Содержание

1 Введение. 2

1.1 Функции, множества, отображения, основные алгебраические структуры. 2

1.2 Отношения. Классы эквивалентности. 2

2 Теория групп. 4

2.1 Полугруппы, группы. 4

2.1.1 Примеры: 5

2.2 Подгруппы. Простейшие конструкции. 6

2.2.1 Подгруппа, порожденная одним элементом; порядок элемента. 7

2.3 Гомоморфизмы, ядро и образ гомоморфизма. 7

2.4 Смежные классы, теорема Лагранжа. 8

2.5 Нормальные подгруппы, факторгруппы 9

2.6 Теорема о гомоморфизме. 10

2.7 Сопряжение элементов. Разбиение на классы сопряженности. . 10

2.8 Симметрическая группа степени n. 11

2.9 Циклические группы. Дискретный логарифм. 11

2.9.1 Дискретный логарифм. 13

2.10 Прямое произведение групп. Разложение конечной циклической группы в прямое произведение 13

2.11 Свободные группы; группы, заданные образующими и соотношениями 14

2.12 Действия групп. Разбиение на орбиты. Стабилизаторы, неподвижные точки. Лемма Бернсайда. 16

2.13 Характеры групп. 16

2.14 Представление абелевых групп в виде произведения циклических. 16

3 Коммутативные кольца. 17

3.0.1 Числовые кольца, свободные кольца, кольца эндоморфизмов. Характеристика. Эндоморфизм Фробениуса. . . 17

3.1 Факторкольцо, классы вычетов, сравнения 19

3.1.1 $K[x]/(f(x))$ 19

3.2 Теорема о гомоморфизме. 19

3.3 Идеалы. Китайская теорема об остатках. 20

3.3.1 Китайская теорема об остатках. Решение системы сравнений. 20

4 Теория чисел. 20

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 <u>отношением эквивалентности</u>, если для любых $x, y, z \in X$ выполнены следующие условия:*

1. *$x \sim x$(рефлексивность);*
2. *$x \sim y \iff y \sim x$ (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 моноидом. 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 — моноúд. 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 <u>подгруппой</u>, 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 $x_1\ldots x_k$, 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 <u>циклической</u>. Порядок подгруппы, порожденной элементом a называется <u>порядком элемента</u> 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 $a^0, a, \ldots, a^{n-1}$ различны и $a^m = a^{m \bmod n}$, поэтому $\langle a\rangle = \{a^0, a, \ldots, a^{n-1}\}$.

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 $G = \{x_1, \dots, x_n\}$. 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 $x \in H$. $\Box$

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

Доказательство:

1. Разделим m на n с остатком:
$$m = qn + r,\ 0 \leqslant r < n.$$
Тогда
$$g^m = (g^n)^q \cdot g^r = g^r$$
$$g^r = e \Longleftrightarrow r = 0$$
2. В силу предыдущего
$$g^k = g^l \Longleftrightarrow g^{k-l} = e \Longleftrightarrow n|(k-l) \Longleftrightarrow k \equiv l \mod n.$$

□

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

$$(g^k)^m = e \Longleftrightarrow n|km \Longleftrightarrow n_1|k_1m \Longleftrightarrow n_1|m.$$

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

$\square$

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

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 $H = \langle g^{n/d} \rangle$. □

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 $G/H = \langle gH \rangle$, $g^d \in H$. □

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*

$$\begin{gathered} F \times H \longrightarrow G \\ (f, h) \mapsto fh, \end{gathered}$$

  является изоморфизмом групп.

Доказательство: Нетрудно проверить, что

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

□

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 $C_{mn} \cong C_m \times C_n \Longleftrightarrow \gcd(m, n) = 1$.*

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 $[u][v] = [uv]$.

Теорема 8 *Так определенное умножение корректно, т.е. не зависит от выбора представителей в классах. Множество $F(X)$ является группой относительно этого умножения.*

Доказательство: Каждый класс слов $[u]$ содержит единственное несократимое слово $\overline{u}$.

> Нетрудно убедиться, что слово наименьшей длины в классе $[u]$ является 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 <u>свободной группой</u> 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

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

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 $g, h \in G$, $x \in X$

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

Пример: Группа S_n действует на множестве $\{1, \ldots, n\}$.

Рассмотрим следующее отношение на множестве X:
$x \sim y \iff \exists g \in G : gx = y$. Нетрудно проверить, что $\sim$ — отношение эквивалентности. Таким образом множество X разбивается на непересекающиеся классы эквивалентности, которые называются орбитами.

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

2.13 Характеры групп.

2.14 Представление абелевых групп в виде произведения циклических.

Абелевы группы

3 Коммутативные кольца.

