Содержание

1 Введение.

1.1 Функции, множества, отображения, основные алгебраические структуры.

Основные понятия и обозначения: $\emptyset, \subset, \cup, \cap, \setminus, \coprod, \times$.

Определение 1 *Функция — это тройка (X, Y, Γ), где X и Y — множества, а Γ — подмножество в $X \times Y$ такое, что для любого $x \in X$ существует единственный $y \in Y$, удовлетворяющий условию $(x, y) \in \Gamma$. При этом X называется областью определения, Y — множеством значений, а Γ — графиком функции.*

Определение 2 *Образ, прообраз, сужение, инъекция, сюръекция, биекция.*

Определение 3 *Композиция отображений, тождественное отображение, обратное отображение.*

Предложение 1 *Следующие условия на отображение $g := x \longrightarrow Y$ эквивалентны:*

1. *g биективно;*
2. *существует отображение $g' : Y \longrightarrow X$, такое, что $g \circ g' = \mathrm{id}_Y$, $g' \circ g = \mathrm{id}_X$;*
3. *g обадает левым и правым обратными отображениями.*

1.2 Отношения. Классы эквивалентности.

Определение 4 *Бинарное отношение между множествами X и Y — подмножество $Z \subseteq X \times Y$.*

Для $(x, y) \in Z$ часто используют обозначение xZy. Если $X = Y$, то будем говорить, что задано отношение на множестве X.

Примеры: $<, \leqslant, \equiv$, график функции.

Определение 5 *Бинарное отношение $\sim$ на X называется отношением эквивалентности, если для любых $x, y, z \in X$ выполнены следующие условия:*

1. *$x \sim x$(рефлексивность);*
2. *$x \sim y \Longleftrightarrow y \sim x$ (симметричность);*
3. *$x \sim y \& y \sim z \Longrightarrow x \sim z$ (транзитивность);*

Пусть $\sim$ — отношение эквивалентности на X, а $x \in X$. Классом эквивалентности элемента x, называется множество всех элементов, эквивалентных x.

Лемма 1 • *Два класса эквивалентности либо совпадают либо не пересекаются. Множество X распадается на дизъюнктное объединение классов эквивалентности.*

- *Всякого разбиение множества X на непересекающиеся подмножества есть разбиение на классы по некоторому отношению эквивалентности.*

Доказательство: В силу рефлексивности каждый элемент x лежит в своем классе эквивалентности. Обозначим через $\overline{x}$ класс эквивалентности элемента x. Легко видеть, что $X = \cup_{x \in X} \bar{x}$. Если теперь $\bar{x} \cap \bar{y} \neq \emptyset$ и $z \in \bar{x} \cap \bar{y}$, то $x \sim z$, $y \sim z$ и, в силу транзитивности $x \sim y$, откуда $\bar{x} = \bar{y}$. Значит различные классы не пересекаются. $\square$

Определение 6 *Фактормножеством $X/\sim$ называется множество классов эквивалентности.*

Определение 7 • *Частичным порядком на множестве X называется отношение $\preccurlyeq$, удовлетворяющее следующим условиям:*
для любых $x, y, z \in X$:

- $x \preccurlyeq x$ *(рефлексивность);*
- $x \preccurlyeq y \& y \preccurlyeq x \Longrightarrow x = y$ *(антисимметричность)*
- $x \preccurlyeq y \& y \preccurlyeq z \Longrightarrow x \preccurlyeq z$ *(транзитивность).*

Примеры: $\leqslant$ на $\mathbb{R}$, $\subseteq$ на множестве подмножеств множества X, делимость в $\mathbb{N}$, отношение $\leqslant$ на $C([0,1])$, где $f \leqslant g \Longleftrightarrow f(x) \leqslant g(x)$, $\forall x \in [0,1]$.

Определение 8 • *Отношение порядка называется линейным, если для любых $x, y \in X$ или $x \preccurlyeq y$ или $y \preccurlyeq x$.*

- *Элемент M частично упорядоченного множества A называется максимальным элементом, если*

$$\forall a \in A (a \geqslant M \Longrightarrow a = M).$$

- *Элемент m частично упорядоченного множества A называется наибольшим элементом, если $\forall a \in A : a \leqslant m$.*

Наибольший элемент всегда максимален. Максимальных элементов может быть много, а наибольший элемент, если существует, то определен однозначно. Аналогично определяются наименьший и минимальный элементы.

Определение 9 *Пусть X — частично упорядоченное множество и $Y \subseteq X$. Элемент $x \in X$ называется верхней гранью подмножества Y, если $y \leqslant x$ для всех $y \in Y$.*

Лемма 2 ***Лемма Цорна***
Частично упорядоченное множество, в котором любое линейно упорядоченное подмножество имеет верхрюю грань, содержит максимальный элемент.

Следствие 1 *Пусть семейство множеств $\mathfrak{M}$ обладает тем свойством, что объединение любого упорядоченного подмножества из $\mathfrak{M}$ есть снова множество из этого семейства. Тогда $\mathfrak{M}$ содержит максимальное множество.*

Примеры:

2 Теория групп.

Вступление. Пусть X — множество, а $\star : X \times X \longrightarrow X$ — бинарная операция на X. Рассмотрим следующие свойства.

1. $\forall x, y, z \in X : (x \star y) \star z = x \star (y \star z)$ (ассоциативность).
2. $\exists e \in X : \forall x \in X : e \star x = x \star e = x$ (e называетася нейтральным элементом).
3. $\forall x \in X \exists x' \in X : xx' = x'x = e$ (x' называется элементом обратным к x).
4. $\forall x, y \in X : x \star y = y \star x$ (коммутативность).

Рассмотрим множество всех отображений $X \longrightarrow X$, его элементы можно умножать с помощью композиции и такое умножение будет ассоциативно и обадает нейтральным элементом (тождественное отображение). Ясно, что отображение обладает обратным тогда и только тогда, когда оно является биекцией.

2.1 Полугруппы, группы.

