СЕМИНАРЫ ПО ДИСКРЕТНОМУ АНАЛИЗУ

Кирилл Чувилин <kirill@chuvilin.pro>
кафедра МОУ МФТИ

http://kirill.chuvilin.pro/wiki/МФТИ/Кафедра_МОУ/Дискретный_анализ_(семестр_2)

2011–2020 гг.

ОГЛАВЛЕНИЕ

1 Понятие группы **3**

1.1 Определение и примеры групп 3

1.2 Изоморфизмы и гомоморфизмы групп 6

2 Порядки элементов. Циклические группы **7**

2.1 Порядки элементов 7

2.2 Циклические группы 8

3 Мультипликативные группы числовых вычетов **11**

3.1 Теорема Эйлера, малая теорема Ферма 12

3.2 Первообразные корни 13

3.3 Квадратичные вычеты 14

4 Симметрические группы **16**

5 Классы смежности. Нормальный делитель **20**

6 Теорема о гомоморфизме **27**

7 Прямая сумма **32**

8 Понятия кольца и поля **36**

9 Кольца и поля вычетов **43**

10 Идеалы **48**

11 Факторкольца **53**

СЕМИНАР 1

ПОНЯТИЕ ГРУППЫ

1.1. Определение и примеры групп

Определение 1.1 (Группа).

Непустое множество G с заданной на нём бинарной операцией $*\colon G \times G \to G$ называется *группой* $< G, * >$, если выполнены следующие аксиомы:

1) ассоциативность: $\forall a, b, c \in G\ (a*b)*c = a*(b*c)$;

2) наличие нейтрального (единичного) элемента: $\exists \iota \in G\colon \forall a \in G\ \iota * a = a * \iota = a$;

3) наличие обратного элемента: $\forall a \in G\ \exists a^{-1} \in G\colon a * a^{-1} = a^{-1} * a = \iota$.

Операция $*$ называется *алгебраической операцией.*

Определение 1.2 (Подгруппа).

Группа $< G', * > —$ *подгруппа* группы $< G, * >$, если $G' \subset G$.

Определение 1.3 (Порядок группы).

Порядком группы $< G, * >$ называется мощность (количество элементов) множества G.

Определение 1.4 (Абелева группа).

Коммутативная группа, т. е. группа, любые два элемента a и b которой перестановочны: $a * b = b * a$.

Не все группы абелевы.

Определение 1.5 (Аддитивная группа).

Группа элементов с операцией сложения.

Определение 1.6 (Мультипликативная группа).

Группа элементов с операцией умножения.

Везде далее, если рассматривается только одна группа с операцией $*$, будут применяться обозначения:

$$ab = a * b, \quad a^0 = \iota, \quad a^k = \underbrace{a * \ldots * a}_{k}, \quad a^{-k} = \underbrace{a^{-1} * \ldots * a^{-1}}_{k}.$$

Упражнение 1.1. Выяснить, образует ли группу каждое из следующих множеств при указанной операции над элементами:

а) целые числа относительно сложения;

б) четные числа относительно сложения;

в) нечетные целые числа относительно сложения;

г) степени действительного числа $a \neq 0$ с целыми показателями $(\ldots, a^{-1}, a^0, a^1, \ldots)$ относительно умножения;

д) остатки от деления на натуральное число n относительно сложения;

е) ненулевые остатки от деления на натуральное число n относительно умножения;

ж) рациональные числа относительно сложения;

з) рациональные числа относительно умножения;

и) рациональные числа, отличные от нуля, относительно умножения;

к) параллельные переносы трехмерного пространства $\mathbb{R}^3$, если за произведение переносов принято их последовательное выполнение.

Ответ: а) да; б) да; в) нет; г) да; д) да; е) да, если n — простое; нет, если n — составное; ж) да; з) нет; и) да; к) да.

Утверждение 1.1. Верхние треугольные матрицы порядка n, все диагональных элементы которых равны 1, образуют мультипликативную группу. Такая группа называется *унитреугольной* и обозначается UT_n.

Утверждение 1.2. Корни n-й степени из единицы (как действительные, так и комплексные) образуют мультипликативную группу.

Пример 1.1. Доказать, что группа корней n-й степени из единицы является единственной мультипликативной группой n-го порядка с числовыми элементами.

Решение. Предположим, что существует некоторая числовая группа порядка n. Рассмотрим произвольный её элемент a порядка k. Тогда $l = \frac{n}{k} \in \mathbb{Z}$, $a^n = a^{kl} = (a^k)^l = 1^l = 1$. Таким образом, a — корень n-й степени из единицы. □

Пример 1.2. Пусть H — конечное подмножество элементов группы $< G, * >$, произведение любых двух элементов которого снова лежит в H. Доказать, что $< H, * >$ — группа.

Решение. Достаточно показать, что $\iota \in H$ и $\forall a \in G\ a^{-1} \in G$.

Пусть $|H| = m$. Если $a \in H$, то $\{a, \ldots, a^{m+1}\} \subset H$. Эти элементы не могут быть все различными, иначе $|H| > m$. Пусть $a^p = a^q$, $p > q$. Тогда $\iota = a^{p-q}$, поэтому $\iota \in H\ a^{-1} = a^{p-q-1}$, поэтому $a^{-1} \in H$. □

Пример 1.3. Доказать, что непустое конечное множество G, в котором определена ассоциативная алгебраическая операция, и каждое из уравнений $ax = b$, $ya = b$ для любых a и b из G имеет в G не более одного решения, будет группой.

Решение. Пусть $G = \{g_1, \ldots, g_n\}$.

Докажем, что уравнения вида $ax = b$ и $ya = b$ имеют решения в G. Рассмотрим произвольный $a \in G$. Пусть $ag_i = b_i$, $i = 1, \ldots, n$. Если для каких-то $i \neq j$ окажется, что $b_i = b_j$, то уравнение $ax = b_i$ имеет в G два решения: g_i и g_j. Значит, $G = \{b_1, \ldots, b_n\}$, и g_i — решение уравнения $ax = b_i$, $i = 1, \ldots, n$. В силу произвольного выбора a получается, что каждое уравнения вида $ax = b$ имеет единственное решение в G. Аналогично показывается, что каждое уравнение вида $ya = b$ имеет единственное решение в G.

Покажем, что в G есть единичный элемент. Рассмотрим произвольный $a \in G$. Пусть $e \in G$ — решение уравнения $ax = a$. Рассмотрим произвольный $b \in G$. Пусть $c \in G$ — решение уравнения $ya = b$. Тогда

$$ae = a \Rightarrow c(ae) = ca \Rightarrow (ca)e = ca \Rightarrow be = b.$$

В силу произвольности выбора b, $\forall b \in G\ be = b$. В частности, $ee = e$. Пусть $d \in G$ — решение уравнения $ex = b$. Тогда

$$ee = e \Rightarrow (ee)d = ed \Rightarrow e(ed) = ed \Rightarrow eb = b.$$

В силу произвольности выбора b, $\forall b \in G\ eb = b$. Значит, $\forall b \in G\ be = eb = b$, т. е. e — единичный элемент.

Остается проверить существование обратного. Рассмотрим произвольный $a \in G$. Пусть $b \in G$ — решение уравнения $ax = e$, а $c \in G$ — решение уравнения $ya = e$. Тогда

$$b = eb = (ca)b = c(ab) = ce = c.$$

Таким образом, $b = c = a^{-1}$. □

1.2. Изоморфизмы и гомоморфизмы групп

Определение 1.7 (Гомоморфное отображение групп).

Отображение $\varphi\colon G_1 \to G_2$ группы $< G_1, * >$ в группу $< G_2, \circ >$ называется *гомоморфизмом*, если $\forall a_1, a_2 \in G_1\ \varphi(a_1 * a_2) = \varphi(a_1) \circ \varphi(a_2)$.

Определение 1.8 (Изоморфное отображение групп).

Взаимно однозначный гомоморфизм $\varphi\colon G_1 \to G_2$ называется *изоморфизмом*. Группы, между которыми можно установить изоморфное отображение, называются *изоморфными*.

Упражнение 1.2. Доказать, что группы (а), (б) и (г) из упражнения 1.1 изоморфны.

Пример 1.4. Изоморфны ли группы:

а) $< \mathbb{R}, + >$ и группа положительных действительных чисел с операцией умножения;

б) $< \mathbb{Q}, + >$ и группа положительных рациональных чисел с операцией умножения?

Решение.

а) Рассмотрим отображение $\varphi\colon \mathbb{R} \to \mathbb{R}_+$ такое, что $\forall x \in \mathbb{R}\ \varphi(x) = 2^x$. Отображение обратимо: $\forall y \in \mathbb{R}_+\ \varphi^{-1}(y) = \log_2 y$, поэтому является биекцией. Кроме того, оно является гомоморфизмом: $\forall x_1, x_2 \in \mathbb{R}\ \varphi(x_1 + x_2) = 2^{x_1+x_2} = 2^{x_1} \cdot 2^{x_2} = \varphi(x_1)\varphi(x_2)$. Поэтому φ задаёт изоморфизм указанных групп.

б) Предположим, что существует изоморфизм $\varphi\colon \mathbb{Q} \to \mathbb{Q}_+$. В частности, это означает, что $\exists x \in \mathbb{Q}\colon \varphi(x) = 2$. Тогда $2 = \varphi(\frac{x}{2} + \frac{x}{2}) = \varphi(\frac{x}{2})\varphi(\frac{x}{2}) \Rightarrow \varphi(\frac{x}{2}) = \sqrt{2} \notin \mathbb{Q}_+$. Полученное противоречие означает, что такого изоморфизма не может существовать.

□

СЕМИНАР 2

ПОРЯДКИ ЭЛЕМЕНТОВ. ЦИКЛИЧЕСКИЕ ГРУППЫ

2.1. Порядки элементов

Определение 2.1 (Порядок элемента группы).

Пусть a — некоторый элемент группы $< G, * >$. *Порядком элемента* a называется минимальное натуральное число k такое, что $a^k = \iota$. Если такого числа не существует, то говорят, что элемент имеет *бесконечный порядок*.

Пример 2.1. Доказать, что если любой элемент группы имеет порядок 2, то эта группа абелева.

Решение. Пусть a и b — два произвольных элемента группы. Тогда

$$ab = ab\iota = ab(aa) = aba(bb)a = (ab)(ab)ba = (ab)^2ba = \iota ba = ba.$$

□

Упражнение 2.1. Доказать, что элементы ab и ba имеют один и тот же порядок.

Утверждение 2.1. Порядок любого элемента группы является делителем порядка группы.

Доказательство. ... □

Пример 2.2. Доказать, что в группе нечётного порядка все элементы являются квадратами.

Решение. Так как порядок элемента должен быть делителем порядка группы, то все элементы имеют нечетные порядки. Пусть $a^{2p+1} = \iota$. Тогда $a = a^{(2p+1)+1} = (a^{p+1})^2$. □

Упражнение 2.2. Найти все подгруппы группы порядка 8, все не нейтральные элементы которых имеют порядок 2.

Пример 2.3. Пусть порядок элемента x равен n. Найти порядок элемента x^k.

Р е ш е н и е. Пусть m — порядок x^k, НОД$(n,k) = d$, $n = n_1 d$, $k = k_1 d$. Тогда $\iota = (x^k)^m = = x^{k_1 dm}$. Это означает, что n — делитель $k_1 dm$, т. е. n_1 — делитель $k_1 m$, и , поскольку НОД$(n_1, k_1) = 1$, n_1 — делитель m. Поэтому минимальное подходящее $m = n_1 = \frac{n}{\text{НОД}(n,k)}$. □

2.2. Циклические группы

Определение 2.2. Группой, *порождённой множеством элементов*, называется минимальная группа, содержащая все элементы этого множества.

Определение 2.3 (Циклическая группа $< a >$, C_n).

Если для некоторого элемента a группы $< G, * >$ выполнено

$$\forall b \in G \ \exists k \in \mathbb{Z} \colon a^k = b,$$

то говорят, что *группа* $< G, * >$ *порождена элементом* a *и операцией* $*$. Такая группа называется *циклической* и обозначается $< a >$.

Если элемент a имеет конечный порядок n, то он называется *образующим* элементом, а группа состоит из элементов $\{\iota, a^1, \ldots, a^{n-1}\}$, тоже имеет порядок n и обозначается C_n.

Утверждение 2.2. Циклические группы всегда абелевы.

Д о к а з а т е л ь с т в о. Пусть b и c — произвольные элементы группы $< a >$. Значит, есть такие целые p и q, что $b = a^p$, $c = a^q$. Тогда $bc = a^p a^q = a^{p+q} = a^{q+p} = a^q a^p = cb$. □

Упражнение 2.3. Найти все порождающие элементы аддитивной группы целых чисел.
О т в е т : 1 и -1.

Определение 2.4 (Аддитивная группа вычетов по модулю n — $\mathbb{Z}_n$).

Пусть n — натуральное число. *Аддитивной группой вычетов по модулю* n называется множество $\{0, \ldots, n-1\}$ с алгебраической операцией $*$, определяемой следующим образом:

$$a * b = c \Longleftrightarrow a + b \equiv c \pmod{n}.$$

Утверждение 2.3. Все конечные циклические группы порядка n изоморфны аддитивной группе вычетов по модулю n. Все бесконечные циклические группы изоморфны аддитивной группе целых чисел.

Упражнение 2.4. Найти все изоморфизмы между группами $< \mathbb{Z}_4, + >$ и $< \mathbb{Z}_5, \times >$.

Р е ш е н и е. Пусть φ — такой изоморфизм и $\varphi([1]_4) = x$. Значит, x имеет порядок порядок 4. В $< \mathbb{Z}_5, \times >$ такой порядок имеют только элементы $[2]_5$ и $[3]_5$. Поэтому возможны два варианта: $\varphi([k]_4) = [2]_5^k$ и $\varphi([k]_4) = [3]_5^k$ □

Пример 2.4. Пусть $< a >= C_n$ и $b = a^k$. Доказать, что элемент b тогда и только тогда будет образующим группы $< a >$, когда числа n и k взаимно просты.

Р е ш е н и е. В примере 2.3 было показано, что порядок элемента b равен $\frac{n}{\text{НОД}(n,k)}$. Взаимная простота n и k означает, что $\operatorname{ord} b = n$. Таким образом, степени элемента b формируют все n элементов $< a >$. □

Упражнение 2.5. Найти все подгруппы циклической группы порядка 6.