Определение 27 *ассоциатвное кольцо, кольцо с 1, коммутативное кольцо, поле*

Лемма 15 *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 28 *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 5 *Гомоморфный образ кольца с 1 не обязательно содержит единицу (постройте пример).*

Лемма 16 *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 29 *Ядро и образ гомоморфизма. Мономорфизм, эпиморфизм, изоморфизм.*

Лемма 17 *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 18 *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 30 *Определим характеристику кольца* $\operatorname{char} R$ *следующим образом* $\operatorname{char} R = \begin{cases} 0, \textit{если } \varphi \textit{ инъективен} \\ \textit{наименьшее натуральное } p, \textit{ для которого } \varphi(p) = 0, \textit{иначе.} \end{cases}$

Предложение 2 *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 31 *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 19 *Пусть $f : R \longrightarrow A$ — гомоморфизм колец. Тогда* $\operatorname{Im} f$ *подкольцо в A, а* $\operatorname{Ker} f$ *— двусторонний идеал в R.*

Определение 32 *Пусть X — подмножество кольца R. Идеалом (левым, правым, двусторонним), порожденным множеством X, называется наименьший идеал в R, содержащая X.*

Замечание 6 $\sum_{x \in X} xR = \bigcap_{I\ -\ \textit{идеал} R, X \subset I} I.$

Лемма 20 *Подкольцо, порожденное X состоит из всевозможных сумм элементов вида $x_1 \ldots x_k$, где k — некоторое натуральное число, а $x_i \in X \cup 1$ (если имеется в виду подкольцо без 1, то $x_i \in X$).*

Левый (правый, двусторонний) идеал кольца R, порожденный X, состоит из всевозможных сумм элементов вида rx (соотв., xr, rxs), где $r, s \in R$, $x \in X$.

Определение 33 *Идеал $(a) = Ra$, порожденный одним элементом a называется главным идеалом.*

факторкольцо

3.1 Факторкольцо, классы вычетов, сравнения

Любой идеал (левый или правый) I кольца R, являясь подгруппой аддитивной группы кольца, определяет разбиение кольца R на смежные классы или классы вычетов по модулю идеала I.

Определение 34 *Будем говорить, что элементы a и b кольца R сравнимы по модулю I и писать $a \equiv b \mod I$, если они принадлежат одному классу вычетов, т.е. $a - b \in I$.*

Лемма 21 *Сравнимость обладает следующими свойствами:*

1. *если $a \equiv a' \mod I$ и $b \equiv b' \mod I$, то*

$$a + b \equiv a + b' \equiv a' + b' \mod I$$
$$ab \equiv ab' \equiv a'b' \mod I$$

Примеры:$\mathbb{Z}/n\mathbb{Z}$

3.1.1 $K[x]/(f(x))$

3.2 Теорема о гомоморфизме.

Так же как и в параграфе 2.6 могут быть доказаны следующие утверждения (нужно лишь проверить, что h сохраняет умножение).

Теорема 10 *Пусть R, R' и R'' — кольца, $f : R \longrightarrow R'$ — эпиморфизм, а $g : R \longrightarrow R''$ — гомоморфизм. Если $\operatorname{Ker} f = \operatorname{Ker} g$, то существует единственный мономорфизм $h : R' \longrightarrow R''$ такой, что $g = h \circ f$. Если g — эпиморфизм, то h — изоморфизм.*

Следствие 7 *(теорема о гомоморфизме колец)*
Пусть $f : R \longrightarrow R''$ — гомоморфизм колец. Тогда $\operatorname{Im} f \cong R/\operatorname{Ker} f$.

Кольца, подкольца,

прямое произведение колец. (этот параграф возможно лучше в другое место)

Определение 35 *Кольцо R называется прямой сумммой колец R_1 и R_2, если $R = R_1 \times R_2, (r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ и $(r_1, r_2)(s_1, s_2) = (r_1 s_1, r_2 s_2)$, где $r_1, s_1 \in G_1$, а $r_2, s_2 \in G_2$. В этом случае пишут $R = R_1 \bigoplus R_2$.*

3.3 Идеалы. Китайская теорема об остатках.

R — коммутативное кольцо, I, J — идеалы в R. Легко проверить, что $I + J = \{a + b | a \in I,\, b \in J\}$ является идеалом, причем это наименьший идеал, содержащий $I \cup J$.

Замечание 7 *Множество $\{ab | a \in I, b \in J\}$ не замкнуто относительно сложения, поэтому не является идеалом.*

Произведением идеалов IJ будем называть идеал, порожденный множеством $\{ab | a \in I, b \in J\}$, т.е.

$$IJ = \{\sum_{i=1}^{k} a_i b_i | a_i \in I,\, b_i \in J,\, k \in \mathbb{N}\}.$$

Определение 36 *Идеалы I и J кольца R называются взаимно простыми, если $I + J = R$.*

Лемма 22 *Если I и J взаимно простые идеалы, то $I \cap J = IJ$.*

Примеры:

Теорема 11 $R/IJ \cong R/I \bigoplus R/J$.

Лемма 23 *Если идеал J взаимно прост с каждым из идеалов $I_1, \ldots, I_n$, то он взаимно прост с их произведением.*

Следствие 8 *(Китайская теорема об остатках).*
$R/(I_1 \ldots I_n) \cong R/I_1 \bigoplus \ldots \bigoplus R/I_n$.

Замечание 8 *Если R некоммутативно, то IJ надо заменить на $IJ + JI$.*

3.3.1 Китайская теорема об остатках. Решение системы сравнений.

4 Теория чисел.

Список литературы

[1] Теория чисел