Определение 10 *Множество X с операцией $\star$ называется*

- *полугруппой, если $\star$ ассоциативна;*
- *монойдом, если $\star$ ассоциативна и существует нейтральный элемент;*
- *группой, если $\star$ ассоциативна, существует нейтральный элемент и у каждого элемента есть обратный.*
- *абелевой группой, если X группа и $\star$ коммутативна.*

Простейшие свойства:

Лемма 3 *1. Нейтральный элемент единственнен.*

2. *Если операция ассоциативна и обладает нейтральным элементом, то элемент, обратный к данному, единственный.*
3. *Если в моноиде элементы x и y обратимы, то xy тоже обратим, причем $(xy)^{-1} = y^{-1}x^{-1}$.*

4. Множество обратимых элементов моноида является группой.

Доказательство:

1. $e = ee' = e'$.
2. Пусть y и y' — обратные к x, тогда $y' = y'e = y'(xy) = (y'x)y = ey = y$.

□

2.1.1 Примеры:

Как было показано выше, множество всех отображений $X \longrightarrow X$ является монойдом. В силу леммы множество его обратимых элементов является группой, которую мы будем называть симметрической группой множества X.

Симметрическая группа.

Определение 11 *X — множество. Симметрическая группа множества X:*
$S(X)$ — множество биекций $X \longrightarrow X$ с операцией композиции. Если $X = \{1, \ldots, n\}$, то $S(X)$ обозначается S_n и называется симметрической группой порядка n.

Запись перестановок. Циклическая запись перестановок. Транспозиция — цикл длины 2.

Определение 12 *Пусть $\sigma \in S_n$. Инверсией называется пара (i, j), $1 \leqslant i < j \leqslant n$, такая, что $\sigma(i) > \sigma(j)$. Четность количества инверсий называется четностью перестановки σ.*

Примеры:

1. $\mathbb{Z}, \mathbb{Q}^*, \mathbb{Q}^*_{>0}$;
2. четные целые числа, целые числа, кратные трем;
3. $\{1, -1\}$;
4. Повороты плоскости относительно фиксированной точки P и отражения относительно всех прямых, проходящих через точку P.
5. Пусть G — группа, S — непустое множество. Множество отображений $M(S, G)$ из S в G является группой; для любых двух отображений $f, g : S \longrightarrow G$ определеим

$$(fg)(x) := f(x)g(x).$$

Если G абелева, то такова же и $M(S, G)$.

Определение 13 *действие группы на множестве*

Пусть X — множество, G — монойд. Действие G на X (слева) — отображение

$$G \times X \longrightarrow X$$
$$(g, x) \mapsto gx,$$

такое, что для всех $g, h \in G$, $x \in X$

- $(gh)x = g(hx)$;
- $ex = x$.

Пусть G — группа. Тогда для каждого $g \in G$ отображение $G \times X \longrightarrow X$ индуцирует отображение $T_g : X \longrightarrow X$, задаваемое формулой $T_g(x) = gx$. Легко видеть, что каждое T_g есть перестановка множества X.

2.2 Подгруппы. Простейшие конструкции.

Определение 14 *Непустое подмножество H группы G называется подгруппой, если $ab, a^{-1} \in H$ для любых $a, b \in H$.*

Заметим, что подгруппа обязательно содержит нейтральный элемент и сама является группой относительно той же операции. Если H подгруппа G, то пишут $H \leqslant G$.

В любой группе есть две тривиальные подгруппы: сама группа и множество состоящее из одного нейтрального элемента.

Для подмножеств X и Y группы G будем обозначать $XY = \{xy | x \in X,\ y \in Y\}$, $X^{-1} = \{x^{-1} | x \in X\}$.

Лемма 4 *Пусть G — группа. Подмножество H является подгруппой группы G тогда и только тогда, когда H вместе с любыми элементами $a, b \in H$ содержит и элемент ab^{-1}.*

Примеры: 1) $4\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z} < \mathbb{Q}$;
2) $A_n < S_n$;
3) Пусть $Y \subset X$, тогда множество перестановок из $S(X)$ оставляющее на месте элементы множества Y, образует подгруппу группы $S(X)$.

Определение 15 *Пусть X — подмножество группы G. Подгруппой, порожденной множеством X, называется наименьшая подгруппа в G, содержащая X.*

Подгруппа, порожденная множеством X, обозначается $\langle X \rangle$. Так как пересечение подгрупп снова подгруппа, то подгруппа, порожденная X, всегда существует и

$$\langle X \rangle = \bigcap_{X \subset H \leqslant G} H.$$

Лемма 5 *$\langle X \rangle$ состоит из всех элементов вида $x_1 \dots x_k$, где k — некоторое натуральное число, а $x_i \in X \cup X^{-1}$.*

2.2.1 Подгруппа, порожденная одним элементом; порядок элемента.

Определение 16 *Подгруппа, порожденная одним элементом называется циклической. Порядок подгруппы, порожденной элементом a называется порядком элемента a.*

Ясно, что $\langle a \rangle = \{a^i | i \in \mathbb{Z}\}$. Есть две возможности. Либо все степени a^i различны и тогда $\langle a \rangle$ бесконечна, либо они повторяются, т.е. $a^k = a^l$, $k, l \in N, k > l$. Но тогда $a^{k-l} = e$. Покажем, что $\operatorname{ord} a = \min\{n | a^n = e, n > 0\}$. Действительно, все степени $a^0, a, \dots, a^{n-1}$ различны и $a^m = a^{m \bmod n}$, поэтому $\langle a \rangle = \{a^0, a, \dots, a^{n-1}\}$.

2.3 Гомоморфизмы, ядро и образ гомоморфизма.

Определение 17 *Пусть $(G, \star)$ и $(H, \cdot)$ — группы. Функция $f : G \longrightarrow H$ называется гомоморфизмом, если $f(a \star b) = f(a) \cdot f(b)$ для любых $a, b \in G$.*

Определение 18 *Ядро гомоморфизма* $\operatorname{Ker} f = f^{-1}(e)$*; образ гомоморфизма* $\operatorname{Im} f = \{f(x) | x \in G\}$.
Мономорфизм — инъективный гомоморфизм, эпиморфизм — сюръективный гомоморфизм, изоморфизм — биективный изоморфизм.