Определение 2.5 (Примарная циклическая группа).

Циклическая группа порядка p^n, где p — простое число, $n \in \mathbb{N}$.

Упражнение 2.6. Найти все подгруппы примарной циклической группы порядка p^n.

Пример 2.5. Доказать утверждения:

а) любая подгруппа C_n циклическая;

б) порядок любой подгруппы C_n является делителем n (не используя теорему Лагранжа и её следствия);

в) для любого делителя d числа n существует единственная подгруппа, имеющая порядок d.

Р е ш е н и е. Пусть $< G, * >$ — подгруппа порядка m группы $C_n =< a >$, состоящая из элементов $\iota, a^{k_1}, \ldots, a^{k_{m-1}}$.

а) Пусть $p = \text{НОД}(k_1, \ldots, k_{m-1})$, тогда найдутся такие коэффициенты $\alpha_1, \ldots, \alpha_{m-1} \in \mathbb{Z}$, что $\alpha_1 k_1 + \ldots + \alpha_{m-1} k_{m-1} = p$ (вычислить подходящие $\alpha_1, \ldots, \alpha_{m-1}$ можно с помощью расширенного алгоритма Евклида). Это означает, что $a^p \in G$, т. е. $< G, * >= =< a^p >$. Таким образом, все подгруппы циклической группы тоже циклические.

б) Рассмотрим произвольную подгруппу $< a^p >$ группы $< a >$. Её порядок d совпадает с порядком элемента a^p, Это означает, что $(a^p)^d = \iota$ и $\forall d_1 \in \mathbb{N}\ d_1 < d \to (a^p)^{d_1} \neq \iota$.

Пусть r — остаток от деления n на d, т. е. $n = kd + r$, $k, r \in \mathbb{Z}$, $0 \leqslant r < d$. Тогда

$$(a^p)^r = a^{p(n-kd)} = a^{np} a^{-kpd} = (a^n)^p ((a^p)^d)^{-k} = \iota^p \iota^{-k} = \iota.$$

Это возможно только если $r = 0$, т. е. $n = kd$. Значит, d — делитель n.

в) Покажем, что $< a^p >=< a^k >$. Пусть q — остаток от деления p на k, т. е. $p = lk + q$, $l, q \in \mathbb{Z}$, $0 \leqslant q < k$. Тогда

$$a^{qd} = a^{(p-lk)d} = a^{pd}a^{-kdl} = (a^p)^d(a^n)^{-l} = \iota^d\iota^{-l} = \iota,$$

при этом $qd < kd = n$. Это возможно только если $q = 0$, т. е. $p = lk$. Последнее равенство означает, что $a^p = (a^k)^l \Rightarrow a^p \in < a^k > \Rightarrow < a^p > \subset < a^k >$. Но, поскольку $| < a^p > | = d = | < a^k > |$, то $< a^p >=< a^k >$.

□

СЕМИНАР 3

МУЛЬТИПЛИКАТИВНЫЕ ГРУППЫ ЧИСЛОВЫХ ВЫЧЕТОВ

Определение 3.1 (Мультипликативная группа вычетов по модулю n — $U(\mathbb{Z}_n)$)**.**

Пусть $n \in \mathbb{N}$, $n > 1$. *Мультипликативной группой вычетов по модулю* n называется множество обратимых элементов аддитивной группы $\mathbb{Z}_n$ вычетов по модулю n

$$U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n |\ \exists y \in \mathbb{Z}_n \colon xy \equiv 1 \mod n\}.$$

с алгебраической операцией $*$, определяемой следующим образом:

$$a * b = c \iff a \cdot b \equiv c \mod p.$$

Покажем, что определение корректно. Для этого докажем следующие факты.

Утверждение 3.1. $k \in \mathbb{Z}_n$ обратим тогда и только тогда, когда $\text{НОД}(k, n) = 1$.

Доказательство. Пусть $\text{НОД}(k, n) = 1$. Из примера 2.4 следует, что k является образующим элементом аддитивной группы $\mathbb{Z}_n$. Это означает, что найдётся $q \in \mathbb{N}$ такое, что $\underbrace{k + \ldots + k}_{q} \equiv 1 \mod n$. Возьмём $r \in \mathbb{Z}_n \colon r \equiv q \mod n$. Тогда $rk \equiv qk \equiv 1 \mod n$, т. е. k обратим.

Обратно, если $\text{НОД}(k, n) = d > 1$, то $k = k'd$, $n = n'd$ $(k', n' \in \mathbb{Z}_n)$. Если бы k был обратим, то $n' \equiv (k^{-1}k)n' \equiv k^{-1}k'(dn') \equiv (k^{-1}k')n \equiv 0 \mod n$. □

Из этого утверждения следует замкнутость операции $*$, поскольку для целых чисел

$$\text{НОД}(k, n) = \text{НОД}(m, n) = 1 \iff \text{НОД}(km, n) = 1.$$

Наличие единичного элемента в $U(\mathbb{Z}_n)$ очевидно: $1 * 1 = 1$. Наличие обратного следует из определения $U(\mathbb{Z}_n)$. Ассоциативность операции $*$ следует из ассоциативности операции умножения.

В частном случае, когда p — простое натуральное число, $U(\mathbb{Z}_p)$ состоит из всех положительных вычетов по модулю p, и $|U(\mathbb{Z}_p)| = p - 1$.

В общем случае для вычисления количества элементов $U(\mathbb{Z}_n)$ используется следующая функция.

Определение 3.2 (Функция Эйлера — $\varphi(n)$)**.**

Пусть $n \in \mathbb{N},\ n > 1$. Тогда $\varphi(n)$ — количество натуральных чисел меньших n взаимно простых с n.

Основные свойства, позволяющие рекурсивно вычислять $\varphi(n)$, следующие:

1) $\varphi(p^k) = p^k - p^{k-1}$, где p — простое натуральное число;

2) $\varphi(n,m) = \varphi(n)\varphi(m)$, если НОД$(n,m) = 1$.

Упражнение 3.1. Найти порядок $U(\mathbb{Z}_{72})$.

Ответ: 24.

3.1. Теорема Эйлера, малая теорема Ферма

Теорема 3.1 (Теорема Эйлера)**.**

Пусть $a, n \in \mathbb{N},\ \text{НОД}(a,n) = 1,\ n > 1$. Тогда $a^{\varphi(n)} \equiv 1 \mod n$.

Доказательство. Пусть r — остаток от деления a на n. Тогда НОД$(r,n) = 1$, поэтому $r \in U(\mathbb{Z}_n)$. Обозначим через k порядок r в $U(\mathbb{Z}_n)$. В силу следствия из теоремы Лагранжа найдётся такое натуральное q, что $\varphi(n) = |U(\mathbb{Z}_n)| = kq$. Тогда по модулю n: $a^{\varphi(n)} \equiv r^{kq} \equiv$ $\equiv (r^k)^q \equiv 1^q \equiv 1$. □

Следующая теорема получается, как частный случай этой.

Теорема 3.2 (Малая теорема Ферма)**.**

Пусть $a, p \in \mathbb{N},\ \text{НОД}(a,p) = 1,\ p$ — простое. Тогда $a^{p-1} \equiv 1 \mod p$.

Пример 3.1. Вычислить $10^{111} \mod 121$.

Решение. 10 и $121 = 11^2$ взаимно просты, поэтому по модулю 121: $1 \equiv 10^{\varphi(121)} \equiv$ $\equiv 10^{\varphi(11^2)} \equiv 10^{11^2-11} \equiv 10^{110}$. В итоге, $10^{111} = 10 \cdot 10^{110} \equiv 10 \mod 121$. □

Пример 3.2. Вычислить $26^{21^{100500}} \mod 14$.

Решение. Обозначим $n = 100500$. Следующие рассуждения верны для произвольного $n \in \mathbb{N}$.

По модулю 14: $26^{21^n} \equiv 13^{21^n} 2^{21^n} \equiv (-1)^{21^n} 2^{21^n}$.

Число 21^n нечётное, поэтому $(-1)^{21^n} = -1$.

Заметим, что $2^{3+1} = 16 \equiv 2^1 \mod 14$, поэтому $2^{21^n} = 2^{3p+3} \equiv 2^3 \mod 14$.

Окончательно, по модулю 14: $(-1)^{21^n} 2^{21^n} \equiv -1 \cdot 2^3 \equiv -8 \equiv 6$. □

3.2. Первообразные корни

Определение 3.3 (Первообразный корень).

Пусть $n \in \mathbb{N}$, $n > 1$. Натуральное число a $(a < n)$ называется *первообразным корнем по модулю* n, если $a^{\varphi(n)} \equiv 1 \pmod n$ и $\forall p\colon 0 < p < \varphi(n)$ $a^p \not\equiv 1 \mod n$.

Определение означает, что $a \in U(\mathbb{Z}_n)$ и имеет порядок $\varphi(n)$ в этой группе. Учитывая, что $\varphi(n)$ — количество всех элементов группы, получается, что $U(\mathbb{Z}_n) = C_{\varphi(n)} =< a >$.

Из примера 2.4 следует, что количество образующих элементов группы C_m равно $\varphi(m)$. Поэтому если есть хоть один первообразный корень по модулю n, количество различных первообразных корней по модулю n равно $\varphi(\varphi(n))$.

И также из примера 2.4 следует, что каждый первообразный корень представим в виде a^p, где $p \in \mathbb{N}$, НОД$(p, \varphi(n)) = 1$.

Пример 3.3. Найти все первообразные корни по модулю 29.

Решение. $\varphi(29) = 28 = 2^2 7$.

Рассмотрим произвольный $a \in U(\mathbb{Z}_{29})$, $a \neq 1$. По следствию из теоремы Лагранжа, a может иметь порядки: 2, 4, 14, 28. Если $a^2 \equiv 1 \mod 29$, то $a^4 \equiv 1 \mod 29$ и $a^{14} \equiv 1 \mod 29$. Поэтому для подтверждения того, что a является первообразным корнем, необходимо и достаточно проверить, что $a^4 \not\equiv 1 \mod 29$ и $a^{14} \not\equiv 1 \mod 29$.

В общем случае, если $\varphi(n) = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, необходимо и достаточно проверить, что $\forall i = 1, \ldots, k$ $a^{\frac{\varphi(n)}{p_i}} \not\equiv 1 \mod n$.

Начнём перебирать элементы $U(\mathbb{Z}_{29})$. Пусть $a = 2$. По модулю 29: $2^4 \equiv 16 \not\equiv 1$, $2^1 4 \equiv$ $\equiv 2^5 2^5 2^4 \equiv 3^2 2^4 \equiv 144 \equiv 28 \not\equiv 1$. Значит, 2 — первообразный корень.

Все остальные первообразные корни представимы в виде 2^p, где НОД$(p, 28) = 1$ (сравнения по модулю 29):

1) $2^1 \equiv 1$;

2) $2^3 \equiv 8$;

3) $2^5 \equiv 32 \equiv 3$;

4) $2^9 \equiv 3 \cdot 2^4 \equiv 48 \equiv 19$;

5) $2^{11} \equiv 3^2 2 \equiv 18$;

6) $2^{13} \equiv 18 \cdot 2^2 \equiv 72 \equiv 14$;

7) $2^{15} \equiv 3^3 \equiv 27$;

8) $2^{17} \equiv 27 \cdot 2^2 \equiv 108 \equiv 21$;

9) $2^{19} \equiv 21 \cdot 2^2 \equiv 84 \equiv 26$;

10) $2^{23} \equiv 3^4 2^3 \equiv 81 \cdot 8 \equiv 23 \cdot 8 \equiv 184 \equiv 10$;

11) $2^{25} \equiv 10 \cdot 2^2 \equiv 40 \equiv 11$;

12) $2^{27} \equiv 11 \cdot 2^2 \equiv 44 \equiv 15$.

Проверим, что ничего не забыли: $\varphi(\varphi(29)) = \varphi(28) = \varphi(2^2 7) = (2^2 - 2)(7 - 1) = 12$. □

3.3. Квадратичные вычеты

Определение 3.4 (Квадратичный вычет).

Пусть $n \in \mathbb{N}$, $n > 1$. Натуральное число a называется *квадратичным вычетом по модулю* n, если уравнение $a = x^2$ имеет решения в $U(\mathbb{Z})_n$. В противном случае a называется *квадратичным невычетом по модулю* n.

В частности, $1 = 1^2$ является квадратичным вычетом по любому модулю.

Утверждение 3.2. Если a — квадратичный вычет по простому модулю $p > 2$, то уравнение $a = x^2$ имеет ровно два решения в $U(\mathbb{Z})_p$.

Доказательство. Из определения квадратичного вычета следует, что существует хотя бы одно решение, обозначим его как b. Тогда для натуральных чисел по модулю p:

$$x^2 \equiv a \iff x^2 \equiv b^2 \iff x^2 - b^2 \equiv 0 \iff (x - b)(x + b) \equiv 0.$$

Если x — вычет по модулю p то $-p < x - b < x + b < 2p$. В интервале $(-p; 2p)$ только 0 и p дают нулевой остаток при делении на p. Поэтому либо $x = b$, либо $x + b = p \Leftrightarrow x = p - b$. Одновременно эти равенства выполняться не могут, иначе $p = 2b$. □

Это утверждение означает, что в мультипликативной группе вычетов по простому модулю $p > 2$ ровно $\frac{p-1}{2}$ элементов являются квадратичными вычетами, и, соответственно, оставшиеся $\frac{p-1}{2}$ элементов являются квадратичными невычетами.

Пример 3.4. Найти сумму всех квадратичных вычетов в мультипликативной группе вычетов по простому модулю $p > 3$.

Решение. В сумме $1^2 + \ldots + (p-1)^2$ каждый квадратичный вычет учтён дважды. Поэтому искомая сумма S равна половине этой. И по модулю p:

$$S = \frac{1^2 + \ldots + (p-1)^2}{2} \equiv \frac{\frac{(p-1)p(2p-1)}{6}}{2} \equiv \frac{(p-1)p(2p-1)}{12} \Longrightarrow 12S \equiv 0.$$

Но НОД$(p, 12) = 1$, поэтому $S \equiv 0 \mod p$. □

СЕМИНАР 4

СИММЕТРИЧЕСКИЕ ГРУППЫ

Определение 4.1 (Симметрическая группа — S_n).

