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* <u>*отношением эквивалентности*</u>, *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 *Факторомножеством $X/\sim$ 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;*
- *моноидом, 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 — моноид. 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 $a^0, a, \ldots, a^{n-1}$ 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 $G = \{x_1, \ldots, x_n\}$. 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. □

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.

□

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* $ord g = n$. *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* $ord g = n$, *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 $G = \langle g \rangle$ — 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*

$$\begin{aligned} \varphi : F \times H &\longrightarrow G \\ (f, h) &\mapsto fh, \end{aligned}$$

является изоморфизмом групп.

Доказательство: Нетрудно проверить, что

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

□

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

Замечание 5 *На случай не двух, а нескольких групп обобщение теоремы примет следующий вид:*

Теорема 7 *Пусть G — группа и $H_1, \ldots, H_n \leqslant G$. Обозначим через $T_i = H_1 \ldots H_{i-1} H_{i+1} \ldots H_n$. Тогда следующие свойства эквивалентны:*

- $G = H_1 \ldots H_n$, $H_i \cap T_i = \{1\}$, $\forall 1 \leqslant i \leqslant n$ *и* $\forall h_i \in H_i$, $h_j \in H_j (h_i h_j = h_j h_i), \forall i, j$;
- *отображение*

$$\varphi : H_1 \times \ldots \times H_n \longrightarrow G$$
$$(h_1, \ldots, h_n) \mapsto h_1 \ldots h_n,$$

является изоморфизмом групп.

Теорема 8 *Пусть $m, n \in \mathbb{N}$. Тогда $C_{mn} \cong C_m \times C_n \iff \gcd(m, n) = 1$.*

Доказательство: $\Longrightarrow$
Заметим, что $\forall g \in C_m \times C_n \operatorname{ord} g | \mathrm{HOK}(m, n) = \frac{mn}{(m,n)}$. 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. $\square$

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 9 *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 10 *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.

(см. [6])
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 6 *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 $gG_x \longleftrightarrow gx$ является биекцией между смежными классами по G_x и орбитой Gx.*
3. *$|G| = |Gx| \cdot |G_x|$;*
4. *$G_{ax} = aG_xa^{-1}$, $\forall a \in G$.*

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. $g \in G_{ax} \iff gax = ax \iff a^{-1}gax = x \iff g \in aG_xa^{-1}$.

□

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

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

□ Приложения леммы Бернсайда в комбинаторных задачах замечательно разобраны в [6].

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 $G_p \leqslant G$.

Лемма 17 $|G_p| = p^n$, $n \in \mathbb{N} \cup \{0\}$.

Доказательство: Пусть $\forall g \in G \exists m \in \mathbb{N} \cup \{0\} : \operatorname{ord} g = p^m$. Индукцией по порядку $|G|$ покажем, что $|G| = p^n$ для некоторого n. Если $G = \{e\}$, то утверждение очевидно. Пусть $H \leqslant G$. Ясно, что если порядки всех элементов группы G являются степенями простого числа p, то то же самое верно и для всех элементов групп H и G/H. Пусть $g \in G \setminus \{e\}$. Рассмотрим $H = \langle g \rangle$. Тогда $|H| = \operatorname{ord} g = p^m$ и $|G/H| < |G|$. По индукционному предположению $|G/H| = p^k$. Поэтому по теореме Лагранжа $|G| = |G/H||H| = p^{k+m}$.

□

Лемма 18 *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 $G_{p_i} \cap \oplus_{j \neq i} G_{p_j} = \{0\}$. Поэтому сумма всех G_p прямая. Более того, в силу теоремы 8 $\sum G_p$ 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 7 *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.

Представление абелевых групп в виде произведения циклических.

Теорема 11 *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 $|G| = p^n$. Будем доказывать утверждение индукцией по n. При $n = 1$ утверждение очевидно. 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. Действительно, пусть 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 $p^kG \longrightarrow p^{k+1}G$ умножения на p совпадает с $p^{l-1}G$ и содержит ровно p элементов, поэтому $|p^kG| = p|p^{k+1}G|$ 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 8 *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 адди-

тивной записи).