Лемма 6 *Если $f : G \longrightarrow H$ — гомоморфизм групп, то $f(e_G) = e_H$ и $f(x^{-1}) = (f(x))^{-1}$ для любого $x \in G$.*

Лемма 7 *Пусть $f : G \longrightarrow H$ — гомоморфизм групп, $g \in G$, а $h = f(g)$. Тогда $f^{-1}(h) = g \operatorname{Ker} f$.*
Гомоморфизм инъективен тогда и только тогда, когда его ядро состоит из одного элемента.

Теорема 1 *Теорема Кэли*
Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.

Доказательство: Пусть G — группа, $|G| = n$ и $G = \{x_1, \ldots, x_n\}$. Поставим элементу $g \in G$ в соответствие подстановку $\sigma_g \in S_n$ такую, что $x_i g = x_{\sigma(i)}$. Нетрудно проверить, что $\sigma_g \in S_n$ и полученное соответствие является мономорфизмом. $\square$

2.4 Смежные классы, теорема Лагранжа.

Определение 19 *Пусть H — подгруппа в группе G. Левый смежный класс группы G по H — это подмножество в G вида aH, где $a \in G$. Элемент a называют представителем класса aH. Аналогично определяются правые смежные классы. G/H — множество всех левых смежных классов. $H\backslash G$ — правых.*

Определим $a \equiv b \mod H \iff a \in bH \iff b^{-1}a \in H \iff aH = bH$.

Лемма 8 *1. Сравнимость по модулю H является отношением эквивалентности. Два смежных класса либо совпадают, либо не пересекаются.*

2. Множества G/H и $H\backslash G$ равномощны, т.е. между ними существует биекция. В частности, если количество левых или правых смежных классов конечно, то $|G/H| = |H\backslash G|$.

3. Любые два смежных класса равномощны, т.е. между ними существует биекция. В частности, если они конечны, то они содержат одинаковое количество элементов.

Доказательство:

1. (a) рефлексивность: $a = ae \in aH$.
   (b) симметричность: $a \in bH \Longrightarrow \exists h \in H : a = bh \Longrightarrow b = ah^{-1} \in aH$.
   (c) транзитивность: пусть $a \in bH$, $b \in cH$, тогда $a = bh$, $b = ch'$, $h, h' \in H \Longrightarrow a = chh' \in cH$.
2. Биекция $G/H \longrightarrow H\backslash G$ задается по правилу $aH \mapsto (aH)^{-1} = Ha^{-1}$.
3. Отображение $x \mapsto ax$ индуцирует биекцию H на aH.

$\square$

Количество смежных классов называют индексом подгруппы H в G и обозначают $|G : H|$.

Теорема 2 *(теорема Лагранжа).*
Если H — подгруппа конечно группы G, то $|G| = |H| \cdot |G/H|$.

Примеры:

2.5 Нормальные подгруппы, факторгруппы

Определение 20 *Нормальная подгруппа*
Подгруппа H группы G называется нормальной, если для любых $g \in G$ и $h \in H$ имеет место включение $ghg^{-1} \in H$. В других обозначениях $gHg^{-1} \subset H$.

Заметим, что любая подгруппа абелевой группы является нормальной.

Лемма 9 *Следующие утверждения равносильны:*

1. *Подгруппа H группы G является нормальной.*
2. $\forall g \in G : gH = Hg$.
3. $\forall g \in G : gHg^{-1} = H$.

Лемма 10 *Пусть $f : G \longrightarrow H$ — гомоморфизм групп. Тогда* $\operatorname{Im} f \leqslant H$, $\operatorname{Ker} f \lhd G$.
Более того, всякая нормальная подгруппа является ядром некоторого гомоморфизма.

Факторгруппа Пусть $H \lhd G$. Положим $F = G/H$ и зададим операцию в F по формуле $(xH) \cdot (yH) = xyH$. Так как H — нормальная подгруппа в G, то эта операция задана корректно. Для этого необходимо проверить, что операция не зависит от выбора представителей x и y смежных классов xH и yH. Действительно, $xhyh' = xy(y^{-1}hy)h' \in xyH$. Нетрудно проверить, что относительно рассмотренной операции F является группой. Построенная группа называется факторгруппой G по H.

Ясно, что всякая нормальная подгруппа $H \leqslant G$ является ядром естественного эпиморфизма (проекции)

$$G \longrightarrow G/H$$
$$g \mapsto gH.$$

Пример: $\mathbb{Z}/n\mathbb{Z}, |\mathbb{Z} : n\mathbb{Z}| = n$;

2.6 Теорема о гомоморфизме.

Теорема 3 *Пусть G, G' и $G"$ — группы, $f : G \longrightarrow G'$ — эпиморфизм, а $g : G \longrightarrow G"$ — гомоморфизм. Если $\operatorname{Ker} f = \operatorname{Ker} g$, то существует единственный мономорфизм $h : G' \longrightarrow G"$ такой, что $g = h \circ f$. Если g — эпиморфизм, то h — изоморфизм.*

(этой теоремы не было на лекциях)

Следствие 2 *(теорема о гомоморфизме групп)*
Пусть $f : G \longrightarrow G_1$ *— гомоморфизм групп. Тогда* $\operatorname{Im} f \cong G/\operatorname{Ker} f$.

2.7 Сопряжение элементов. Разбиение на классы сопряженности.

Будем говорить, что элемент a сопряжен с элементом b посредством элемента x, если $a = x^{-1}bx$. Иногда для $x^{-1}bx$ используется обозначение b^x. Заметим, что подгруппа H группы G является нормальной тогда и только тогда, когда $H^G \subset H$. Заметим также, что при фиксированном $x \in G$ отображение $\varphi_x : a \mapsto a^x$ является автоморфизмом группы G.

Легко проверить, что отношение сопряженности является отношением эквивалентности. Таким образом множество элементов группы распадается на классы сопряженных элементов. Более того, множество всех подгрупп группы G распадается на непересекающиеся классы сопряженных подгрупп.