Симметрической группой множества называется группа всех перестановок элементов множества.

Определение 4.2 (Знак перестановки).

$\operatorname{sign}(\pi) = (-1)^{n+k}$, где n — количество элементов в перестановке, k — количество циклов в цикловом представлении перестановки, включая единичные циклы. Если $\operatorname{sign}(\pi) = 1$, то перестановка π называется *чётной*, в противном случае — *нечётной*.

Определение 4.3 (Транспозиция — $[(i,j)]$).

Перестановка, которая меняет местами ровно два элемента с индексами i и j.

Утверждение 4.1. Порядок перестановки равен НОК длин всех циклов в её цикловом представлении.

Упражнение 4.1. Пусть $s = (14)(23)(7869),\ \ s \in S_9$. Найти порядок s и решить в S_9 уравнение $xs = (123)(456)(789)$.

Упражнение 4.2. Доказать утверждения:

а) симметрическая группа S_n при $n > 1$ порождается всеми транспозициями;

б) симметрическая группа S_n при $n > 1$ порождается транспозициями

$$[(1,2)], [(1,3)], \ldots, [(1,n)].$$

Утверждение 4.2. Чётность перестановки соответствует чётности количества транспозиций, с помощью которых можно реализовать эту перестановку.

Определение 4.4 (Знакопеременная группа — A_n).

Подгруппа симметрической группы S_n, состоящая из всех чётных перестановок.

Пример 4.1. Доказать, что знакопеременная группа A_n при $n > 2$ порождается множеством всех тройных циклов $[(i,j,k)]$.

Р е ш е н и е. Рассмотрим произвольную перестановку из A_n. Она чётная, поэтому представима в виде произведения чётного числа перестановок. Разобьем эти перестановки последовательно на пары и покажем, что каждая пара представима в виде произведения тройных циклов.

Рассмотрим произведение перестановок $[(i,j)]$ и $[(k,l)]$:

$$[(i,j)][(k,l)] = [(i,j)]\left([(i,k)][(i,k)]\right)[(k,l)] = \left([(i,j)][(i,k)]\right)\left([(i,k)][(k,l)]\right) = [(k,j,i)][(l,i,k)].$$

□

Лемма 4.1. Пусть $< G, * >$ — группа порядка n.

$$a \in G, \quad \varphi_a \colon G \to G, \quad \forall g \in G \ \varphi_a(g) = ag.$$

Тогда φ_a — перестановка элементов G.

Д о к а з а т е л ь с т в о. Рассмотрим произвольные $x, y \in G$.

$$\varphi_a(x) = \varphi_a(y) \Longleftrightarrow ax = ay \Longleftrightarrow a^{-1}ax = a^{-1}ay \Longleftrightarrow x = y.$$

Это означает, что при преобразовании φ_a из n различных элементов получится n различных элементов. т. е. преобразование φ_a переводит множество G во всё множество G и является перестановкой. □

Теорема 4.1 (Теорема Кэли).

Любая конечная группа порядка n изоморфна некоторой группе перестановок n элементов.

Д о к а з а т е л ь с т в о. Пусть $< G, * >$ — группа порядка n. Докажем, что она изоморфна группе перестановок своих элементов. Для этого построим взаимно однозначное гомоморфное отображение элементов G в некоторое множество перестановок.

Каждому элементу a группы сопоставим преобразование $\varphi_a \colon G \to G$ по правилу

$$\forall x \in G \ \varphi_a(x) = ax.$$

По лемме 4.1 такое преобразование будет перестановкой.

$$\forall a, b \in G \ \varphi_a(x) = \varphi_b(x) \Longleftrightarrow ax = bx \Longleftrightarrow axx^{-1} = bxx^{-1} \Longleftrightarrow a = b.$$

Это означает, что отображение элементов в подмножество множества перестановок инъективно и, следовательно, обратимо.

Остается проверить сохранение групповой операции:

$$\forall x \in G \ \varphi_{ab}(x) = (ab)x = a(bx) = a\varphi_b(x) = \varphi_a(\varphi_b(x)) = (\varphi_a\varphi_b)(x).$$

□

Важное значение этой теоремы заключается в том, что любую группу можно описать с помощью группы перестановок.

Пример 4.2. Найти все, с точностью до изоморфизма, группы:

а) порядка 3;

б) порядка 4.

Решение. Опишем всевозможные группы в виде групп перестановок.

а) Элементов порядка больше 3 быть не может, поскольку порядок элемента должен быть делителем порядка группы.

1.1) Существует элемент a порядка 3. Тогда вся группа состоит из элементов: ι, a, a^2. Можно считать, что $\iota = (1)(2)(3)$, $a = (123)$, тогда $a^2 = (132)$.

1.2) Все элементы имеют порядок не выше 2. Но 2 не является делителем 3, поэтому элементы могут иметь только порядок 1. А такой порядок имеет только единичный элемент. Значит, такой случай не возможен.

б) Элементов порядка больше 4 быть не может, поскольку порядок элемента должен быть делителем порядка группы.

2.1) Существует элемент a порядка 4. Тогда вся группа состоит из элементов: ι, a, a^2, a^3. Можно считать, что $\iota = (1)(2)(3)(4)$, $a = (1234)$, тогда $a^2 = (13)(24)$, $a^3 = = (1432)$.

2.2) Все элементы имеют порядок не выше 3. Но 3 не является делителем 4, поэтому элементы могут иметь только порядок 1 или 2. Но порядок 1 имеет только единичный элемент. Значит, все элементы, кроме единичного, имеют порядок 2. Один элемент a порождает подгруппу ι, a, поэтому должен быть еще хотя

бы элемент b ($b \neq a$). Поскольку элементы a и b имеют порядок 2, группа, порожденная ими, является абелевой. Покажем, что элементы ι, a, b, ab замкнуты относительно групповой операции. Для этого запишем «таблицу умножения»:

	ι	a	b	ab
ι	ι	a	b	ab
a	a	ι	ab	b
b	b	ab	ι	a
ab	ab	b	a	ι

Таким образом, группа состоит из элементов: ι, a, b, ab. Можно считать, что $\iota = (1)(2)(3)(4)$, $a = (12)(3)(4)$, $b = (1)(2)(34)$, тогда $ab = (12)(34)$.

□

4.1. Доказать, что группа A_4 не имеет подгруппы порядка 6.

СЕМИНАР 5

КЛАССЫ СМЕЖНОСТИ. НОРМАЛЬНЫЙ ДЕЛИТЕЛЬ

Определение 5.1 (Класс смежности).

Левым и правым смежными классами элемента g группы $< G, * >$ по подгруппе $< H, * >$ называются, соответственно, множества

$$gH = \{x \colon x = gh, h \in H\}, \quad Hg = \{x \colon x = hg, h \in H\}.$$

В силу теоремы Кэли, если H конечная, то $\forall g \in G \ |gH| = |H|$.

Определение 5.2 (Индекс подгруппы).

Число различных смежных классов (левых или правых) по этой подгруппе.

Упражнение 5.1. Найти все смежные классы:

а) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу d;

б) мультипликативной группы комплексных чисел, отличных от нуля, по подгруппе чисел, равных по модулю единице;

в) симметрической группы S_n по подгруппе перестановок, оставляющих число n на месте.

Ответ: а) классы чисел с одинаковыми остатками по модулю d; б) классы равных по модулю чисел; в) n классов, определяемых образом или прообразом n-го элемента.

Пример 5.1. В группе $< \mathbb{Q}, + >$ рассмотрим подгруппу H, порождённую числами $\frac{1}{2}$, $\frac{1}{6}$, $\frac{1}{7}$. Верно ли, что числа $\frac{1}{9}$ и $-\frac{7}{27}$ принадлежат одному смежному классу по подгруппе H?

Решение. Заметим, что $\frac{1}{42} = \frac{1}{6} - \frac{1}{7} \in H$. При этом $\frac{1}{2} = \underbrace{\frac{1}{6} + \ldots + \frac{1}{6}}_{21}$, $\frac{1}{6} = \underbrace{\frac{1}{6} + \ldots + \frac{1}{6}}_{7}$, $\frac{1}{7} = \underbrace{\frac{1}{6} + \ldots + \frac{1}{6}}_{6}$. Поэтому $H =< \frac{1}{42} >$, т. е. H состоит из элементов вида $\frac{k}{42}$, где $k \in \mathbb{Z}$.

Если $\frac{1}{9}$ и $-\frac{7}{27}$ принадлежат одному смежному классу, то они представимы в виде $\frac{1}{9} = q + h_1,\ -\frac{7}{27} = q + h_2$, где $q \in \mathbb{Q},\ h_1, h_2 \in H$. Тогда $\frac{10}{27} = \frac{1}{9} - (-\frac{7}{27}) = h_1 - h_2 \in H$. Но $\frac{10}{27} = \frac{140}{9} \cdot \frac{1}{42} \notin H$, поскольку $\frac{140}{9} \notin \mathbb{Z}$. □

Упражнение 5.2. Пусть G — группа вращений трёхмерного куба, H_v — её подгруппа, состоящая из вращений, оставляющих вершину v на месте. Указать повороты на 90° и 180° из одного левого смежного класса по подгруппе H.

Упражнение 5.3. Привести пример конечной группы, содержащей несколько подгрупп индекса два.

Ответ: $\{\iota, a, b, ab\}$.

Пример 5.2. Доказать, что:

а) подгруппа порядка k конечной группы порядка $2k$ содержит квадраты всех элементов группы;

б) подгруппа индекса два любой группы содержит квадраты всех элементов группы.

Решение.

а) Пусть $< H, * >$ — подгруппа порядка k группы $< G, * >$ порядка $2k$. Если $g \in H$, то, очевидно, $g^2 \in H$. Пусть $g \in G$, $g \notin H$. Тогда $\forall h \in H\ gh \notin H$, иначе $g = (gh)h^{-1} \in H$. Кроме того, из леммы 4.1 следует, что $\forall h_1, h_2 \in G\ h_1 \neq h_2 \to gh_1 \neq gh_2$. Значит, все множество G разделяется на множество H и множество gH, каждое из которых содержит k элементов, и, соответственно, множество gG разделяется на множество gH и множество g^2H. Но множество G замкнуто относительно групповой операции, поэтому $G = gG$. Значит, $g^2H = H$. В частности, это означает, что $g^2 = g^2\iota \in H$.

б) Пусть $< H, * >$ — подгруппа индекса 2 группы $< G, * >$. Если $g \in H$, то, очевидно, $g^2 \in H$. Пусть $g \in G$, $g \notin H$. Тогда $\forall h \in H\ gh \notin H$, иначе $g = (gh)h^{-1} \in H$. Значит, всё множество G разделяется на два класса смежности по подгруппе $< H, * >$: множество $H = \iota H$ и множество gH. Соответственно, множество gG разделяется на множество gH и множество g^2H. Дальнейшее доказательство аналогично предыдущему пункту.

□

Пример 5.3. Доказать, что при $n > 1$ знакопеременная группа A_n является единственной подгруппой индекса два в симметрической группе S_n.

Р е ш е н и е. Пусть g — нечётная перестановка n элементов. Тогда gA_n — все нечётные перестановки. Значит, множество S_n распадается на два смежных класса по подгруппе A_n: $\iota A_n = A_n$ и gA_n. Таким образом, A_n является подгруппой индекса 2.

Пусть подгруппа H группы S_n имеет индекс два. Из примера 5.2 следует, что H содержит квадраты всех перестановок. Но произвольных тройной цикл представим в виде $[(i,j,k)] = [(i,k,j)][(i,k,j)]$. Это означает, что H содержит все тройные циклы. Тогда из примера 4.1 следует, что $A_n \subseteq H$. Но если $H \neq A_n$, то $|H| \geqslant 2|A_n| = |S_n|$. □

Определение 5.3 (Нормальный делитель / нормальная подгруппа).

Подгруппа $< H, * >$ группы $< G, * >$ такая, что $\forall g \in G\ gH = Hg$.

Определение 5.4 (Простая группа).

Группа, не имеющая нормальных делителей, кроме себя самой и единичной подгруппы.

Пример 5.4. Доказать, что любая подгруппа индекса два является нормальным делителем.

Р е ш е н и е. Пусть $< H, * >$ — подгруппа индекса 2 группы $< G, * >$, g — произвольный элемент G, не принадлежащий H. Тогда множество G разбивается на два левых смежных класса: $H = \iota H$ и gH, т. е. gH сотоит из всех элементов G, не входящих в H. Аналогично Hg сотоит из всех элементов G, не входящих в H. Таким образом, $gH = Hg$ для всех $g \notin H$. Если $g \in H$, то $gH = H = Hg$. □

Пример 5.5. Доказать, что в любой группе перестановок, содержащей хотя бы одну нечётную перестановку:

а) число чётных перестановок равно числу нечётных;

б) чётные перестановки образуют нормальный делитель;

Р е ш е н и е.

а) Пусть группа состоит из чётных перестановок $a_1, \ldots, a_k$ и нечётных $b_1, \ldots, b_l$. Взаимнооднозначно отобразим группу на себя по следующему правилу: $\varphi(x) = b_1 x$. Тогда если x — чётная перестановка, то $\varphi(x)$ — нечётная, и наоборот. Поэтому после отображения получится k нечётных перестановок и l чётных. Но, поскольку отображение взаимнооднозначное, эти количества должны совпадать с изначальными. Поэтому $k = l$.

б) Пусть H — подгруппа чётных перестановок группы G. $\forall h \in H\ hH = H = Hh$. Пусть $g \in G$: $g \notin H$. Тогда $\forall g_1 \in G\ g_1 \notin H \to g^{-1}g_1 \in H \Rightarrow g_1 = g(g^{-1}g_1) \in gH$. То есть gH — множество всех нечётных перестановок G. Аналогично Hg — множество всех нечётных перестановок G. Поэтому $gH = Hg$.

□

Упражнение 5.4. Доказать, что все простые группы перестановок n элементов ($n > 2$) содержатся в знакопеременной группе A_n.

Определение 5.5 (Коммутатор).

Коммутатором элементов a и b группы называется элемент

$$[a, b] = aba^{-1}b^{-1}.$$

Определение 5.6 (Коммутант группы).