Последнее разложение единственно:

Лемма 19 *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: (или см. [3, гл.2 §3 теорема 9]) 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. Чуть позже теоремы о строении абелевых групп будут проиллюстрированы на примере разложения группы $(\mathbb{Z}/n\mathbb{Z})^*$.

На данном этапе не планируется изучение бесконечных абелевых групп, но ниже без доказательств будут сформулированы некоторые полезные утверждения.

Предложение 3 *Всякая конечно порожденная абелева группа без кручения изоморфна группе вида* $\mathbb{Z}^n = \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$.

Следующая теорема дает представление о структуре всех конечно порожденных абелевых групп.

Теорема 12 *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. Начальные сведения.

см. [5, §3.4],[2],[3].

3.1 Определения и основные понятия

Определение 28 • *Множество* R *с операциями сложения* $+$ *и умножения* $\cdot$ *называется кольцом, если относительно сложения* $(R, +)$ *является абелевой группой, а сложение с умножением связаны законом дистрибутивности*

$$x(y+z) = xy + xz,\ (x+y)z = xz + yz,\ \forall x, y, z \in R.$$

- *Кольцо называется*
  - *ассоциативным, если операция умножения ассоциативна.*
  - *коммутативным кольцом, если операция умножения коммутативна.*
  - *кольцом с единицей, если в нем существует нейтральный элемент по умножению.*
- *Ассоциативное кольцо с единицей* ($1 \neq 0$)*, в котором каждый ненулевой элемент имеет обратный (по умножению) называется телом.*
- *Коммутативное тело называется полем.*

В этой главе мы будем рассматривать исключительно ассоциативные кольца с 1. Таким образом в рамках данной главы под словом "кольцо"будем подразумевать коммутативное ассоциативное кольцо с единицей. Для кольца R, группа $(R, +)$ называется аддитивной группой кольца.

Примеры:

1. Поля:$\mathbb{Q}, \mathbb{R}$. $\mathbb{C}$ (будет описано позже).$\mathbb{Z}/p\mathbb{Z}$.
2. $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$. $n\mathbb{Z}$(без 1 при $n \neq 1$).
3. Пусть R — коммутативное ассоциативное кольцо с единицей. Рассмотрим $R[x] = \{a_0 + a_1x + \ldots + a_nx^n | a_i \in R, n \in \mathbb{N} \cup \{0\}\}$ — кольцо многочленов над R. (Также можно рассматривать кольцо многочленов от нескольких переменных (коммутирующих или некоммутирующих.))
4. Пусть R — ассоциативное кольцо с единицей. Помимо кольца многочленов, можно построить кольцо формальных степенных рядов $R[[x]]$ как множество формальных выражений вида $\sum_{i=0}^{\infty} a_i x^i$ с операциями сложения и умножения.
5. Кольцо функций. Пусть X — множество, K — кольцо. Тогда можно ввести структуру кольца на множестве функций $X \longrightarrow K$.
6. Множество линейных отображений $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$ со следующими операциями:
$$(f + g)(x) = f(x) + g(x);$$
$$f \cdot g := f \circ g$$
7. Кольцо с нулевым умножением: рассмотрим абелеву группу A с умножением $xy = 0$, $\forall x, y \in A$.

Лемма 20 *R — кольцо. $r \in R$. Тогда*

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

$r + 0 = r \Longrightarrow r(r + 0) = r^2 \Longrightarrow r^2 + r \cdot 0 = r^2 \Longrightarrow r \cdot 0 = 0$;
Если $0 = 1$, то $r = r \cdot 1 = r \cdot 0 = 0$, $\forall r \in R$. $\square$
Из определения ассоциативного кольца с единицей следует, что множество элементов кольца относительно умножения образует моноид. По лемме 3 множество обратимых (по умножению) элементов кольца R образует группу. Эта группа называется мультипликативной группой кольца и обозначается R^*. (Примеры:$\mathbb{R}^*, \mathbb{Z}^*, (\mathbb{Z}/n\mathbb{Z})^*$)

"Некоторые"элементы кольца.