Замечание 1 *В отличие от смежных классов классы сопряженных элементов не всегда равномощны.*

Определение 21 *Нормализатор множества* M *в подгруппе* H

$$N_H(M) = \{h | h \in H, M^h = M\} = \{h | h \in H, hM = Mh\}.$$

Замечание 2 *Легко видеть, что* $N(M) < H$.
Нормализатор подгруппы H *в* G *является максимальной подгруппой в* G, *в которой* H *является нормальной подгруппой.*

Теорема 4 *Пусть* M *подмножество, а* H *— подгруппа группы* G. *Тогда мощность класса подмножеств, сопряженныз с* M *элементами из* H, *равна* $|H : N_H(M)|$. *В частности,*

$$|a^G| = |G : N_G(a)|.$$

Доказательство: Имеется следующая биекция между классами подмножеств, сопряженных с M в H и смежными классами группы H по $N_H(M)$. Отобразим множество M^x в $xN_H(M)$ для $x \in H$. $\square$

2.8 Симметрическая группа степени n.

Изучим подробнее строение группы S_n.

1. Всякая подстановка однозначно раскладывается в произведение независимых циклов (с точностью до порядка циклов).
2. Группа S_n порождается множеством транспозиций $(12), (23), \ldots, (n-1, n)$.

3. Порядок цикла длины k равен k.

4. Если циклы независимы, то они коммутируют.

5. Если подстановка σ раскладывается в произведение независимых циклов длин $k_1, \ldots, k_l$, то $\operatorname{ord}\sigma = \operatorname{lcm}(k_1, \ldots, k_l)$.

6. Два элемента S_n сопряжены тогда и только тогда, когда в разложении на независимые циклы они содержат одинаковое число циклов каждой длины, включая и одноэлементные циклы.

2.9 Циклические группы. Дискретный логарифм.

Предварительные замечания о порядках элементов

Лемма 11 *Пусть $ordg = n$. Тогда*

1. $g^m = e \iff n|m$.
2. $g^k = g^l \iff k \equiv l \mod n$.

Доказательство:

1. Разделим m на n с остатком:

$$m = qn + r,\ 0 \leqslant r < n.$$

Тогда

$$g^m = (g^n)^q \cdot g^r = g^r$$
$$g^r = e \iff r = 0$$

2. В силу предыдущего

$$g^k = g^l \iff g^{k-l} = e \iff n|(k-l) \iff k \equiv l \mod n.$$

□

Лемма 12 *Если $ordg = n$, то* $\operatorname{ord} g^k = \frac{n}{(n,k)}$.

Доказательство: Пусть $d = (n, k)$, $n = dn_1, k = dk_1$, т.е. $(n_1, k_1) = 1$. Тогда

$$(g^k)^m = e \iff n|km \iff n_1|k_1 m \iff n_1|m.$$

Следовательно $\operatorname{ord} g^k = n_1$.

□

Следствие 3 $\langle g^k \rangle = \langle g \rangle \iff (k, n) = 1$.

Циклические группы.

Определение 22 *Группа называется циклической, если она порождается одним элементом. Иными словами, существует такой элемент $g \in G$, что $G = \langle g \rangle = \{g^n | n \in \mathbb{Z}\}$.*

Примеры:$\mathbb{Z}, k\mathbb{Z}$;$\mathbb{Z}/n\mathbb{Z}$; Группа вращений правильного n-угольника.

Лемма 13 *Подгруппа циклической группы циклическая.*

Доказательство: Пусть G — циклическая группа и $H \leqslant G$. Если $H = \{e\}$, то H, очевидно, циклическая. Пусть $H \neq \{e\}$, тогда $\{n \in \mathbb{N} | g^n \in H\} \neq \emptyset$. Пусть d — наименьшее натуральное число такое, что $g^d \in H$. Покажем, что $H = \langle g^d \rangle$. Действительно, пусть $g^m \in H$. Представим m в виде $m = qd + r$, $0 \leqslant r < d$. Тогда $g^r = g^m (g^{qd})^{-1} \in H$, что противоречит минимальности r если $r \neq 0$. Значит, $r = 0$ и все элементы H являются степенями g^d. $\square$

Следствие 4 *Каждая подгруппа аддитивной группы $\mathbb{Z}$ имеет вид $n\mathbb{Z}$ для некоторого $n \in \mathbb{N}_0$.*

Теорема 5 *Если циклическая группа G бесконечна, то она изоморфна $\mathbb{Z}$. Конечная циклическая группа изоморфна $\mathbb{Z}/n\mathbb{Z}$, где n — порядок G.*

Доказательство: Пусть $G = \langle g \rangle$. Рассмотрим гомоморфизм

$$\varphi : \mathbb{Z} \longrightarrow G$$
$$m \mapsto g^m.$$

(φ — гомоморфизм, т.к. $g^{k+l} = g^k g^l$, более того φ — эпиморфизм, т.к. G циклическая). Если $\operatorname{Ker} \varphi = \{0\}$, то φ — изоморфизм. Если $\operatorname{Ker} \varphi \neq \{0\}$, то в силу следствия 4 получаем $\operatorname{Ker} \varphi = n\mathbb{Z}, n \in \mathbb{N}$. По теореме о гомоморфизме $G \cong \mathbb{Z}/\operatorname{Ker} \varphi = \mathbb{Z}/n\mathbb{Z}$. $\square$

Следствие 5 *Пусть G — конечная циклическая группа порядка n. Тогда для каждого делителя $d|n$ существует единственная подгруппа порядка d.*

Доказательство: Пусть $d|n$, тогда по лемме 12 $\operatorname{ord} g^{n/d} = d$, т.е. элемент $g^{n/d}$ порождает подгруппу порядка d. Остается показать, что такая подгруппа единственная. Пусть $H < G$ и $|H| = d$. Если $d = 1$, то $H = \{e\}$ и доказывать нечего. Пусть $d \neq 1$. По лемме 13 группа H циклическая, а значит $H = \langle g^m \rangle$. Тогда в силу предварительных замечаний $d = |H| = \operatorname{ord} g^m = \frac{n}{(m,n)}$. Следовательно $\frac{n}{d} | m$, а значит $H = \langle g^m \rangle \leqslant \langle g^{n/d} \rangle$. Но, так как $|H| = d = |\langle g^{n/d} \rangle|$, то $H = \langle g^{n/d} \rangle$. $\square$