Подгруппа, порожденная всеми коммутаторами элементов группы.

Пример 5.6. Доказать, что коммутант — нормальный делитель.

Решение. Пусть $< H, * >$ — коммутант группы $< G, * >$. Рассмотрим произвольные коммутатор $[a, b]$ и элемент g:

$$g[a,b] = g(aba^{-1}b^{-1}) = ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}(g^{-1}g) = \\ = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1})g = [gag^{-1}, gbg^{-1}]g.$$

Аналогично для набора коммутаторов:

$$g[a_1, b_1]\dots[a_n, b_n] = [ga_1g^{-1}, gb_1g^{-1}]\dots[ga_ng^{-1}, gb_ng^{-1}]g.$$

Это означает, что $\forall g \in G\ gH \subseteq Hg$. В обратную сторону доказывается аналогично. □

Определение 5.7 (Нормализатор элемента в группе — $N(a)$).

Множество элементов группы, перестановочных с данным элементом a:

$$\forall n \in N(a)\ na = an.$$

Определение 5.8 (Нормализатор подгруппы в группе — $N(H)$).

Множество элементов группы, перестановочных с данной подгруппой H:

$$\forall n \in N(H)\ nH = Hn.$$

Утверждение 5.1. Нормализаторы элементов и подгрупп являются подгруппами.

Доказательство. Пусть ♠ — подгруппа или элемент группы. Достаточно доказать, что $N(♠)\ldots$

1) замкнуто относительно групповой операции:

$$\forall n_1, n_2 \in N(♠)\ (n_1 n_2)♠ = n_1(n_2♠) = n_1(♠n_2) = \\ = (n_1♠)n_2 = (♠n_1)n_2 = ♠(n_1 n_2) \Longrightarrow (n_1 n_2) \in N(♠);$$

2) содержит ι:

$$ι♠ = ♠ = ♠ι \Longrightarrow ι \in N(♠);$$

3) если содержит элемент группы, то и содержит ему обратный:

$$\forall n \in N(♠)\ n^{-1}♠ = n^{-1}♠(nn^{-1}) = n^{-1}(♠n)n^{-1} = \\ = n^{-1}(n♠)n^{-1} = (n^{-1}n)♠n^{-1} = ♠n^{-1} \Longrightarrow n^{-1} \in N(♠).$$

□

Определение 5.9 (Центр группы).

Центром группы $< G, * >$ называется множество

$$C = \{c \in G \colon \forall g \in G\ cg = gc\}.$$

Из определения следует, что центр группы является её нормальным делителем.

Определение 5.10 (Сопряжённые элементы).

Элемент b *сопряжен элементу* a *посредством элемента* g, если

$$b = gag^{-1}.$$

Утверждение 5.2. Две перестановки сопряжены тогда и только тогда, когда они имеют эквивалентные структуры циклов (одинаковое количество циклов каждой длины).

Пример 5.7. Доказать что все элементы порядка 42 сопряжены в S_{12}.

Решение. Исследуем, какой цикловой вид может иметь перестановка указанного порядка. Длина каждого цикла является делителем порядка перестановки $42 = 2 \cdot 3 \cdot 7$.

Должно найтись хотя бы по одному циклу, длина которого делится на 2, 3 и 7 соответственно. Но $2 + 3 + 7 = 12$. Остаётся заметить, что $2 + 3 < 2 \cdot 3$, $2 + 7 < 2 \cdot 7$, $3 + 7 < 3 \cdot 7$, $2 + 3 + 7 < 2 \cdot 3 \cdot 7$. Поэтому если заменить любой набор, составленный из 2, 3, 7 на произведение соответствующих элементов, то понадобится больше 12 элементов для составления циклов.

Это означает, что каждая перестановка порядка 42 образована тремя циклами длин 2, 3 и 7 соответственно. То есть все они имеют одинаковое цикловое представление, а, значит, сопряжены. □

Определение 5.11 (Сопряжённые подгруппы).

Подгруппа B *сопряжена подгруппе* A *посредством элемента* g, если

$$B = gAg^{-1} \Longleftrightarrow B = \{b\colon b = gag^{-1}, a \in A\}.$$

Пример 5.8. Пусть $N(a)$ — номализатор группы $< G, * >$. Доказать, что:

а) $< a >$ является нормальным делителем $N(a)$;

б) число элементов группы, сопряженных с a, равно индексу $N(a)$ в группе $< G, * >$.

Решение.

а) $\forall n \in N(a) \forall k \in \mathbb{Z}\ na^k = (na)a^{k-1} = (an)a^{k-1} = \ldots = a^k n$.

б) Пусть $g_1, g_2 \in G$.

Если g_1 и g_2 порождают один смежный класс, т. е. $g_1 N(a) = g_2 N(a)$, то существуют $n_1, n_2 \in N(a)$ такие, что $g_1 n_1 = g_2 n_2$. Тогда

$$\begin{aligned} g_1 a g_1^{-1} &= (g_2 n_2 n_1^{-1}) a (g_2 n_2 n_1^{-1})^{-1} = g_2 n_2 n_1^{-1} a n_1 n_2^{-1} g_2^{-1} = \\ &= g_2 n_2 n_1^{-1} (a n_1) n_2^{-1} g_2^{-1} = g_2 n_2 n_1^{-1} (n_1 a) n_2^{-1} g_2^{-1} = g_2 n_2 (n_1^{-1} n_1)(a n_2^{-1}) g_2^{-1} = \\ &= g_2 n_2 (n_2^{-1} a) g_2^{-1} = g_2 (n_2 n_2^{-1}) a g_2^{-1} = g_2 a g_2^{-1}, \end{aligned}$$

т. е. сопряженные с a элементы посредством g_1 и g_2 совпадают.

Пусть $g_1 a g_1^{-1} = g_2 a g_2^{-1}$. Если $b \in g_1 N(a)$, то найдется $n_1 \in N(a)$ такой, что $b = g_1 n_1$. Если $n_2 = g_2^{-1} b \in N(a)$, то $b = g_2 n_2 \in g_2 N(a)$ и, следовательно, $g_1 N(a) \subseteq g_2 N(a)$.

$$n_2 a = (g_2^{-1} g_1 n_1) a = g_2^{-1} g_1 (n_1 a) = g_2^{-1} g_1 (a n_1) = g_2^{-1} g_1 a (g_1^{-1} g_1) n_1 =$$
$$= g_2^{-1} (g_1 a g_1^{-1}) g_1 n_1 = g_2^{-1} (g_2 a g_2^{-1}) g_1 n_1 = (g_2^{-1}(g_2) a (g_2^{-1} g_1 n_1) = a n_2.$$

Аналогично $g_2 N(a) \subseteq g_1 N(a)$, и, значит, $g_1 N(a) = g_2 N(a)$.

Получается, что классам смежности взаимно однозначно соответствуют сопряженные элементы.

□

СЕМИНАР 6

ТЕОРЕМА О ГОМОМОРФИЗМЕ

Определение 6.1 (Гомоморфное отображение — гомоморфизм).

Пусть заданы группы $< G_1, * >$ и $< G_2, \circ >$. Отображение $\varphi\colon G_1 \to G_2$ называют *гомоморфным*, если

$$\forall x, y \in G_1 \ \varphi(x * y) = \varphi(x) \circ \varphi(y).$$

Гомоморфным образом группы $< G_1, * >$ называют множество образов всех её элементов:

$$\operatorname{Im}\varphi = \varphi(G_1) = \{y \in G_2 \mid \exists x \in G_1 \colon y = \varphi(x)\}.$$

Ядром гомоморфизма называют множество элементов, образ каждого из которых является нейтральным элементом:

$$\operatorname{Ker}\varphi = \{x \in G_1 \mid \varphi(x) = \iota_{G_2}\}.$$

Утверждение 6.1. $\operatorname{Im}\varphi$ образует подгруппу группы $< G_2, \circ >$, а $\operatorname{Ker}\varphi$ — подгруппу группы $< G_1, * >$.

Пример 6.1. $\varphi\colon G \to H$ — гомоморфизм из группы $< G, * >$ в группу $< H, \circ >$. Доказать, что

а) если G конечная, то порядок G делится на порядок $\operatorname{Im}\varphi$;

б) для произвольного элемента $a \in G$ порядок a делится на порядок $\varphi(a)$.

Решение.

а) Пусть $\operatorname{Ker}\varphi = \{x_1, \ldots, x_k\}$. Покажем, что количество прообразов каждого элемента из $\operatorname{Im}\varphi$ равно k.

Рассмотрим произвольный $h \in H$. Пусть $\{g \in G \colon \varphi(g) = h\} = \{g_1, \ldots, g_n\}$.

С одной стороны, $\{g_1 * x_1, \ldots, g_1 * x_k\}$ — k попарно различных элементов, образы которых равны h. Поэтому $n \geqslant k$.

С другой стороны, $\{\iota_G, g_1 * g_2^{-1}, \ldots, g_1 * g_n^{-1}\}$ — n попарно различных элементов группы G, образы которых равны ι_H. Поэтому $n \leqslant k$.

В каждый элемент $\operatorname{Im}\varphi$ переходят k элементов G, поэтому $\frac{|G|}{|\operatorname{Im}\varphi|} = k \in \mathbb{Z}$.

б) Пусть n — порядок a. Тогда

$$(\varphi(a))^n = \underbrace{\varphi(a) \circ \ldots \circ \varphi(a)}_{n} = \varphi(\underbrace{a * \ldots * a}_{n}) = \varphi(a^n) = \varphi(\iota_G) = \iota_H.$$

□

Пример 6.2. Найти все гомоморфные отображения циклической группы $< a >$ порядка 6 в циклическую группу $< b >$ порядка 18.

Решение. Обозначим искомое отображение через φ. Пусть $\varphi(a) = b^k$. Тогда $b^{6k} = \varphi(a)^6 = \varphi(a^6) = \varphi(\iota_a) = \iota_b$. Значит, $6k$ кратно 18-и, т. е. $k \in \{0, 3, 6, 9, 12, 15\}$:

1) $k = 0$: $\varphi(< a >) = \{\iota_b\}$,

2) $k = 3$: $\varphi(< a >) = \{\iota_b, b^3, b^6, b^9, b^{12}, b^{15}\}$,

3) $k = 6$: $\varphi(< a >) = \{\iota_b, b^6, b^{12}\}$,

4) $k = 9$: $\varphi(< a >) = \{\iota_b, b^9\}$,

5) $k = 12$: $\varphi(< a >) = \{\iota_b, b^{12}, b^6\}$,

6) $k = 15$: $\varphi(< a >) = \{\iota_b, b^{15}, b^{12}, b^9, b^6, b^3\}$.

□

Пример 6.3. Доказать, что группа $< G', \circ >$ тогда и только тогда является гомоморфным образом конечной циклической группы $< G, * >$, когда $< G', \circ >$ циклическая и её порядок делит порядок группы $< G, * >$.

Решение. Обозначим через a порождающий элемент группы $< G, * >$, а через n — её порядок.

Пусть G' — циклическая группа, b — её порождающий элемент, k — порядок (делитель n). Построим гомоморфизм $\varphi\colon G \to G'$ по двум правилам: $\varphi(a) = b$, $\varphi(a^k) = \iota_{G'}$. Нетрудно показать, что построенный гомоморфизм будет корректным. Заметим, что $b^l = \varphi(a^l)$; при $l = ki + r \ \ (r < k) \ \ \varphi(a^l) = \varphi(a)^l = b^r$. Поэтому $\varphi(G) = G'$.

Пусть $\exists\varphi\colon\ \varphi(G) = G'$ — гомоморфизм, $\varphi(a) = b$, а k $(k \leqslant n)$ — такое наименьшее натуральное число, что $\varphi(a^k) = \iota_{G'}$ (оно существует, т. к. $\varphi(a^n) = \varphi(\iota_G) = \iota_{G'}$). $\forall i\ \varphi(a^i) = b^i$, поэтому b — порождающий элемент G'. k — порядок элемента b (по определению), а, значит, и порядок G'. Пусть n не делится на k, тогда $n = ki + r$ $(r < k)$, $\varphi(a^r) = \iota^i_{G'} \circ \varphi(a^r) = \varphi(a^k)^i \circ$ $\circ\ \varphi(a^r) = \varphi(a^{ki} * a^r) = \varphi(a^n) = \varphi(\iota_G) = \iota_{G'}$, что противоречит определению k. Значит, k — делитель n. □

Пример 6.4. Доказать, что аддитивную группу рациональных чисел нельзя гомоморфно отобразить на аддитивную группу целых чисел.

Решение. Предположим, что такой гомоморфизм существует. Обозначим его через φ. Пусть $\varphi(a) = ,\ \ n \in \mathbb{N}$. Тогда

$$n = \varphi(\underbrace{\frac{a}{2n} + \ldots + \frac{a}{2n}}_{2n}) = \underbrace{\varphi(\frac{a}{2n}) + \ldots + \varphi(\frac{a}{2n})}_{2n} \Longrightarrow \varphi(\frac{a}{2n}) = \frac{n}{2n} = \frac{1}{2} \notin \mathbb{Z}.$$

□

Определение 6.2 (Факторгруппа).

Пусть $< H, * >$ — нормальная подгруппа группы $< G, * >$. Заметим, что

$$(a * H) * (b * H) = (a * H) * (H * b) = a * (H * H) * b = a * (H * b) = (a * b) * H.$$

Поэтому на множестве F классов смежности можно ввести операцию $\circ$:

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

Нетрудно показать, что множество F с операцией $\circ$ образует группу $< F, \circ >$, которая называется *факторгруппой группы G по подгруппе H* и обозначается G/H.

Упражнение 6.1. Найти факторгруппы:

а) аддитивной группы целых чисел по подгруппе чисел, кратных данному натуральному числу d;

б) мультипликативной группы действительных чисел, отличных от нуля, по подгруппе положительных чисел.

Теорема 6.1. Теорема о гомоморфизме Гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма.

Пример 6.5. Пусть $< G_n, + >$ — аддитивная группа векторов n-мерного линейного пространства, $< H_k, + >$ — k-мерное подпространство. Доказать, что факторгруппа G_n/H_k изоморфна $< G_{n-k}, + >$.