Определение 29 *Элемент $r \in R \setminus \{0\}$ кольца R называется*

- *делителем нуля, если существует* $s \in R \setminus \{0\}$ *такой, что* $rs = 0$.
- *нильпотентным, если* $r^n = 0$ *при некотором* $n \in \mathbb{N}$.

Легко показать, что в поле нет делителей нуля, а в $\mathbb{Z}/n\mathbb{Z}$ делители нуля есть тогда и только тогда, когда n — составное.

Упр. 1 *При каких* n *в кольце* $\mathbb{Z}/n\mathbb{Z}$ *есть нильпотенты?*

Тогда и только тогда. когда n свободно от квадратов.

Определение 30 *Коммутативное ассоциативное кольцо с* $1 \neq 0$ *без делителей нуля называется областью целостности (целостным кольцом).*

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

Определение 31 *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* $a, b \in R$.

Определение 32 *Пусть* $f : A \longrightarrow B$ *— гомоморфизм колец.* $\operatorname{Ker} f = f^{-1}(0)$.

Замечание 9 *Таким образом всякий гомоморфизм колец является гомоморфизмом их абелевых групп, а следовательно:*

1. $f(0) = 0$
2. $f(-r) = -f(r)$.
3. *если* $f(a) = b$, *то* $f^{-1}(b) = a + \operatorname{Ker} f$.
4. *Гомоморфизм инъективен тогда и только тогда, когда его ядро состоит из одного элемента.*

Замечание 10 *Гомоморфный образ кольца с 1 не обязательно содержит единицу (постройте пример).*

Лемма 21 *Любой ненулевой гомоморфизм произвольного кольца с единицей в область целостности переводит единицу в единицу.*

Доказательство: $f(1) = f(1 \cdot 1) = f(1)f(1) \Longrightarrow f(1)(f(1) - 1) = 0$. Но $f(1) \neq 0$, т.к. иначе $f(x) = f(1 \cdot x) = f(1) \cdot f(x) = 0, \forall x \in R$. Поэтому $f(1) - 1 = 0$.
□

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

Определение 33 *Ядро и образ гомоморфизма. Мономорфизм, эпиморфизм, изоморфизм.*

Лемма 22 *Если f — гомоморфизм колец с 1, то $f(x^{-1}) = (f(x))^{-1}$ для любого обратимого $x \in R$.*

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 34 *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 4 *Характеристика целостного кольца либо равна нулю либо является простым числом.*

Определение 35 *Непустое подмножество R кольца A называется подкольцом, если $a + b, -a, ab \in R$ для любых $a, b \in R$.*

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

Замечание 11 $\sum_{x \in X} xR = \bigcap_{I\ -\ идеал R, X \subset I} I$.

Лемма 24 *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 $r, s \in R$, $x \in X$.

Начиная с этого момента будем предполагать, что все встречающиеся кольца коммутативны. В этом случае понятия левого/правого/двустороннего идеала эквивалентны.

Определение 37 *Идеал* $(a) = Ra$*, порожденный одним элементом* a *называется главным идеалом.*

Примеры:

1. $n\mathbb{Z}$ в $\mathbb{Z}$;
2. Рассмотреть какими могут быть идеалы в кольцах, перечисленных в п. 3.1.

3.3 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 38 *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 25 *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:$\mathbb{Z}/n\mathbb{Z}$

3.3.1 $K[x]/((f(x))$

Пусть K — поле. Построим факторкольцо $K[x]/((f(x))$.

Предложение 5 *(деление многочленов с остатком)*
Пусть $f, g \in K[x], g \neq 0$*. Тогда существуют единственные многочлены* q *и* r *из* $K[x]$ *такие, что* $f = gq + r$ *и* $\deg r < \deg g$.

Доказательство: Существование можно доказать индукцией по $\deg f$, а единственность очевидна. $\square$
Таким образом если $f = a_0 + a_1x + \ldots + a_nx^n$, то $K[x]/((f(x))$ можно интерпретировать как $\{b_0 + b_1t + \ldots + b_{n-1}t^{n-1} | t^n = -\frac{a_0}{a_n} - \frac{a_1}{a_n}t - \ldots - \frac{a_{n-1}}{a_n}t^{n-1}\}$.