Определение 23 *Элемент группы $\mathbb{Z}/n\mathbb{Z}$ называется первообразным корнем по модулю n если он является порождающим группы $(\mathbb{Z}/n\mathbb{Z})^*$.*

Следствие 6 *Пусть G — конечная циклическая группа порядка n. Тогда для каждого делителя $d|n$ в G существует единственная подгруппа H индекса d. Факторгруппа G/H является циклической группой порядка d.*

Доказательство: В G существует единственная подгруппа H порядка n/d, а именно $H = \langle g^d \rangle$. Легко видеть, что $G/H = \langle gH \rangle$, $g^d \in H$. $\square$

Замечание 3 *Фактически мы доказали следующее утверждение:*
Пусть $G = \langle d \rangle$ — конечная циклическая группа и $n = |G|$.

1. *Пусть $m|n$. Тогда $H = \{g \in G | g^m = 1\} \leqslant G$ и $|H| = m$.*
2. *Пусть $H \leqslant G$ и $m = |H|$. Тогда $m|H$ и $H = \{g \in G | g^m = 1\}$.*

2.9.1 Дискретный логарифм.

Определение 24 *Пусть $G = \langle d \rangle$ — конечная циклическая группа и $n = |G|$. $\exp_d$ — изоморфизм $\mathbb{Z}/nZ \longrightarrow G$, заданный равенством $\exp_d(\overline{a}) = d^a$. Дискретный логарифм по основанию d на группе G — обратный изоморфизм $\exp_d^{-1}$.*

Пусть C_n обозначает циклическую группу из n элементов.

2.10 Прямое произведение групп. Разложение конечной циклической группы в прямое произведение

Определение 25 *Прямое произведение групп G и H — $G \times H$ с операцией $(g, h) \times (g_1, h_1) = (gg_1, hh_1)$.*

Легко проверить, что определенная выше структура действительно является группой.

Теорема 6 *Пусть G — группа и $F, H \leqslant G$. Тогда следующие свойства эквивалентны:*

- $G = FH$, $F \cap H = \{1\}$ *и* $\forall f \in F$, $h \in H (fh = hf)$;
- *отображение*

$$F \times H \longrightarrow G$$
$$(f, h) \mapsto fh,$$

является изоморфизмом групп.

Доказательство: Нетрудно проверить, что

$$f \text{ — гомоморфизм} \iff$$
$$\iff \forall f_1, f_2 \in F, h_1, h_2 \in H \ f_1 f_2 h_1 h_2 = f_1 h_1 f_2 h_2 \iff$$
$$\iff \forall f \in F, h \in H fh = hf (f_1 = e, h_2 = e)$$
$$f\text{— сюръ} \iff \forall g \in G,\ g = fh \iff G = FH$$
$$f \text{ — инъ} \iff \forall f_1, f_2 \in F, h_1, h_2 \in H \ (f_1 h_1 = f_2 h_2 \Longrightarrow f_1 = f_2, h_1 = h2) \iff$$
$$\iff F \cap H = \{e\}.$$

□

Замечание 4 *В случае если G — конечная группа, условие $G = FH$ можно заменить на $|G| = |F||H|$.*

Теорема 7 *Пусть $m, n \in \mathbb{N}$. Тогда $C_{mn} \cong C_m \times C_n \iff \gcd(m, n) = 1$.*

Доказательство: $\Longrightarrow$
Заметим, что $\forall g \in C_m \times C_n \operatorname{ord} g | \text{НОК}(m, n) = \frac{mn}{(m,n)}$. Поэтому, если $(m, n) \neq 1$, то группа $C_m \times C_n$ не является циклической.
$\Longleftarrow$
Пусть $(m, n) = 1$. По теореме о подгруппах циклической группы в группе C_{mn} существуют подгруппы C_m и C_n порядков m и n соответственно. Применяя к ним предудущую теорему получаем требуемое. □

2.11 Свободные группы; группы, заданные образующими и соотношениями

Пусть G — группа. S — подмножество G. Если $\langle S \rangle = G$, то элементы S называются образующими. Если у G существует конечное множество образующих, то G - конечно порожденная.

Свободные группы Зафиксируем два множества символов

$$X = \{x_i | i \in I\} \qquad X^{-1} = \{x_i^{-1} | i \in I\}.$$

Слово в алфавите X — это пустая (1) или конечная последовательность символов из $X \cup X^{-1}$. Число элементов этой последовательности называется длиной слова. Слово несократимо, если оно содержит подслов вида $x_i x_i^{-1}, x_i^{-1} x_i$. На множестве слов (т.е. $\cup (X \cup_{n \geqslant 0} X^{-1})^n$) введем следующее отношение эквивалентности: слова u и v эквивалентны, если v можно получить из u через конечное число вставок и сокращений слов вида $x_i^e x_i^{-e}$, $e = \pm 1$. Пусть $[u]$ обозначает класс эквивалентности слова u. На множестве классов эквивалентных слов $F(X)$ определим умножение, полагая $[u][v] = [uv]$.

Предложение 2 *Так определенное умножение корректно, т.е. не зависит от выбора представителей в классах. Множество $F(X)$ является группой относительно этого умножения.*

Теорема 8 *Каждый класс слов $[u]$ содержит единственное несократимое слово $\overline{u}$.*

Доказательство:

Нетрудно убедиться, что слово наименьшей длины в классе $[u]$ являетя неприводимым. Пусть теперь $u \sim v$ для несократимых слов u, v. Тогда существует последовательность

$$u = u_0, u_2, \ldots, u_n = v,$$

в которой соседние слова получаются друг из друга одной вставкой или сокращением подслова вида $x^{\varepsilon}x^{-\varepsilon}, \varepsilon = \pm 1$. Так как $u \neq v$, то $n \geqslant 2$. Среди всех таких цепочек выберем цепочку $u = u_0, u_2, \ldots, u_n = v$, которая имеет минимальную длину и среди всех цепочек минимальной длины сумма длин, входящих в нее слов наименьшая. Поскольку u и v несократимы, то $l(u) < l(u_1), l(u_{n-1}) > l(v)$. Тогда найдется такой индекс $i : 1 \leqslant i \leqslant n-1$, что $l(u_i) > l(u_{i-1}), l(u_{i+1})$. Это значит, что u_{i+1} получается из u_i вычеркиванием какого-то фрагмента вида $x^{\varepsilon}x^{-\varepsilon}, \varepsilon = \pm 1$, а u_{i-1} — вычеркиванием какого-то фрагмента вида $y^{\varepsilon}y^{-\varepsilon}, \varepsilon = \pm 1$. Если эти фрагменты пересекаются, то $u_{i-1} = u_{i+1}$, что означает существование более короткой цепочки. Если они не пересекаются, то мы могли бы сначала вычеркнуть фрагмент $y^{\varepsilon}y^{-\varepsilon}, \varepsilon = \pm 1$ и только потом вставить фрагмент $x^{\varepsilon}x^{-\varepsilon}, \varepsilon = \pm 1$, получив таким образом цепочку с меньшей суммой длин слов.

Оставшаяся часть доказательства предлагается в виде упражнения. □
Группа $F(X)$ называется свободной группой с порождающим множеством X.

Теорема 9 *Всякая группа изоморфна фактор-группе некоторой свободной группы.*

Лемма 14 *Пусть группа G порождается множеством $M = \{g_i | i \in I\}$. Возьмем алфавит $X = \{x_i | i \in I\}$. Отображение $X \longrightarrow M$ по правилу $x_i \mapsto g_i$ единственным образом продолжается до гомоморфизма $F(X) \longrightarrow G$.*

Элементы ядра гомоморфизма $F(X) \longrightarrow G$ называются соотношениями группы G в алфавите X. Если множество H' соотношений таково, что минимальная нормальная подгруппа в $F(X)$, содержащая H', совпадает с H, то H' называется определяющим множеством соотношений в алфавите X.

Пример: Пусть $s_i = (i, i+1)$, $1 \leqslant i \leqslant n-1$. Группа S_n допускает задание

$$S_n = \langle s_1, \ldots, s_{n-1} | s_i^2 = 1,\ (s_i s_j)^2 = 1, |i-j| \geqslant 2; (s_i s_{i+1})^3 = 1,\ 1 \leqslant i \leqslant n-2 \rangle =$$
$$= \langle s_1, \ldots, s_{n-1} | s_i^2 = 1,\ s_i s_j = s_j s_i, |i-j| \geqslant 2; s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1},\ 1 \leqslant i \leqslant n-2 \rangle$$

2.12 Действия групп. Разбиение на орбиты. Стабилизаторы, неподвижные точки. Лемма Бернсайда.

Напомним, что действие G на X(слева) — отображение

$$G \times X \longrightarrow X$$
$$(g, x) \mapsto gx,$$

такое, что для всех $g, h \in G$, $x \in X$

- $(gh)x = g(hx)$;
- $ex = x$.

Замечание 5 *Пусть $G \times X \longrightarrow X$ задает действие группы G на множестве X. Нетрудно проверить, что для каждого $g \in G$ отображение $\theta_g : X \longrightarrow X$, $x \mapsto gx$ является биекцией. Тогда из свойств (2.12) следует, что сопоставление $g \mapsto \theta_g$ является гомоморфизмом групп $G \longrightarrow S(G)$.*

Пример:

1. Группа S_n действует на множестве $\{1, \ldots, n\}$.
2. Действие левыми сопряжениями:

$$G \times G \longrightarrow G$$
$$(g, x) \mapsto gxg^{-1}$$

Рассмотрим следующее отношение на множестве X:
$x \sim y \Longleftrightarrow \exists g \in G : gx = y$. Нетрудно проверить, что $\sim$ — отношение эквивалентности. Таким образом множество X разбивается на непересекающиеся классы эквивалентности, которые называются орбитами. Фактор-множество $X/\sim$ обозначается X/G и называется множеством орбит для действия G на X. Если имеется единственная орбита, то будем говорить, что группа G действует транзитивно.

Определение 26 *Орбитой элемента $x \in X$ называется подмножество $Gx = \{gx | g \in G\}$.*

Определение 27 *Стабилизатором элемента $x \in X$ называется подмножество*

$$G_x = \{g \in G | gx = x\}.$$

Лемма 15 *Пусть $x \in X$. Тогда*

1. *$G_x \leqslant G$;*
2. *Соответствие $G_x g \longleftrightarrow gx$ является биекцией между смежными классами по G_x и орбитой Gx.*
3. *$|G| = |Gx| \cdot |G_x|$;*
4. *$G_{ax} = aG_x a^{-1}$.*

Доказательство.

1. проверяется непосредственно;
2. Соответствие $gG_x \longleftrightarrow gx$ является биекцией между смежными классами по G_x и орбитой Gx.
3. Следует из предыдущего пункта и теоремы Лагранжа.
4. $g \in G_{ax} \iff gax = ax \iff a^{-1}gax = x \iff g \in aG_x a^{-1}$.

□

Пусть $g \in G$

$$X^g = \{x \in X | gx = x\}.$$

Лемма 16 *(лемма Бернсайда) Пусть G — конечная группа, действующая на X.*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Доказательство. Заметим, что $|G| = |Gx| \cdot |G_x|$. Поэтому

$$\sum_{g \in G} |X^g| = \{(g, x) \in G \times X | gx = x\} = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|Gx|} =$$
$$= |G| \cdot |X/G|.$$

□

2.13 Абелевы группы.

Рассматривая абелевы группы будем использовать аддитивную запись (а не мультипликативную). Вместо прямого произведения конечного числа абелевых групп будем говорить о их прямой сумме $\oplus$.

Примеры:

Абелева группа называется периодической, если порядки всех ее элементов конечны, группой без кручения, если все элементы, кроме нуля, имеют бесконечный порядок. Абелевы группы, порядки всех элементов которых являются степенями фиксированного простого числа p называются примарными по простому числу p.