Решение. Заметим, что любое линейное отображение для линейных пространств является гомоморфизмом для соответствующих аддитивных групп (это непосредственно следует из определений).

Пусть $G_n = H_k \oplus H_{n-k}$. Рассмотрим преобразование $\varphi\colon G_n \to G_n$, являющееся проекцией на H_{n-k} параллельно H_k. Тогда $\forall x \in H_k \ \varphi(x) = \mathbf{0}$, $\forall x \notin H_k \ \varphi(x) \neq \mathbf{0}$. Значит, $H_k = \operatorname{Ker}\varphi$. С другой стороны, в силу построения, $H_{n-k} = \operatorname{Im}\varphi$.

Согласно Теореме о гомоморфизме, подгруппа $< H_{n-k}, + >$ изоморфна факторгруппе G_n/H_k. С другой стороны, подгруппа $< H_{n-k}, + >$ является линейным пространством размерности $n-k$ и изоморфна любому линейному пространству такой же размерности. □

Пример 6.6. Пусть $< G, \times >$ — мультипликативная группа всех комплексных чисел, отличных от нуля, H — множество всех чисел из G, лежащих на действительной и мнимой осях, не включая нуль.

а) Доказать, что H — подгруппа группы G.

б) Найти смежные классы группы G по подгруппе H.

в) Доказать, что факторгруппа G/H изоморфна мультипликативной группе U всех комплексных чисел, равных по модулю единице.

Решение.

а) Для этого достаточно проверить замкнутость и существование обратных элементов. В H лежат все элементы из G двух видов: a и bi, где a и b — действительные числа, а i — мнимая единица. Заметим, что a^{-1}, $(bi)^{-1} = -b^{-1}i$, ab, $(ai)(bi) = -ab$, abi имеют такой же вид.

б) Смежные классы образуются при умножении всех элементов из H на числа вида $R(\cos\alpha + i\sin\alpha)$. Заметим, что изменяя R будем получать один и тот же набор чисел, поэтому смежные классы различаются только параметром α при $\alpha \in [0, \frac{\pi}{2})$. На декартовой плоскости с мнимой и действительной осями каждый класс представляет собой две взаимоперпендикулярные прямые, которые образуют оси при повороте на угол α по направлению от действительной к мнимой.

в) Рассмотрим преобразование $\varphi(R\cos\alpha + iR\sin\alpha) = (\cos(4\alpha) + i\sin(4\alpha))^2$. Заметим, что φ — гомоморфизм. Действительно,

$$\begin{aligned}
&\varphi((R_1\cos\alpha_1 + iR_1\sin\alpha_1)(R_2\cos\alpha_2 + iR_2\sin\alpha_2)) = \\
&\qquad = \varphi(R_1R_2(\cos(\alpha_1+\alpha_2) + i\sin(\alpha_1+\alpha_2))) = \\
&\qquad = (\cos(4(\alpha_1+\alpha_2)) + i\sin(4(\alpha_1+\alpha_2)))^2 = \\
&\qquad = (\cos(4\alpha_1) + i\sin(4\alpha_1))^2(\cos(4\alpha_2) + i\sin(4\alpha_2))^2 = \\
&\qquad = \varphi(R_1\cos\alpha_1 + iR_1\sin\alpha_1)\varphi(R_2\cos\alpha_2 + iR_2\sin\alpha_2).
\end{aligned}$$

Не трудно показать, что $\operatorname{Im}\varphi = U$ и $\varphi(H) = \{1\}$, т. е. $H = \operatorname{Ker}\varphi$. Таким образом, из Теоремы о гомоморфизме следует, что факторгруппа G/H изоморфна U.

□

Упражнение 6.2. Доказать, что факторгруппа G/H коммутативна тогда и только тогда, когда H содержит коммутант группы G.

СЕМИНАР 7

ПРЯМАЯ СУММА

Определение 7.1 (Прямое произведение групп).

Пусть заданы произвольные группы $< G_1, *_1 >, \ldots, < G_n, *_n >$. Их *прямым произведением* $G_1 \otimes \ldots \otimes G_n$ группа, образованная множеством наборов $(g_1, \ldots, g_n)$, где $g_i \in G_i$, с операцией $\circ$: $(g_1, \ldots, g_n) \circ (h_1, \ldots, h_n) = (g_1 *_1 h_1, \ldots, g_n *_n h_n)$.

Упражнение 7.1. Показать, что $< G_1 \otimes \ldots \otimes G_n, \circ >$ — группа.

Упражнение 7.2. Показать, что мультипликативная группа комплексных чисел изоморфна прямому произведению групп положительных действительных чисел и комплексных чисел, равных по модулю единице.

Утверждение 7.1. а) Если $G_1, \ldots, G_n$ — конечные группы, то

$$|G_1 \otimes \ldots \otimes G_n| = |G_1| \times \ldots \times |G_n|.$$

б) Если $g = (g_1, \ldots, g_n)$, то порядок g равен наименьшему общему кратному порядков $g_1, \ldots, g_n$.

в) Группа $G_1 \otimes \ldots \otimes G_n$ абелева тогда и только тогда, когда все группы $G_1, \ldots, G_n$ абелевы.

Далее в этом семинаре рассматриваются аддитивные абелевы группы, а нейтральный элемент обозначается нулём.

Определение 7.2 (Прямая сумма подгрупп).

Говорят, что абелева группа $< G, + >$ раскладывается в *прямую сумму своих подгрупп* $H_1, \ldots, H_n$ и пишут $G = H_1 \oplus \ldots \oplus H_n$, если каждый элемент $g \in G$ единственным образом представляется в виде $g = h_1 + \ldots + h_n$, где $h_i \in H_i$, $i = 1, \ldots, n$.

Утверждение 7.2. Если абелева группа $< G, + >$ представима в виде $G = H_1 \oplus \ldots \oplus H_n$, то она изоморфна $H_1 \otimes \ldots \otimes H_n$.

Упражнение 7.3. Доказать, что при $i \neq j$ $H_i \cap H_j = \{0\}$.

Упражнение 7.4. Доказать, что:

а) аддитивная группа векторов n-мерного пространства есть прямая сумма подгрупп векторов одномерных подпространств, натянутых на векторы любого базиса пространства;

б) аддитивная группа комплексных чисел есть прямая сумма подгрупп действительных и чисто мнимых чисел.

Пример 7.1. Доказать, что если существуют два разложения в прямую сумму абелевой группы $G = A \oplus B_1 = A \oplus B_2$ и $B_2 \subseteq B_1$, то $B_1 = B_2$.

Решение. Пусть $B_1 \neq B_2$. Тогда найдется элемент $b_1 \in G\colon b_1 \in B_1, b_1 \notin B_2$. Разложением этого элемента, соответствующим прямой сумме $A \oplus B_1$, очевидно, является $b_1 = b_1$. С другой стороны, должно существовать разложение, соответствующее прямой сумме $A \oplus B_2$: пусть $b_1 = a + b_2$, где $a \in A,\ b_2 \in B_2$. Но тогда $b_2 \in B_2 \subseteq B_1$, поэтому последнее разложение соответствует и прямой сумме $A \oplus B_1$, что противоречит единственности. □

Пример 7.2. Доказать, что подгруппа H абелевой группы G тогда и только тогда будет слагаемым в некотором прямом разложении $G = H \oplus K$, когда существует гомоморфное отображение G на H, сохраняющее на месте все элементы из H.

Решение. Пусть $G = H \oplus K$. Тогда любой элемент $g \in G$ единственным образом представляется в виде $g = h_g + k_g$, где $h_g \in H$, $k_g \in K$. То есть для каждого $g \in G$ таким образом можно выбрать единственный $h_g \in H$. Пусть $\varphi(g) = h_g$. Заметим, что

$$g_1 + g_2 = (h_{g_1} + k_{g_1}) + (h_{g_2} + k_{g_2}) = (h_{g_1} + h_{g_2}) + (k_{g_1} + k_{g_2})$$

и $(h_{g_1} + h_{g_2}) \in H$. Поэтому $\varphi(g_1 + g_2) = h_{g_1} + h_{g_2} = \varphi(g_1) + \varphi(g_2)$. Значит, $\varphi\colon G \to H$ — гомоморфизм. Кроме того, $\forall g \in H\ \ h_g = g,\ k_g = e$, поэтому $\forall g \in H\ \ \varphi(g) = g$.

Пусть $\varphi\colon G \to H$ — такой гомоморфизм, что $\forall h \in H\ \ \varphi(h) = h$. Рассмотрим произвольный $g \in G$. $\varphi(g) \in H \Rightarrow \exists h \in H\colon \varphi(g) = h$. Обозначим $k = g + (-h)$. Заметим, что

$$\varphi(k) = \varphi(g + (-h)) = \varphi(g) + \varphi(-h) = h + (-h) = 0.$$

Поэтому $k \in \operatorname{Ker}\varphi$. Получается, что $g = h + k$, где $h \in H,\ \ k \in \operatorname{Ker}\varphi$. Причём, такое разложение единственно. Действительно, если есть другое разложение $g = h' + k'$, то

$$h - h' = \varphi(h + (-h')) = \varphi(k' + (-k)) = 0 \Longrightarrow h = h'.$$

Значит, $G = H \oplus \operatorname{Ker}\varphi$. □

Утверждение 7.3. Каждая конечная абелева группа $< G, + >$ единственным образом (с точностью до изоморфизма) представляется в виде $G = H_1 \oplus \ldots \oplus H_n$, где для каждого $i = 1, \ldots, n$ H_i — примарная циклическая группа.

Пример 7.3. Доказать, что конечная абелева группа $< G, + >$, порядок которой равен произведению двух различных простых чисел p и q, является циклической.

Решение. Предположим, что рассматриваемая группа не циклическая. Из утверждения 7.3 следует, что $G =< a > \oplus < b >$, где $< a >$ и $< b >$ — циклические группы порядков p и q соответственно. Значит, произвольный элемент $g \in G$ представим в виде:

$$g = \underbrace{a + \ldots + a}_{k} + \underbrace{b + \ldots + b}_{l} = ka + lb.$$

Покажем, что для любых k и l найдётся $n \in \mathbb{Z}$ такое, что $ka + lb = n(a + b)$. Это будет означать, что G — циклическая группа, а $(a + b)$ — её образующий элемент.

Поскольку p и q взаимно просты, найдутся такие натуральные i $(i \leqslant p)$ и j $(j \leqslant q)$, что $iq \equiv 1 \mod p$ и $jp \equiv 1 \mod q$. Обозначим: $n = iqk + jpl$. Тогда

$$n(a + b) = (iqk + jpl)(a + b) = (iqk)a + (jpl)a + (iqk)b + (jpl)b =$$
$$= k(iqa) + (jl)(pa) + (ik)(qb) + l(jpb) = ka + jl0 + ik0 + lb = ka + lb.$$

□

Пример 7.4. Доказать, что если $G = A \oplus B$, то факторгруппа G/A изоморфна B.

Решение. Для каждого элемента $g \in G$ существует единственное представление $g = a_g + b_g$, где $a_g \in A$, $b_g \in B$. Тогда

$$A + g = A + (a_g + b_g) = (A + a_g) + b_g = A + b_g.$$

С другой стороны, если $A + b_1 = A + b_2$, где $b_1, b_2 \in B$, то $\forall a_i \in A\ \exists a_2 \in A$: $a_1 + b_1 = a_2 + b_2$. Но разложение каждого элемента G должно быть единственным, поэтому $a_1 = a_2$ и $b_1 = b_2$. Таким образом, между элементами группы B и факторгруппы G/A можно построить биекцию $\varphi(b) = A + b$. Не трудно заметить, что она будет удовлетворять свойствам изоморфизма. □

Рассмотрим произвольный гомоморфизм $\varphi\colon G \to H$ такой, что группа $< G, + >$ раскладывается в прямую сумму $G = \operatorname{Ker}\varphi \oplus F$. Из теоремы о гомоморфизме, $\operatorname{Im}\varphi \sim G/\operatorname{Ker}\varphi$, а из примера 7.4, $G/\operatorname{Ker}\varphi \sim F$. Поэтому

$$G = \operatorname{Ker}\varphi \oplus F \sim \operatorname{Ker}\varphi \otimes F \sim \operatorname{Ker}\varphi \otimes \operatorname{Im}\varphi.$$

СЕМИНАР 8

ПОНЯТИЯ КОЛЬЦА И ПОЛЯ

Определение 8.1 (Кольцо).

Множество R, замкнутое относительно двух бинарных операций: $+$ (*сложение*) и $\times$ (*умножение*), называется *кольцом* $< R, +, \times >$, если выполняются следующие аксиомы:

— $\forall a, b \in R\ a + b = b + a$ (коммутативность сложения);

— $\forall a, b, c \in R\ a + (b + c) = (a + b) + c$ (ассоциативность сложения);

— $\exists 0 \in R$: $\forall a \in R\ 0 + a = a + 0 = a$ (наличие нулевого элемента 0);

— $\forall a \in R\ \exists b \in R$: $a + b = b + a = 0$ (наличие противоположного элемента: $b = -a$);

— $\forall a, b, c \in R\ a \times (b \times c) = (a \times b) \times c$ (ассоциативность умножения);

— $\forall a, b, c \in R\ a \times (b + c) = a \times b + a \times c$ (дистрибутивность);

— $\forall a, b, c \in R\ (b + c) \times a = b \times a + c \times a$ (дистрибутивность).

Кольцо называется *кольцом с единицей*, если

— $\exists \iota \in R$: $\forall a \in R\ a \times \iota = \iota \times a = a$ (наличие единичного элемента ι).

Кольцо называется *коммутативным кольцом*, если

— $\forall a, b \in R\ a \times b = b \times a$ (коммутативность умножения).

Кольцо называется *кольцом без делителей нуля*, если

— $\forall a, b \in R\ a \times b = 0 \Longrightarrow (a = 0) \vee (b = 0)$.

Кольцо называется *целостным*, если оно коммутативно и не содержит делителей нуля.

Таким образом, $< R, + >$ образует аддитивную абелеву группу.

Пусть рассматривается кольцо $< R, +, \times >$. Для $a, b, c \in R$ и $n \in \mathbb{N}$ обозначим

$$a + (-b) = a - b, \quad na = \underbrace{a + \ldots a}_{n}.$$

Кроме того, будем считать умножение приоритетнее сложения: $a + b \times c = a + (b \times c)$.