Пусть R — облласть целостности. Тогда также, как и предыдущее предложение можно доказать следующее:

Предложение 6 *(деление многочленов с остатком)*
Пусть $f, g \in R[x], g \neq 0$*, причем старший коэффициент многочлена* g *равен 1. Тогда существуют единственные многочлены* q *и* r *из* $K[x]$ *такие, что* $f = gq + r$ *и* $\deg r < \deg g$.

3.3.2 Простые факты о $R[x]$

В этом параграфе R — область целостности.

Лемма 26 *Пусть* $f(x), g(x) \in [x]$, $\alpha \in K$. *Тогда*

1. *если* $f(\alpha) = 0$, *то* $f(x) = (x - \alpha)q(x)$, *где* $g \in [x], \deg q = \deg f - 1$;*(теорема Безу)*
2. *многочлен* f *имеет не более чем* $\deg f$ *различных корней;*
3. *если* $\deg f = \deg g = n$ *и* $f(\alpha_i) = g(\alpha_i)$ *для* $n + 1$ *различных элементов* $\alpha 1, \ldots, \alpha_{n+1}$, *то* $f = g$.

Доказательство:

1. По предложению 5
$$f(x) = (x - a)q(x) + c.$$
Подставляя $x = \alpha$, получаем, что $c = 0$.
2. По индукции по $\deg f = n$. Для $n = 1$ утверждение очевидно. Для $n > 1$: если многочлен f не имеет корней то все в порядке, а если имеет, то для корня α имеем $f(x) = (x - a)q(x)$ и применяем предполодение индукции к $q(x)$.
3. Применим предыдущее утверждение к многочлену $f - g$.

□

3.4 Теорема о гомоморфизме.

Так же как и в параграфе 2.6 может быть доказано следующее утверждения.

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

прямая сумма колец.

Определение 39 *Кольцо* R *называется прямой суммой 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* $R = R_1 \bigoplus R_2$.

3.5 Идеалы. Китайская теорема об остатках.

(см. [1])
R — коммутативное 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 $I \cup J$. Далее все рассматриваемые кольца будут считаться коммутативными.

Замечание 12 *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 40 *Идеалы I и J кольца R называются взаимно простыми, если $I + J = R$.*

Замечание 13 *Целые числа m и n взаимно просты тогда и только тогда, когда идеалы $m\mathbb{Z}$ и $n\mathbb{Z}$ взаимно просты в $\mathbb{Z}$, т.е. найдутся такие $x, y \in \mathbb{Z}$, что $xn + ym = 1$..*

Действительно, пусть $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ (это равенство следует из того, что все идеалы $\mathbb{Z}$ главные и имеют такой вид), то $d|m$ и $d|n$. А если $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$, то существуют $x, y \in \mathbb{Z} : xm + yn = 1$, откуда следует, что если $d|n, d|m$, то $d = 1$.

Лемма 27 *Если I и J взаимно простые идеалы, то $I \cap J = IJ$.*

Доказательство: По определению $IJ \subseteq I \cap J$. Пусть $x \in I \cap J$. Так как I и J взаимно просты, то существуют $a \in I$ и $b \in J$ такие, что $a + b = 1$. Тогда $x = xa + xb \in (I \cap J)I + (I \cap J)J \subseteq IJ$. $\square$
Примеры:

Теорема 13 *Пусть I и J взаимно простые идеалы коммутативного кольца R. Тогда $R/IJ \cong R/I \bigoplus R/J$.*

Доказательство: Естественный гомоморфизм $R \longrightarrow R/I \bigoplus R/J$ имеет ядро $I \cap J = IJ$. Осталось доказать, что он сюръективен. Пусть $a + b = 1$ для некоторых $a \in I, b \in J$. Тогда очевидно, что $xb + ya$ является прообразом элемента $(x + I, y + J)$. $\square$

Лемма 28 *Если идеал J взаимно прост с каждым из идеалов $I_1, \ldots, I_n$, то он взаимно прост с их произведением.*

Доказательство. $R = J+I_1 = J+I_1R = J+I_1(J+I_2) = (J+I_1J)+I_1I_2 \subseteq J+I_1I_2$. Далее по индукции.$\square$

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

Замечание 14 *Если R некоммутативно, то IJ надо заменить на $IJ+JI$.*

3.5.1 Китайская теорема об остатках. Решение системы сравнений.