Примарное разложение. Пусть p — простое и $p \mid |G|$. Обозначим через G_p множество всех элементов группы G, чей порядок является степенью p, т.е. $G_p = \{g \in G | \operatorname{ord} g = p^m, m \in \mathbb{N}\}$. Нетрудно проверить, что $G_p \leqslant G$ и $|G_p| = p^n$, $n \in \mathbb{N}$.

Лемма 17 *Пусть $p_1, \ldots, p_s$ — все простые, делящие порядок группы G. Тогда $G = G_{p_1} \oplus \ldots \oplus G_{p_s}$.*

Более того это разложение G единственно, а именно если $G = B_1 \oplus \ldots \oplus B_s$, где $|B_i| = p_i^{r_i}$, то $B_i = G_{p_i}$.

Доказательство: Легко видеть, что $G_p \leqslant G$ и $G_p \cap G_q = \{0\}$ при различных p и q. Поэтому сумма всех G_p прямая. Более того, в силу теоремы 7 $\sum G_p$ совпадает с G.

Покажем, что такое разложение единственно. Ясно, что $B_i \leqslant G_{p_i}$. Далее, пусть $0 \neq x \notin B_i$. Так как $G = \sum B_j$, то x можно представить в виде $x = \sum x_j$, $x_j \in B_j$, где $x_j \neq 0$ хотя бы для одного $j \neq i$. Тогда $\operatorname{ord}(x) = \prod \operatorname{ord}(x_j)$, (т.к. $\operatorname{ord}(x_j) \mid p^j$, а значит взаимно просты.) Последнее означает, что $x_j \notin G_{p_i}$.

□

Замечание 6 *Можно было не предполагать конечность группы G. Достаточно, чтобы группа G была периодической, а p_i — все простые, делящие порядки элементов группы G. В частности, из леммы следует, что всякая конечно порожденная периодическая абелева группа конечна. Для неабелевых групп аналогичное утверждение верным уже не будет.*

разложение на циклические слагаемые.

Представление абелевых групп в виде произведения циклических.

Теорема 10 *Каждая конечная абелева группа является прямой суммой примарных циклических групп.*

Доказательство: По предыдущей лемме достаточно показать, что любая абелева p-группа G допускает нетривиальное разложение в прямую сумму. Пусть $|G| = p^n$. Пусть A — максимальная циклическая подгруппа G. Тогда $|A| = p^l$, где p^l — наибольший порядок элемента в G, т.е $p^l G = 0$, $p^{l-1}G \neq 0$. Индукцией по порядку G покажем, что найдется такая подгруппа $B \leqslant G$, что $G \cong A \oplus B$.

Построим сначала нетривиальную подгруппу $H \leqslant G$ такую, что $A \cap H = \{0\}$. Для этого сначала заметим, что не все элементы порядка p лежат в A. Т.к. A — циклическая, то в силу доказанных выше утверждений, в ней содержится ровно p элементов порядка p. Ясно, что все элементы из $p^{l-1}G$ либо равны 0 либо имеют порядок p. Но, т.к. $p^{l-1}G \neq 0$, то $|p^{l-1}G| = p$. Таким образом $\forall 0 \leqslant k \leqslant l-2$: ядро гомоморфизма умножения на p совпадает с $p^{l-1}G$ и содержит ровно p элементов, поэтому $|p^k G| = p|p^{k+1}G|$ для $0 \leqslant k \leqslant l-2$. Таким образом $|G| = p|pG| = p^2|p^2G| = \ldots = p^{l-1}|p^{l-1}G| = p^l = |A|$, что влечет $G = A$, а значит G — циклическая.

Таким образом в G найдется элемент x порядка p, не лежащий в A. Тогда нам подойдет $H = \langle x \rangle$.

Рассмотрим теперь каноническую проекцию $\varphi : G \longrightarrow G/H$. По индукционному предположению найдется такая подгруппа $C \leqslant G/H$, что $G/H = \varphi(A) \oplus C$. Положим $B = \varphi^{-1}(C)$. Т.к. $B \geqslant H$, то $G = A + B$. Чтобы показать, что $G = A \oplus B$, осталось показать, что $A \cap B = \{0\}$. Действительно, если $x \in A \cap B$, то $\varphi(x) \in \varphi(A) \cap C = \{0\}$, что означает, что $x \in \operatorname{Ker}\varphi = H$, но $H \cap A = \{0\}$. $\square$

Замечание 7 *Фактически мы доказали следующее утверждение:*
Пусть A — конечная абелева p-группа, $|A| = p^r$, $r \geqslant 1$. Тогда $A \cong A_1 \oplus \ldots \oplus A_k$, где $A_i = \langle a_i \rangle, \operatorname{ord}(a_i) = p^{c_i}$, $r = c_1 + \ldots + c_k$ (т.е. $A \cong C_{p^{c_1}} \times \ldots \times C_{p^{c_k}}$ или же $A \cong \oplus_{i=1}^k \mathbb{Z}/p^{c_i}\mathbb{Z}$ если придерживаться аддитивной записи).

Последнее разложение единственно:

Лемма 18 *Последовательность $c_1, \ldots, c_k$ определена однозначно, а именно: если $A \cong C_{p^{c'_1}} \times \ldots \times C_{p^{c'_l}}$, то $k = l$ и множества $c'_1, \ldots, c'_k$ и $c_1, \ldots, c_k$ совпадают.*

Прежде чем будет приведено доказательство леммы, перечислим несколько тривиальных утверждений, доказательство которых рекомендуется оставить в качестве упражнений и которые периодически используются в приведенных доказательствах.

1. Если $f : G \longrightarrow H$ — изоморфизм групп и $g \in G$, то $\mathrm{ord}(g) = \mathrm{ord}(f(g))$.
2. $m\mathbb{Z}/(mn\mathbb{Z}) = \{mx | x \in \mathbb{Z}/mn\mathbb{Z}\} \cong \mathbb{Z}/n\mathbb{Z}$.
3. $C_{mn}^m \cong C_n$(мультипликативная формулировка предыдущего утверждения).

