее получаем остальные функции системы Штурма.

Пример.

Построим систему Штурма: $f(x)=x^4-x-1,\ f_1(x)=4x^3-1,\ f_2(x)=3x+4,\quad f_3(x)=1$.

Подставим различные a:

a	Последовательность				$w(a)$
$+\infty$	+	+	+	+	0
$-\infty$	+	–	–	+	2
0	–	–	+	+	1
1	–	+	+	+	1
2	+	+	+	+	0

-1	$+$	$-$	$+$	$+$	2

Получаем, что на отрезке $[-\infty;+\infty]$ имеется ровно два корня, причем один из них принадлежит отрезку $[1;2]$, а другой отрезку $[-1;0]$

§ 20. Поле из четырех элементов

Рассмотрим поле Z_2 и кольцо многочленов $Z_2[x]$ над этим полем. Фактор-кольцо $Z_2[x]/(x^2+x+1)Z_2[x]$ является полем, т.к. многочлен x^2+x+1 неприводим над полем Z_2. В получившемся поле ровно четыре элемента.

Уравнение $x^2+x+1=0$ в поле Z_2 не имеет решений, найдем корень этого уравнения и добавим его к элементам поля Z_2: $Z_2(\alpha)=\{0,1,\alpha,\alpha+1\}$.

Т.к. α – корень многочлена x^2+x+1, то можно получить:

1) $x^2+x+1=(x-\alpha)(x-(\alpha+1))=x^2-\alpha x-(\alpha+1)x+\alpha(\alpha+1)\Rightarrow \alpha(\alpha+1)=1$;

2) $\alpha^2+\alpha+1=0\Rightarrow \alpha^2=-\alpha-1=\alpha+1$;

3) $(\alpha+1)^2+\alpha+1+1=0\Rightarrow (\alpha+1)^2=-\alpha=\alpha$.

Ниже приведены таблицы сложения и умножения.

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

$\times$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Аналогично, поле из 8-ми элементов получается, если к полю Z_2 добавить корни многочлена x^3+x^2+1.

§ 21. Алгебры над полем

Ввиду крайней простоты своего строения векторные пространства не интересны сами по себе, но они служат необходимым фоном для многих алгебраических (и не только алгебраических) теорий. Так, комбинирую понятия векторного пространства и кольца, мы приходим, к важному понятию алгебры.

Алгебра над полем P – пара кольцо $(K,+,\times)$ и векторное пространство над полем P. Причем бинарные операции у кольца и векторного пространства одинаковые, нулевой элемент и базисная область совпадают и выполнена еще одна операция: $\lambda(xy)=(\lambda x)y=x(\lambda y)$, для $\forall\lambda\in P,\forall x,y\in K$.

Алгебра называется *ассоциативной*, если кольцо ассоциативно.

Размерность алгебры – размерность над P векторного пространства.

Алгебра с делением – *тело*.

Примеры:

1) Бинарная алгебра;
2) Множество квадратных матриц с элементами из поля P;
3) Алгебра кватернионов: $H=\square+i\square+j\square+k\square,i,j,k\in Q_8$;
4) Всякое поле L, содержащее K в качестве подполя, можно рассматривать как алгебру над K. В частности, поле $\square$ есть алгебра над $\square$;
5) Пространство E^3 есть алгебра относительно операции векторного умножения;
6) Множество $F(X,K)$ функций на множестве X со значениями в поле K является алгеброй над K относительно обычный операций сложения и умножения функций и умножения функции на число. Эта алгебра коммуникативна, ассоциативна и обладает единицей (каковой является функция, тождественно равная единице).

На алгебры переносятся, с незначительными уточнениями, основные понятия теории колец. Так, *подалгеброй* Алгебры A, считается всякое подкольцо B, являющееся одновременно подпространством векторного пространства A. Если T – подмножество в A, то порожденная им подалгебра $P[T]$ является пересечением всех подалгебр в A, содержащих T. Аналогичным образом определяются идеалы и факторалгебры по ним. Гомоморфизмами алгебр служат гомоморфизмы колец, являющиеся с тем P-линейными отображениями.

Список рекомендованной литературы

Основная литература

1. Кострикин А.И. Введение в алгебру. В 3 частях. – М.: МЦНМО, 2009.

2. Кострикин А.И. Сборник задач по алгебре. – М.: ФИЗМАТЛИТ, 2001.

3. Курош А.Г. Курс высшей алгебры. – СПб.: Лань, 2007.

Дополнительная литература

1. Винберг Э.Б. Курс алгебры. – М.: «Факториал Пресс», 2002.

2. Биркгоф Г., Барти Т. Современная прикладная алгебра. – СПб.: Лань, 2005.

3. Ван дер Варден Б.Л. Алгебра. Определения, теоремы, формулы. – СПб.: Лань, 2004.