Применим китайскую теорему об остатках для случая $R = \mathbb{Z}, I_i = m_i\mathbb{Z}$. Пусть $m_1, \dots m_k$ попарно взаимно просты и $n = m_1 \dots m_k$.

$$(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/m_1\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/m_k\mathbb{Z}).$$

Последнее утверждение можно переформулировать следующим образом.

Предложение 7 *Для любого набора остатков $r_1, \dots, r_k$ от деления на попарно взаимно простые числа $m_1, \dots m_k$ существует такое целое число x, что*

$$\begin{cases} x \equiv r_1 \mod m_1 \\ \dots \\ x \equiv r_k \mod m_k \end{cases}, \tag{1}$$

причем любые два решения $x_1, x_2 \in \mathbb{Z}$ этой системы сравнений будут сравнимы по модулю $n = m_1 \dots m_k$.

Построим явно решение системы (1). Заметим, во-первых, что по лемме 28 числа m_i и $l_i := \frac{n}{m_i} = m_1 \dots m_{i-1}m_{i+1} \dots m_k$ взаимно просты. Поэтому для каждого i $m_i\mathbb{Z} + l_i\mathbb{Z} = \mathbb{Z}$, т.е. найдутся такие $x_i, y_i \in \mathbb{Z}$, что $m_ix_i + l_iy_i = 1$. Последнее означает, что $l_iy_i \equiv 1 \mod m_i$. При этом $m_j \mid l_iy_i$, $\forall j \neq i$. Рассмотрим

$$x = r_1l_1y_1 + \dots + r_kl_ky_k.$$

Легко видеть, что x удовлетворяет системе сравнений (1).

3.6 Делимость в коммутативных кольцах.

Определение 41 *Элемент a кольца R делится на элемент b, если в кольце R существует элемент c, такой что $a = bc$.*

Лемма 29 *Пусть R — коммутативное кольцо с 1, тогда Для любых $a, b \in R$ выполнено:*

1. $(a|b) \Longleftrightarrow (b \in aR) \Longleftrightarrow (bR \subseteq aR)$.
2. $a \in R^* \Longleftrightarrow aR = R$.

3.7 Простые и максимальные идеалы

Определение 42 *Собственный идеал I называется простым, если $ab \in I$ влечет $a \in I$ или $b \in I$;*
Собственный идеал I называется максимальным, если он не содержится ни в каком другом собственном идеале.

Лемма 30 *Для любого собственного идеала J существует максимальный идеал, содержащий его.*

Доказательство: Рассмотрим множество всех идеалов I кольца R таких, что $I \supseteq J, I \neq R$. Отношение $\subset$ является отношение частичного порядка на этом множестве. Легко проверить, что если $\{I_i\}$ — линейно упорядоченное подмножество, то $\cup I_i$ — идеал R и является верхней гранью множества $\{I_i\}$. Применим к рассматриваемому множеству лемму Цорна и получим требуемое утверждение. $\square$

Замечание 15 *Комм. асс. кольцо с 1 является областью целостности тогда и только тогда, когда $\{0\}$ является простым идеалом.*

Упр. 2 *докажите следующие утверждения:*
Прообраз простого идеала при гомоморфизме — простой идеал. Прообраз максимального идеала при эпиморфизме — максимальный.

Следствие 9 *1. Идеал I простой тогда и только тогда, когда R/I — область целостности.*

2. Идеал I максимальный тогда и только тогда, когда R/I — поле.

3. Любой максимальный идеал является простым.

Доказательство:

1. Идеал I простой тогда и только тогда, когда $\{0\}$ простой в R/I.