Утверждение 8.1. Для любого элемента a кольца $< R, +, \times >$:

$$a \times 0 = 0 \times a = 0.$$

Доказательство.

$$a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0 \Longrightarrow 0 = a \times 0 - a \times 0 = a \times 0 + a \times 0 - a \times 0 = a \times 0.$$

$$0 \times a = (0 + 0) \times a = 0 \times a + 0 \times a \Longrightarrow 0 = 0 \times a - 0 \times a = 0 \times a + 0 \times a - 0 \times a = 0 \times a.$$

□

Утверждение 8.2. Для любых двух элементов a и b кольца $< R, +, \times >$:

$$-(a \times b) = (-a) \times b = a \times (-b).$$

Доказательство.

$$a \times b + (-a) \times b = (a - a) \times b = 0 \times b = 0 \Longrightarrow (-a) \times b = -(a \times b).$$

$$a \times b + a \times (-b) = a \times (b - b) = a \times 0 = 0 \Longrightarrow a \times (-b) = -(a \times b).$$

□

Пример 8.1. Показать, что в кольце с единицей $\imath$ коммутативность сложения вытекает из остальных аксиом.

Решение. Рассмотрим два произвольных элемента кольца: a и b. С одной стороны,

$$(a + b) \times (\imath + \imath) = (a + b) \times \imath + (a + b) \times \imath = a + b + a + b.$$

С другой стороны,

$$(a + b) \times (\imath + \imath) = a \times (\imath + \imath) + b \times (\imath + \imath) = a + a + b + b.$$

Правые части:

$$a + b + a + b = a + a + b + b \Longleftrightarrow$$

$$\Longleftrightarrow (-a) + a + b + a + b + (-b) = (-a) + a + a + b + b + (-b) \Longleftrightarrow b + a = a + b.$$

□

Упражнение 8.1. Доказать, что диагональные матрицы порядка n с действительными элементами образуют кольцо.

Пример 8.2. Показать, что в кольце диагональных матриц порядка n с действительными элементами есть делители нуля.

Решение. Рассмотрим матрицы

$$A = \operatorname{diag}(a, 0, 0, \ldots, 0) \quad \text{и} \quad B = \operatorname{diag}(0, b, 0, \ldots, 0),$$

где $a, b \neq 0$. Тогда $A \neq 0$, $B \neq 0$, но $A \times B = 0$. Поэтому A является левым делителем нуля, а B — правым. □

Пример 8.3. Бывают ли кольца матриц, обладающих несколькими левыми или несколькими правыми единицами?

Решение. Рассмотрим квадратные матрицы 2×2 вида $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$, где $a, b \in \mathbb{R}$. Не трудно показать, что они образуют кольцо. Причём, для для произвольного $c \in \mathbb{R}$

$$\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix} \times \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Поэтому все матрицы вида $\begin{pmatrix} 1 & c \\ 0 & 0 \end{pmatrix}$ являются в этом кольце левыми единицами.

Аналогично, в кольце матриц вида $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ все матрицы вида $\begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}$ являются правыми единицами. □

Пример 8.4. Доказать, что ненулевой элемент a кольца $< R, +, \times >$ не является левым делителем нуля тогда и только тогда, когда

$$\forall x, y \in R \; a \times x = a \times y \Longrightarrow x = y.$$

Решение. Если a не является левым делителем нуля, то

$$a \times x = a \times y \Longleftrightarrow a \times x - a \times y = 0 \Longleftrightarrow a \times (x - y) = 0 \Longrightarrow x - y = 0 \Longleftrightarrow x = y.$$

Если a — левый делитель нуля, то в R найдется $b \neq 0$ такой, что $a \times b = 0$. Тогда

$$a \times b = a \times b + a \times b = a \times (b + b),$$

но $b \neq b + b$. □

Пример 8.5. Показать, что в кольце функций, непрерывных на отрезке $[-1;1]$, есть делители нуля.

Решение. Рассмотрим две функции

$$f(x) = \begin{cases} x, & -1 \leqslant x < 0 \\ 0, & 0 \leqslant x \leqslant 1 \end{cases}, \quad g(x) = \begin{cases} 0, & -1 \leqslant x \leqslant 0 \\ x, & 0 < x \leqslant 1 \end{cases}.$$

При $-1 \leqslant x \leqslant 0$ $f(x)g(x) = 0$, поскольку $g(x) = 0$; при $0 \leqslant x \leqslant 1$ $f(x)g(x) = 0$, поскольку $f(x) = 0$ □

Упражнение 8.2. Пусть $< R, +, \times >$ — коммутативное кольцо с единицей. Доказать, что:

а) обратимый элемент (делитель единицы) не может быть делителем нуля;

б) обратимый элемент имеет единственный обратный;

в) если a и b обратимые, то c делится на d ($\exists k\colon c = k \times d$) тогда и только тогда, когда $a \times c$ делится на $b \times d$.

Определение 8.2 (Поле)**.**

Кольцо $< F, +, \times >$, в котором $< F \setminus \{0\}, \times >$ — абелева группа.

Утверждение 8.3. В поле нет делителей нуля.

Доказательство. Рассмотрим два произвольных ненулевых элемента a и b поля.

$$a \times b = 0 \Longleftrightarrow a^{-1}a \times b = a^{-1} \times 0 \Longleftrightarrow b = 0.$$

□

Упражнение 8.3. Выяснить образуют ли указанное множество кольцо (но не поле) или поле:

а) целые числа;

б) рациональные числа;

в) действительные числа;

г) комплексные числа;

д) числа вида $m + n\sqrt{2}$ с целыми m и n.

Ответ: а) кольцо; б) поле; в) поле; г) поле; д) кольцо.

Пример 8.6. Показать, что числа вида $p + q\sqrt[3]{2} + r\sqrt[3]{4}$ с рациональными p, q и r образуют поле. Найти элемент, обратный числу $1 - \sqrt[3]{2} + 2\sqrt[3]{4}$.

Решение. Сначала покажем замкнутость. Относительно сложения:

$$(p_1 + q_1\sqrt[3]{2} + r_1\sqrt[3]{4}) + (p_2 + q_2\sqrt[3]{2} + r_2\sqrt[3]{4}) = (p_1 + p_2) + (q_1 + q_2)\sqrt[3]{2} + (r_1 + r_2)\sqrt[3]{4}.$$

Относительно умножения:

$$\begin{aligned}(p_1 + q_1\sqrt[3]{2} + r_1\sqrt[3]{4}) \times (p_2 + q_2\sqrt[3]{2} + r_2\sqrt[3]{4}) = \\ = (p_1p_2 + 2q_1r_2 + 2r_1q_2) + (p_1q_2 + q_1p_2 + 2r_1r_2)\sqrt[3]{2} + (p_1r_2 + q_1q_2 + r_1p_2)\sqrt[3]{4}.\end{aligned}$$

Необходимые арифметические свойства операций выполняются, т. к. они верны для всех действительных чисел. Нуль принадлежит этому множеству, поскольку

$$0 = 0 + 0\sqrt[3]{2} + 0\sqrt[3]{4},$$

и для каждого $p + q\sqrt[3]{2} + r\sqrt[3]{4}$ найдется противоположный: $(-p) + (-q)\sqrt[3]{2} + (-r)\sqrt[3]{4}$. Единичный элемент также входит в множество

$$1 = 1 + 0\sqrt[3]{2} + 0\sqrt[3]{4}.$$

Для того,чтобы доказать, что указанное множество является полем, осталось обосновать существование обратного элемента для каждого ненулевого. Для элемента $p + q\sqrt[3]{2} + r\sqrt[3]{4}$ существование обратного $x_p + x_q\sqrt[3]{2} + x_r\sqrt[3]{4}$ определяется наличием решения системы линейных уравнений:

$$\begin{cases} px_p + 2qx_r + 2rx_q = 1 \\ px_q + qx_p + 2rx_r = 0 \\ px_r + qx_q + rx_p = 0 \end{cases} \iff \begin{pmatrix} p & 2r & 2q \\ q & p & 2r \\ r & q & p \end{pmatrix} \begin{pmatrix} x_p \\ x_q \\ x_r \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Докажем, что определитель матрицы системы $(p^3 + 2q^3 + 4r^3 - 6pqr)$ не может обращаться в нуль ни при каких рациональных p, q и r. Пусть

$$p = \frac{m_p}{n_p}, \quad q = \frac{m_q}{n_q}, \quad r = \frac{m_r}{n_r},$$

где $m_p, m_q, m_r \in \mathbb{Z}$, $n_p, n_q, n_r \in \mathbb{N}$. Тогда равенство определителя нулю запишется следующим образом:

$$\left(\frac{m_p}{n_p}\right)^3 + 2\left(\frac{m_q}{n_q}\right)^3 + 4\left(\frac{m_r}{n_r}\right)^3 - 6\left(\frac{m_p}{n_p}\right)\left(\frac{m_q}{n_q}\right)\left(\frac{m_r}{n_r}\right) = 0 \Longleftrightarrow$$
$$\Longleftrightarrow (m_p n_q n_r)^3 + 2(n_p m_q n_r)^3 + 4(n_p n_q m_r)^3 - 6(m_p n_q n_r)(n_p m_q n_r)(n_p n_q m_r) = 0.$$

Если обозначить $x = m_p n_q n_r$, $y = n_p m_q n_r$, $z = n_p n_q m_r$, получится, что уравнение

$$x^3 + 2y^3 + 4z^3 - 6xyz = 0$$

должно иметь ненулевое решение в целых числах.

1) $x^3 = 2(3xyz - y^3 - 2z^3) \Longrightarrow x = 2x_1$, $x_1 \in \mathbb{Z}$;

2) $y^3 = 2(3yzx_1 - z^3 - 2x_1^3) \Longrightarrow y = 2y_1$, $y_1 \in \mathbb{Z}$;

3) $z^3 = 2(3zx_1y_1 - x_1^3 - 2y_1^3) \Longrightarrow z = 2z_1$, $z_1 \in \mathbb{Z}$;

4) $x_1^3 + 2y_1^3 + 4z_1^3 - 6x_1y_1z_1 = 0$.

Получили, что каждое из чисел x, y, z должно делиться на 2, причем для частных выполняется такое же уравнение. Значит, можно показать, что x_1, y_1 и z_1 тоже четные и т. д. А это возможно, только если $x = y = z = 0$, что противоречит требованиям.

Значит, определитель матрицы системы всегда отличен от нуля, т. е. система имеет единственное решение, которое и позволяет найти обратный элемент.

Решая аналогичную систему для элемента $1 - \sqrt[3]{2} + 2\sqrt[3]{4}$, находим ему обратный: $\frac{5}{43} + + \frac{9}{43}\sqrt[3]{2} - \frac{1}{43}\sqrt[3]{4}$. Правильность можно проверить умножением. □

Пример 8.7. Доказать, что конечное коммутативное кольцо R без делителей нуля, содержащее более одного элемента, является полем.

Решение. Пусть a — произвольный ненулевой элемент кольца R. Из примера 8.4 следует, что преобразование $f(x) = a \times x$ является биекцией.

Возьмём произвольный ненулевой элемент $r \in R$. Поскольку кольцо конечное, найдутся такие $n, m \in \mathbb{N}$, что $n > m$ и $a^n \times r = a^m \times r$. Тогда

$$0 = a^n \times r - a^m \times r = a^m \times (a^{n-m} \times r - r) \Longrightarrow a^{n-m} \times r - r = 0 \Rightarrow a^{n-m} \times r = r.$$

Таким образом, для любого ненулевого элемента r кольца существует степень a^{p_r} такая, что $a^{p_r} \times r = r$. Если взять произведение всех показателей этих степеней: $p = \prod\limits_{r \in R, r \neq 0} p_r$, получится, что a^p — единичный элемент ι.

С другой стороны, $a^{p-1} \times a = a^p = \iota$. Это означает, что для элемента a существует обратный a^{p-1}. Поскольку a был выбран произвольным образом, обратный существует для любого ненулевого элемента. $\square$

СЕМИНАР 9

КОЛЬЦА И ПОЛЯ ВЫЧЕТОВ

Определение 9.1 (Сравнимость по модулю).

Пусть задано натуральное n. Говорят, что *два целых числа сравнимы по модулю* n и пишут $a \equiv b \mod n$, если $a - b$ делится на n, т. е. a и b имеют одинаковые остатки при делении на n.

Два числа сравнимы по модулю 0 тогда и только тогда, когда они равны.

Определение 9.2 (Числовое кольцо вычетов).

Если задано натуральное n, кольцо целых чисел $\mathbb{Z}$ разбивается на непересекающиеся классы чисел, имеющих одинаковые остатки при делении на n. Определим сложение и умножение этих классов через операции над их элементами: пусть числа a и b принадлежат классам A и B соответственно, тогда классы $A + B$ и $A \times B$ — это те классы, которые содержат числа $a + b$ и $a \times b$ соответственно. Не трудно проверить, что такое определение корректно. Кроме того множество классов с этими операциями образует кольцо, которое называют *кольцом* $\mathbb{Z}_n$ *вычетов по модулю* n. Единичным элементом в нём является класс, содержащий 1, нулевым — содержащий 0.

Аналогичным образом кольцо вычетов можно получить из любого кольца, в котором определено деление с остатком.

Пример 9.1. Показать, что кольцо $\mathbb{Z}_n$ вычетов по модулю n будет полем тогда и только тогда, когда n — простое число.

Решение. Будем обозначать через A_k класс вычетов, содержащий число k.

Если $n = p \times q$, где p и q — натуральные числа, большие 1. Тогда $A_p \times A_q = A_n = A_0$, т. е. A_q и A_p — делители нуля, которых не может быть в поле.

Если n — простое, то для того, чтобы $\mathbb{Z}_n$ было полем, необходимо и достаточно, чтобы каждый ненулевой класс вычетов имел обратный. Рассмотрим произвольный класс A_p $(1 < p < n)$. Все числа $p, 2p, \ldots, (n-1)p$ имеют попарно различные ненулевые остатки при делении на n. По принципу Дирихле, среди них найдется равный 1. Таким образом, $\exists k\colon 1 < k < n, A_{kp} = A_1$. Но $A_p \times A_k = A_{kp}$. Значит, для A_p существует обратный. □

Определение 9.3 (Характеристика поля).