Доказательство: Покажем,сначала что $k = l$. Для этого посчитаем количество элементов порядка p в группе A. Если $x \in A \cong C_{p^{c'_1}} \times \ldots \times C_{p^{c'_l}}$, то $x = x_1 \ldots x_l, x \in C_{p^{c'_i}}$. Тогда $x^p = 1$ тогда и только тогда, когда $x_i^p = 1$ для всех $1 \leqslant i \leqslant l$. Но, как нам известно, в $C_{p^{c'_i}}$ ровно p элементов порядка p. Таким образом в группе A ровно p^l элементов порядка p. Тем же образом можно получить, что их ровно p^k. Таким образом $k = l$.
Покажем теперь, что наборы c_i и c'_i совпадают. Для удобства предположим, что $c_1 \leqslant c_2 \leqslant \ldots \leqslant c_k$ и $c'_1 \leqslant c'_2 \leqslant \ldots \leqslant c'_k$. Пусть $c_1 = c'_1, c_2 = c'_2, \ldots, c_{s-1} = c'_{s-1}, c_s \neq c'_s$. Пусть $c_s < c'_s$. Тогда

$$A^{p^{c_s}} \cong C_{p^{c_{s+1}}}^{p^{c_s}} \times \ldots \times C_{p^{c_k}}^{p^{c_s}}.$$

С другой стороны

$$A^{p^{c_s}} \cong C_{p^{c'_s}}^{p^{c_s}} \times \ldots \times C_{p^{c_k}}^{p^{c_s}}.$$

Получили два разложения с разным количеством сомножителей, что противоречит доказанному выше.□

Полученные выше утверждения дают полную классификацию конечных абелевых групп. Следующая теорема дает представление о структуре всех конечно порожденных абелевых групп.

Теорема 11 *Пусть G — конечно порожденная абелева группа. Тогда*

$$G \cong T(G) \oplus G',$$

где $G' \cong \bigoplus_{i=1}^k \mathbb{Z}$, а $T(G)$ — конечная абелева группа (и, соответственно, $T(G) \cong \bigoplus_{i=1}^l (\mathbb{Z}/p_i^{c_i}\mathbb{Z})$).

3 Коммутативные кольца.

Определение 28 *ассоциатвное кольцо, кольцо с 1, коммутативное кольцо, поле*

Лемма 19 *R — кольцо. $r \in R$. Тогда*

1. $0 \cdot r = r \cdot 0 = 0$;
2. *Если R — кольцо с единицей, то $-1 \cdot r = -r$.*

По лемме 3 множество обратимых (по умножению) элементов кольца R образует группу. Эта группа называется мультипликативной группой кольца и обозначается R^*.

3.0.1 Числовые кольца, свободные кольца, кольца эндоморфизмов. Характеристика. Эндоморфизм Фробениуса.

Определение 29 *гомоморфизм колец Пусть R и A — кольца. Функция $f := R \longrightarrow A$ называется гомоморфизмом, если $f(a+b) = f(a) + f(b)$ и $f(ab) = f(a)f(b)$ для любых $a, b \in R$.*

Замечание 8 *Гомоморфный образ кольца с 1 не обязательно содержит единицу (постройте пример).*

Лемма 20 *Любой ненулевой гомоморфизм произвольного кольца с единицей в область целостности переводит единицу в единицу.*

Далее по умолчанию все кольца являются кольцами с единицей, а все гомоморфизмы являются гомоморфизмами колец с единицей, т.е. $f(1) = 1$.

Определение 30 *Ядро и образ гомоморфизма. Мономорфизм, эпиморфизм, изоморфизм.*

Лемма 21 *Если $f : R \longrightarrow A$ — гомоморфизм колец, то $f(0) = 0$ и $f(-a) = -f(a)$ для любого $a \in R$. Кроме того, если f — гомоморфизм колец с 1, то $f(x^{-1}) = (f(x))^{-1}$ для любого обратимого $x \in R$.*

Лемма 22 *Пусть $f : R \longrightarrow A$ — гомоморфизм колец, $r \in R$, а $a = f(r)$. Тогда $f^{-1}(a) = r + \operatorname{Ker} f$.*
Гомоморфизм инъективен тогда и только тогда, когда его ядро состоит из одного элемента.

Простое подполе и характеристика Для любого кольца с единицей R имеется канонический гомоморфизм

$$\varphi : \mathbb{Z} \longrightarrow R$$
$$\varphi(\pm n) = \pm(1 + \ldots + 1),\ n \in \mathbb{N}.$$

Определение 31 *Определим характеристику кольца* $\operatorname{char} R$ *следующим образом* $\operatorname{char} R = \begin{cases} 0, \text{ если } \varphi \text{ инъективен} \\ \text{наименьшее натуральное } p, \text{ для которого } \varphi(p) = 0, \text{ иначе.} \end{cases}$

Предложение 3 *Характеристика целостного кольца либо равна нулю либо является простым числом.*

Эндоморфизм Фробениуса Пусть F — поле и $\operatorname{char} F = p > 0$. Тогда $(a+b)^p = a^p + b^p$ Поэтому

$$\varphi : F \longrightarrow F$$
$$x \mapsto x^p.$$

является эндоморфизмом поля F. Он называется эндоморфизмом Фробениуса.

Определение 32 *Подкольцо*

Аддитивная подгруппа I кольца R называется левым (правым) идеалом, если для любых $r \in R$ и $s \in I$ имеет место включение $rs \in I$ (соотв., $sr \in I$). В других обозначениях: $RI \subseteqq I$ (соотв., $IR \subseteqq I$). Если I одновременно левый и правый идеал, то он называется двусторонним.

Лемма 23 *Пусть $f : R \longrightarrow A$ — гомоморфизм колец. Тогда* $\operatorname{Im} f$ *подкольцо в A, а* $\operatorname{Ker} f$ *— двусторонний идеал в R.*

Определение 33 *Пусть X — подмножество кольца R. Идеалом (левым, правым, двусторонним), порожденным множеством X, называется наименьший идеал в R, содержащая X.*

Замечание 9 $\sum_{x \in X} xR = \bigcap_{I \,-\, идеал R, X \subset I} I$.

4 Обозначения

Для множества X $|X|$ обозначает мощность множества X.

Список литературы

[1] Теория чисел