Минимальное натуральное n такое, что

$$n\iota = \underbrace{\iota + \ldots + \iota}_{n} = 0,$$

где ι — единичный элемент. Если это не верно ни для какого натурального числа, говорят, что поле имеет *характеристику нуль*.

Поскольку в поле нет делителей нуля, то характеристика поля — либо нуль, либо простое число.

Пример 9.2. Доказать, что минимальное подполе поля $< F, +, \times >$ характеристики p изоморфно полю вычетов по модулю p.

Решение. Пусть ι — единичный элемент в F. Рассмотрим произвольное подполе F'. Оно должно содержать элементы $\iota, 2\iota, \ldots, (p-1)\iota$. Все они ненулевые, т. к. в противном случае нашлось бы натуральные число $0 < k < p$ такое, что $k\iota = 0$. Кроме того, все они различны, т. к. в противном случае нашлись бы натуральные числа $0 < k < l < p$ такие, что $k\iota = l\iota \Rightarrow (l-k)\iota = 0$. Значит F' содержит по крайней мере эти $p-1$ элемент и нулевой $(0\iota = 0)$.

Взаимно однозначно сопоставим каждому элементу $k\iota$ класс вычетов A_k по модулю p, содержащий k. Покажем, что такое сопоставление сохраняет операции сложения и умножения. Действительно, пусть целые неотрицательные числа $k_1 < p$ и $k_1 < p$ такие, что

$$k_1 + k_2 = n_+ p + r_+ \quad \text{и} \quad k_1 k_2 = n_\times p + r_\times,$$

где n_+ и $n_\times$ — целые неотрицательные, а r_+ и $r_\times$ — остатки от деления на p. Тогда

$$A_{k_1} + A_{k_2} = A_{r_+}, \quad A_{k_1} \times A_{k_2} = A_{r_\times}.$$

С другой стороны,

$$k_1\iota + k_2\iota = n_+(p\iota) + r_+\iota = n_+ \cdot 0 + r_+\iota = r_+\iota,$$

$$k_1\iota \times k_2\iota = n_\times(p\iota) + r_\times\iota = n_\times \cdot 0 + r_\times\iota = r_\times\iota.$$

Таким образом, все элементы $k\iota$ $(0 \leqslant k < p)$ образуют поле, которое является минимальным подполем F и изоморфно полю вычетов по модулю p. □

На практике каждый числовой класс вычетов по модулю n отождествляется с наименьшим неотрицательным числом, которое содержит, — остатком от деления любого его элемента на n. Соответственно, при сложении и умножении чисел вычисляется остаток от деления результата на n.

Пример 9.3. Решить систему уравнений

$$\begin{cases} x + 2z = 1 \\ y + 2z = 2 \\ 2x + z = 1 \end{cases}$$

а) в поле вычетов по модулю 3;

б) в поле вычетов по модулю 5.

Решение.

а) Умножив первое уравнение на 2, получим $2x + z = 2$, что вкупе с третьим уравнением приводит к неверному равенству $1 = 2$, т. е. система несовместна.

б) Умножив первое уравнение на 3, получим $3x + z = 3$. Сложив с последним уравнением: $2z = 4$, т. е. $z = 2$. Подставим в первые два уравнения исходной системы:

$$\begin{cases} x + 2 = 1 \\ y + 2 = 2 \end{cases} \iff \begin{cases} x = 4 \\ y = 0 \end{cases}.$$

Таким образом, найдено единственное решение: $x = 4$, $y = 0$, $z = 1$.

□

Упражнение 9.1. Решить систему уравнений

$$\begin{cases} 3x + y + 2z = 1 \\ x + 2y + 3z = 1 \\ 4x + 3y + 2z = 1 \end{cases}$$

а) в поле вычетов по модулю 5;

б) в поле вычетов по модулю 7.

Ответ: а) система несовместна; б) $x = 2$, $y = 6$, $z = 5$.

Упражнение 9.2. Найти наибольший общий делитель многочленов

$$f(x) = x^4 + 1 \quad \text{и} \quad g(x) = x^3 + x + 1$$

а) в поле вычетов по модулю 3;

б) в поле вычетов по модулю 5.

Ответ: а) $2x^2 + 2x + 1$; б) 1.

Пример 9.4. Найти наибольший общий делитель многочленов

$$f(x) = x^3 + 2 \quad \text{и} \quad g(x) = x^2 + 2x + 1$$

а) в поле рациональных чисел;

б) в поле вычетов по модулю 3.

Решение. В обоих случаях применим алгоритм Евклида: будем последовательно считать остатки от деления.

а) Над полем рациональных чисел:

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

1.2) $g(x) = (x^2 + 2x + \frac{8}{9}) + \frac{1}{9} = (\frac{1}{3}x + \frac{2}{9})(3x + 4) + \frac{1}{9}$;

1.3) $3x + 4 = (27x + 36)\frac{1}{9} + 0$.

Таким образом, наибольшим общим делителем является многочлен нулевой степени.

б) Над полем вычетов по модулю 3:

2.1) $f(x) = (x^3 + 1) + 1 = (x + 1)g(x) + 1$;

2.2) $g(x) = g(x) \cdot 1 + 0$.

Таким образом, наибольшим общим делителем является многочлен нулевой степени.

□

Пример 9.5. Разложить многочлен $f(x) = x^5 + x^3 + x^2 + 1$ на неприводимые множители над полем вычетов по модулю 2.

Р е ш е н и е. Корнями многочлена могут быть 0 и 1. Заметим, что $f(1) = 0$, поэтому $f(x) = (x+1)f_1(x)$. Делением находим: $f_1(x) = x^4 + x^3 + x + 1$.

Аналогично $f_1(1) = 0$, поэтому $f_1(x) = (x+1)f_2(x)$; $f_2(x) = x^3 + 1$ и т. д.

В итоге, $f(x) = (x+1)^3(x^2 + x + 1)$. Если бы $g(x) = x^2 + x + 1$ был приводим, то раскладывался бы на произведение многочленов первой степени, но он не имеет корней ($g(0) \neq 0$, $g(1) \neq 0$). □

Упражнение 9.3. Разложить многочлен $f(x) = x^3 + 2x^2 + 4x + 1$ на неприводимые множители над полем вычетов по модулю 5.

О т в е т : $f(x) = (x+3)(x^2 + 4x + 2)$

Упражнение 9.4. Разложить многочлен $f(x) = x^4 + x^3 + x + 2$ на неприводимые множители над полем вычетов по модулю 3.

О т в е т : $f(x) = (x^2 + 2)(x^2 + x + 2)$

Пример 9.6. Разложить на неприводимые множители все многочлены от x второй степени над полем вычетов по модулю 2.

Р е ш е н и е. Определим сначала количество таких многочленов. Каждый имеет вид $a_2x^2 + a_1x + a_0$, где $a_2 = 1$, $a_1, a_0 \in \{0,1\}$. Всего способов выбрать коэффициенты $1 \times 2 \times \times 2 = 4$.

Каждый многочлен либо неприводим, либо раскладывается на произведение двух многочленов первой степени. Рассмотрим все такие произведения:

1) $x \times x = x^2$;

2) $x \times (x+1) = x^2 + x$

3) $(x+1) \times (x+1) = x^2 + 1$.

Остался единственный многочлен, который неприводим: $x^2 + x + 1$. □

СЕМИНАР 10

ИДЕАЛЫ

Определение 10.1 (Идеал).

Пусть задано кольцо $< R, +, \times >$. *Левым идеалом* этого кольца называется подкольцо I, замкнутое относительно умножения на элементы из R:

$$\forall a \in I, b \in R \; a \times b \in I \quad (I \times R = I).$$

Аналогично для *правого идеала*:

$$\forall a \in I, b \in R \; b \times a \in I \quad (R \times I = I).$$

Идеал, порожденный одним элементом $a \in R$, называется *главным*:

$$I = a \times R \; (\textit{левый}) \quad \text{или} \quad I = R \times a \; (\textit{правый}).$$

Если идеал одновременно и левый, и правый, он называется *двухсторонним*. В коммутативном кольце левые и правые идеалы совпадают и называются просто *идеалами*.

Определение 10.2 (Кольцо главных идеалов).

Кольцо, все идеалы которого главные.

Пример 10.1. Пусть $< R, +, \times >$ — коммутативное кольцо с единицей ι. Доказать, что главный идеал I, порожденный элементом $a \in R$ тогда и только тогда отличен от R, когда a необратим.

Решение. Пусть $I = R$. Это означает, что $\iota \in I$. А, т. к. I — главный идеал, найдется такой элемент $b \in R$, что $\iota = a \times b$. Но это означает, что $b = a^{-1}$.

Пусть a обратим. Тогда для любого элемента $b \in R$ найдется $b' \in R$, равный $a^{-1} \times b$, такой, что $a \times b' = b$, что означает, что $b \in I$. Таким образом, $R \subseteq I$, т. е. $R = I$. □

Определение 10.3 (Ассоциированные элементы целостного кольца).

Два элемента a и b, для которых существует обратимый элемент c такой, что

$$a = c \times b.$$

Пример 10.2. Пусть $< R, +, \times >$ — целостное кольцо с единицей ι. Доказать, что:

а) элементы a и b тогда и только тогда ассоциированы, когда каждый из них делится на другой;

б) главные идеалы I_a и I_b, порожденные элементами a и b соответственно, тогда и только тогда совпадают, когда a и b ассоциированы.

Р е ш е н и е.

а) Если a и b ассоциированы, то $b = c \times a$, $a = c^{-1} \times b$, где c — обратимый элемент кольца R. Таким образом, a и b делятся друг на друга.

Если a и b делятся друг на друга, то $b = c \times a$ и $a = d \times b$, т. е.

$$b = c \times d \times b \Longleftrightarrow b \times (c \times d - \iota) = 0 \Longrightarrow c \times d - \iota = 0 \Longleftrightarrow c \times d = \iota \Longrightarrow c^{-1} = d.$$

б) Пусть a и b ассоциированы, т. е. $b = c \times a$, $a = c^{-1} \times b$. Рассмотрим произвольный элемент $d \in I_a$. Поскольку $I_a = a \times R$, существует элемент $r_a \in R$ такой, что

$$d = a \times r_a = b \times c^{-1} \times r_a = b \times r_b,$$

где $r_b = c^{-1} \times r_a$, причем $r_b \in R$. Таким образом, $d \in I_b$, а поскольку b выбирался произвольно, $I_a \subseteq I_b$. Аналогично можно показать, что $I_b \subseteq I_a$, что означает, что $I_a = I_b$.

Пусть $I_a = I_b$. $b \in I_b \Rightarrow b \in I_a$. Значит, существует $c \in R$: $b = c \times a$. Аналогично существует $d \in R$: $a = d \times b$. Поскольку a и b делятся друг на друга, они ассоциированы.

□

Пример 10.3. Доказать, что пересечение любого конечного множества идеалов коммутативного кольца R является идеалом.

Р е ш е н и е. Будем доказывать по методу математической индукции.

База: I_1 и I_2 — идеалы кольца R. Докажем, что $I' = I_1 \cap I_2$ — тоже идеал. Во-первых, I' — подкольцо R, поскольку является пересечением двух подколец. Во-вторых, рассмотрим произвольный элемент $a \in I'$.

$$a \in I_1 \cap I_2 \Longrightarrow a \in I_1 \Longrightarrow a \times R \subseteq I_1.$$

Аналогично $a \times R \subseteq I_2$. Таким образом, $a \times R \subseteq I_1 \cap I_2 = I'$, т. е. кольцо I' замкнуто относительно умножения на элементы R, что определяет I' как идеал.

Пусть для любого набора из $k \leqslant n$ идеалов $I_1, \ldots, I_k$ кольца R их пересечение — идеал. Тогда пересечение произвольного набора из $n+1$ идеала $I_1 \cap \ldots \cap I_{n+1} = I' \cap I_{n+1}$, где $I' = I_1 \cap \ldots \cap I_n$ — идеал, т. е. тоже является идеалом.

Согласно принципу математической индукции, предположение верно для любого натурального числа идеалов. □

Определение 10.4 (Сумма идеалов).

Пусть $< R, +, \times >$ — коммутативное кольцо. *Суммой его идеалов* $I_1, \ldots, I_n$ называется множество элементов $x \in R$, представимых в виде

$$x = x_1 + \ldots + x_n, \quad x_i \in I_i, \quad i = 1, \ldots, n.$$

И обозначается $I = I_1 + \ldots + I_n$. Если для каждого $x \in I$ такое разложение единственно, сумма называется *прямой* и обозначается $I = I_1 \oplus \ldots \oplus I_n$.

Пример 10.4. Доказать, что сумма любого конечного числа идеалов кольца R есть идеал этого кольца.

Решение. Будем доказывать по методу математической индукции.

База: I_1 и I_2 — идеалы кольца R. Докажем, что $I' = I_1 + I_2$ — тоже идеал. Во-первых, очевидно, что I' содержит нулевой элемент и, если $a \in I'$, то и $-a \in I'$. Во-вторых, заметим, что множество I' замкнуто относительно операции сложения. Рассмотрим произвольные элементы $x = x_1 + x_2$ и $y = y_1 + y_2$ множества I', где $x_1, y_1 \in I_1$, $x_2, y_2 \in I_2$. Тогда $x + y = (x_1 + y_1) + (x_2 + y_2)$. Поскольку $x_1 + y_1 \in I_1$, а $x_2 + y_2 \in I_2$, получаем, что $x + y \in I'$. И наконец, для произвольного элемента $r \in R$ верно, что

$$x_1 \times r \in I_1, \quad x_2 \times r \in I_2.$$

Это означает, что

$$x \times r = (x_1 + x_2) \times r = (x_1 \times r) + (x_2 \times r) \in I'.$$

Таким образом, I' — подкольцо, замкнутое относительно умножения на элементы R, что определяет I' как идеал.

Пусть для любого набора из $k \leqslant n$ идеалов $I_1, \ldots, I_k$ кольца R их сумма — идеал. Тогда сумма произвольного набора из $n+1$ идеала $I_1 + \ldots + I_{n+1} = I' + I_{n+1}$, где $I' = I_1 + \ldots + I_n$ — идеал, т. е. тоже является идеалом.

Согласно принципу математической индукции, предположение верно для любого натурального числа идеалов. □

Пример 10.5. Доказать, что в коммутативном кольце R:

а) $I = I_1 \oplus I_2 \Leftrightarrow I_1 \cap I_2 = \{0\}$;

б) $I = I_1 \oplus I_2 \Rightarrow \forall x_1 \in I_1, x_2 \in I_2 \; x_1 \times x_2 = 0$.

Решение.

а) Пусть $I = I_1 \oplus I_2$. Если $a \in I_1 \cap I_2$, $a \neq 0$, то для произвольного элемента $x \in I$ помимо разложения $x = x_1 + x_2 \;\; (x_1 \in I_1, \;\; x_2 \in I_2)$ существует

$$x = (x_1 + a) + (x_2 - a), \quad \text{где} \quad x_1 + a \in I_1, \quad x_1 - a \in I_2,$$

что противоречит определению прямой суммы.

Если $I = I_1 + I_2$, но $I \neq I_1 \oplus I_2$, рассмотрим элемент, для которого разложение не единственно:

$$x = a_1 + a_2 = b_1 + b_2, \quad \text{где} \quad a_1, b_1 \in I_1, \quad a_2, b_2 \in I_2.$$

Тогда $b_1 - a_1 = a_2 - b_2 = c \neq 0$. Но $b_1 - a_1 \in I_1, \;\; a_2 - b_2 \in I_2$, т. е. $c \in I_1 \cap I_2$.

б) Предположим, что

$$x_1 \times x_2 \neq 0, \quad \text{где} \quad x_1 \in I_1, \quad x_2 \in I_2.$$

Поскольку кольцо I_1 замкнуто относительно умножения на элементы из R, а $x_2 \in R$, получаем, что $x_1 \times x_2 \in I_1$. Аналогично $x_1 \times x_2 \in I_2$. Выходит, что $I_1 \cap I_2$ содержит ненулевой элемент, что противоречит пункту а.

□

Пример 10.6. Пусть $R = I_1 \oplus I_2$ — разложение коммутативного кольца $< R, +, \times >$ с единицей ι в прямую сумму идеалов. Доказать, что если

$$\iota = \iota_1 + \iota_2, \quad \text{где} \quad \iota_1 \in I_1, \quad \iota_2 \in I_2,$$

то ι_1 и ι_2 — единицы в I_1 и I_2 соответственно, но не в R.

Решение. Рассмотрим произвольный элемент кольца $a = a_1 + a_2$, где $a_1 \in I_1$, $a_2 \in I_2$. Тогда

$$a_1 + a_2 = a \times \iota = a_1 \times \iota_1 + a_1 \times \iota_2 + a_2 \times \iota_1 + a_2 \times \iota_2 = a_1 \times \iota_1 + a_2 \times \iota_2.$$

Если $a \in I_1$, то $a_2 = 0$ и $a \times \iota_1 = a$, т. е. ι_1 — единичный элемент в I_1. Аналогично ι_2 — единичный элемент в I_2. Но если $a_1 \neq 0$ и $a_2 \neq 0$, то $a \times \iota_1 = a_1 \neq a \neq a_2 = a \times \iota_2$. □

Пример 10.7. Пусть $< R, +, \times >$ — коммутативное кольцо. Для произвольного элемента $a \in R$ рассматривается минимальный идеал, его содержащий. Доказать, что он состоит из элементов вида:

а) $r \times a \ \ (r \in R)$, если кольцо содержит единицу;

б) $r \times a + na \ \ (r \in R,\ n \in \mathbb{Z})$, если кольцо не содержит единицу.

Решение. Пусть I_a — такой идеал для элемента a. Поскольку $\forall x \in I_a, r \in R\ x \times r \in I_a$ и $a \in I_a$, получаем, что I содержит все элементы вида $a \times r$.

Покажем, что если $e \in R$ — единичный элемент, то произведения $a \times r$ $(r \in R)$ образуют идеал I, очевидно содержащий a. Во-первых, не трудно заметить, что $0 \in I$ и если $a \times r \in$ $\in I$, то и $-(a \times r) = a \times (-r) \in I$. Во-вторых, если $a \times r_1 \in I$ и $a \times r_2 \in I$, то $(a \times r_1) + (a \times$ $\times\, r_2) = a \times (r_1 + r_2) \in I$. И наконец, для произвольных элементов $a \times r \in I$ и $r' \in R$ их произведение $(a \times r) \times r' = a \times (r \times r')$ снова лежит в I. Поэтому, I образует подкольцо, замкнутое относительно умножения на элементы из R, т. е. идеал.

Если единичного элемента в кольце нет, то, поскольку $a \in I_a$, и множество I_a замкнуто относительно сложения, оно содержит все элементы вида $r \times a + na$ $(r \in R,\ n \in \mathbb{Z})$. Аналогично предыдущему случаю можно показать, что они образуют идеал. □

СЕМИНАР 11

ФАКТОРКОЛЬЦА

Определение 11.1 (Классы вычетов по модулю идеала).

Классами вычетов кольца R по модулю идеала I называют смежные классы $[r] = r + I$ аддитивной группы R по подгруппе I. Два различных элемента из одного класса вычетов называются *равными по модулю идеала.*

Определение 11.2 (Факторкольцо).

Факторкольцом R/I кольца R по модулю его двухстороннего идеала I называют кольцо классов вычетов с операциями:

$$[r_1] + [r_2] = [r_1 + r_2], \quad [r_1] \times [r_2] = [r_1 \times r_2].$$

Корректность проверить несложно:

$$[r_1] + [r_2] = (r_1 + I) + (r_2 + I) = (r_1 + r_2) + (I + I) = [r_1 + r_2],$$

$$[r_1] \times [r_2] = (r_1 + I) \times (r_2 + I) = r_1 r_2 + r_1 I + I r_2 + I \times I = (r_1 \times r_2) + I + I + I = [r_1 \times r_2].$$

Пример 11.1. Доказать, что факторкольцо $\mathbb{R}[x]/\langle x^2 + 1\rangle$ кольца $\mathbb{R}[x]$ многочленов с действительными коэффициентами по идеалу многочленов, делящихся на $x^2 + 1$, изоморфно полю комплексных чисел со стандартными операциями сложения и умножения.

Решение. Рассмотрим операции сложения и умножения в кольце классов вычетов многочленов по модулю $\langle x^2 + 1\rangle$:

$$[a_1 x + a_0] + [b_1 x + b_0] = [(a_1 + b_1)x + (a_0 + b_0)],$$

$$\begin{aligned}[a_1 x + a_0] \times [b_1 x + b_0] &= [a_1 b_1 x^2 + (a_0 b_1 + a_1 b_0)x + a_0 b_0] = \\ &= [a_1 b_1 (x^2 + 1) + (a_0 b_1 + a_1 b_0)x + (a_0 b_0 - a_1 b_1)] = [(a_0 b_1 + a_1 b_0)x + (a_0 b_0 - a_1 b_1)].\end{aligned}$$

Таким образом, если взаимно однозначно сопоставить классу $[ax+b]$ комплексное число $a+bi$, то операции сложения и умножения сохранятся. □

Определение 11.3 (Гомоморфное отображение колец).

Пусть заданы кольца R_1 и R_2. Отображение $\varphi\colon R_1 \to R_2$ называют *гомоморфным*, если

$$\forall x,y \in R_1\ \varphi(x+y)=\varphi(x)+\varphi(y), \quad \forall x,y \in R_1\ \varphi(x\times y)=\varphi(x)\times\varphi(y).$$

Гомоморфным образом кольца R_1 называют множество образов всех его элементов:

$$\operatorname{Im}\varphi=\varphi(R_1)=\{y\in R_2 \mid \exists x\in R_1\colon y=\varphi(x)\}.$$

Ядром гомоморфизма называют множество элементов, образ которых является нулевым элементом:

$$\operatorname{Ker}\varphi=\{x\in R_1 \mid \varphi(x)=0_{R_2}\}.$$

В примере 11.1 можно было рассмотреть гомоморфизм, который переводит каждый многочлен в комплексное число $a+bi$, где $ax+b$ — остаток от деления многочлена на x^2+1, и воспользоваться следующей теоремой.

Теорема 11.1. Теорема о гомоморфизме колец

Ядро гомоморфизма является идеалом, а гомоморфный образ кольца изоморфен факторкольцу по ядру гомоморфизма.

Пример 11.2. Пусть $P[x,y]$ — кольцо многочленов от двух переменных x и y над некоторым полем P, а I — множество всех многочленов этого кольца с нулевым свободным членом. Доказать, что:

а) I является идеалом, но не является главным идеалом;

б) факторкольцо $P[x,y]/I$ изоморфно полю P.

Решение.

а) Нетрудно показать, что I — подкольцо. Минимальная степень одночлена произведения двух многочленов равна сумме минимальных степеней одночленов множителей, поэтому результат умножения произвольного многочлена из $P[x,y]$ на многочлен, не имеющий свободного члена, так же не может содержать свободный член, т. е. I — идеал.

Если I — главный идеал, то должен быть $a(x,y) \in I$ — элемент, его порождающий. $x \in I$, поэтому

$$\exists p_x(x,y) \in P[x,y] \colon p_x(x,y)a(x,y) = x \Rightarrow a(x,y) = a(x).$$

Аналогично, $a(x,y) = a(y)$. Одновременно оба равенства могут выполняться, только если $a(x,y) = a = \text{const}$, но $aP[x,y] = P[x,y]$, если $a \neq 0$, и $aP[x,y] = \{0\}$, если $a = 0$.

б) Рассмотрим преобразование $\varphi(\sum\limits_{i,j} a_{ij}x^iy^j) = a_{00}$, сопоставляющее каждому многочлену его свободный член. Нетрудно видеть, что оно является гомоморфизмом, причем $\operatorname{Ker}\varphi = I$. Тогда, согласно теореме 11.1, факторкольцо $P[x,y]/I$ изоморфно $\operatorname{Im}\varphi$. Но образ φ составлен из свободных членов, которые образуют поле P.

□

Пример 11.3. Доказать, что любое гомоморфное отображение поля F в кольцо R является или изоморфным отображением на некоторое поле, входящее в R как подкольцо, или отображением в нулевой элемент R.

Решение. Рассмотрим гомоморфизм $\varphi \colon F \to R$. Пусть a, b — произвольные ненулевые элементы из $\operatorname{Im}\varphi$, тогда $\exists x, y \in F \colon \varphi(x) = a, \varphi(y) = b$. Проверим коммутативность:

$$a \times b = \varphi(x \times y) = \varphi(y \times x) = b \times a.$$

$\varphi(\iota_F) \times a = \varphi(\iota_F \times x) = \varphi(x) = a$, а, поскольку a выбран произвольно, $\iota_{\operatorname{Im}\varphi} = \varphi(\iota_F)$ — единица в $\operatorname{Im}\varphi$. $a \times \varphi(x^{-1}) = \varphi(x \times x^{-1}) = \varphi(\iota_F) = \iota_{\operatorname{Im}\varphi}$, поэтому $\varphi(x^{-1})$ — обратный элемент для a.

Таким образом, $\operatorname{Im}\varphi$ является кольцом (как гомоморфный образ кольца), коммутативным, с единицей, каждый элемент которого обратим, т. е. полем. □

Пример 11.4. Пусть $\mathbb{Z}$ — кольцо целых чисел, а R — кольцо с единицей ι. Доказать, что отображение $\varphi \colon \mathbb{Z} \to R$ такое, что $\varphi n = n\iota$, является гомоморфизмом.

Решение. Если $\forall n \in \mathbb{N}\ n\iota \neq 0$, то отображение φ, очевидно, является изоморфизмом с образом, составленным из всех элементов вида $z\iota$, где $z \in \mathbb{Z}$.

Пусть p — такое минимальное натуральное число, что $p\iota = 0$. Тогда $\varphi n = r\iota$, где r — остаток от деления n на p, а образом $\mathbb{Z}$ является набор элементов $0, \iota, \ldots, (p-1)\iota$, который образует подкольцо кольца R, изоморфное кольцу классов вычетов по модулю p. □

Пример 11.5. Пусть $\mathbb{Z}[i]$ — кольцо целых гауссовых чисел, $I = 2\mathbb{Z}[i]$ — множество всех чисел вида $m + ni$ с четными m и n.

а) Показать, что I — идеал в $\mathbb{Z}[i]$.

б) Найти классы вычетов $\mathbb{Z}[i]$ по модулю I.

в) Найти делители нуля в факторкольце $\mathbb{Z}[i]/I$.

Решение.

а) Несложно проверить, что I — подкольцо. Покажем, что выполняется свойство идеала. Пусть $z \in \mathbb{Z}[i]$ $(z = x + iy,\ x, y \in \mathbb{Z})$, $a \in I$ $(a = 2m + 2ni,\ m, n \in \mathbb{Z})$. Тогда $za = 2(xm - yn) + 2(xn + ym)i$, т. е. $za \in I$.

б) Элементы x и $x + 2m + 2ni$ порождают одинаковые классы вычетов по модулю I $([x] = x + I = x + (2m + 2ni + I) = (x + 2m + 2ni) + I = [x + 2m + 2ni])$. Таким образом, все классы вычетов можно описать набором $[0]$, $[1]$, $[i]$, $[1 + i]$.

в) $[1 + i] \times [1 + i] = [1 - 1 + 2i] = [0]$.

□

Пример 11.6. Доказать, что факторкольцо $\mathbb{Z}[i]/\langle 3\rangle$ кольца целых гауссовых чисел $\mathbb{Z}[i]$ по главному идеалу $\langle 3\rangle = 3\mathbb{Z}[i]$ является полем из девяти элементов.

Решение. Аналогично примеру 11.5, факторкольцо состоит из следующих элементов $[0]$, $[1]$, $[i]$, $[2]$, $[1 + i]$, $[2i]$, $[2 + i]$, $[1 + 2i]$, $2 + 2i$. Нетрудно заметить, что оно коммутативно и содержит единицу $[1]$, а $[0]$ — нулевой элемент. Остается показать, что каждый ненулевой имеет обратный. Для этого составим пары, произведения элементов которых равны $[1]$:

$$[1] = [1] \times [1] = [i] \times [2i] = [2] \times [2] = [1 + i] \times [2 + i] = [1 + 2i] \times [2 + 2i].$$

□