2. Пусть R/I — поле. Тогда $\forall r \in R\, \exists x \in R : rx \equiv 1 \mod I$, т.е. $1 \in I + rx$, а значит $I + rR = (I, r) = R$, $\forall r$. Пусть $I \subset J \subseteq R$, тогда рассмотрим $r \in J \setminus I$. Тогда $R = I + rR \subseteq J$, а значит $R = J$.

   Обратно, пусть I — максимальный идеал. Тогда $\forall r \in R \setminus I$ выполнено $(r, I) = I + rR = R$, а значит $\exists x \in R$ такой, что $rx \equiv 1 \mod I$. Последнее означает, что в R/I всякий ненулевой элемент обратим.

3. Следует из того, что всякое поле является областью целостности.

$\square$

Замечание 16 *Утверждение можно было доказать как следствие упражнения 2.*

Обратное утв. к п.3. верным уже не будет. Рассмотрим, например, идеал (x) в кольце $\mathbb{Q}[x,y]$. Этот идеал простой, т.к. $\mathbb{Q}[x,y]/(x) \cong \mathbb{Q}[y]$, но не максимален.

Лемма 31 *В кольце главных идеалов любой ненулевой простой идеал является максимальным.*

Доказательство: (см. [1, глава 3]) Пусть $p \in R\backslash\{0\}$ таков, что pR — простой идеал. Пусть M — идеал и $pR \subset M \subset R$. Так как все идеалы главные, то $M = qR$ для некоторого $q \in R \setminus R^*$. Следовательно $p = qr$ для некоторого $r \in R$. Но, т.к. идеал pR простой и $p = qr \in pR$, то либо $q \in pR$ либо $r \in pR$. Если $r \in pR$, то $r = ps$ для некоторого $s \in R$. Но, тогда $p = qr = qps$, откуда, т.к. R область целостности, получаем $qs = 1$, что означает $M = qR = R$.

Если $q \in pR$, то $qR \subseteq pR$, откуда $qR = pR$. $\square$ Чуть позже будут рассмотрены примеры построения полей как колец классов вычетов. Один из важных таких примеров — поле комплексных чисел $\mathbb{C} = \mathbb{R}[x]/(x^2+1)$.

3.8 Факториальность колец главных идеалов.

(см. [глава 3 §3][1])

В этом параграфе будем рассматривать только области целостности.

Определение 43 *Элементы $a, b \in R$ называются ассоциированными, если $aR = bR$.*
Элемент $a \in R \setminus R^*$ называется неприводимым, если из равенства $a = bc$ следует, что b или c ассоциирован с a. простой элемент

Лемма 32 *Пусть R область целостности.*

1. *Элементы $a, b \in R$ ассоциированы тогда и только тогда, когда $a = b\varepsilon$ для некоторого $\varepsilon \in R^*$.*
2. *Элемент $a \in R$ неприводим, если он не раскладывается в произведение необратимых элементов.*

Доказательство:

$\square$

Определение 44 *Область целостности называется факториальным кольцом, если любой ненулевой необратимый элемент раскладывается в произведение неприводимых единственным образом. Единственность понимается в следующем смысле: если $\prod_{i=1}^{m} p_i$ ассоциировано с $\prod_{j=1}^{n} q_j$ для*

некоторых неприводимых элементов $p_i, q_j \in R$, *то* $m = n$ *и существует перестановка* $\sigma \in S_n$ *такая, что* p_i *ассоциирован с* $q_{\sigma(i)}$ *для всех* $i = 1, \ldots, n$.

Теорема 14 *Область главных идеалов является факториальным кольцом.*

Для доказательства потребуются следующие леммы.

Лемма 33 *Пусть* R *— область главных идеалов,* $a, c \in R$, *причем* c *— неприводимый,* a *не делится на* c. *Тогда* $aR + cR = R$.

Доказательство: Т.к. любой идеал главный, то $aR + cR = bR$ для некоторого $b \in R$. Так как $c \in bR$ и c неприводим, то либо $cR = bR$, либо $bR = R$. Но если $cR = bR$, то $a \in cR$, что противоречи условию. Значит $bR = R$. $\square$

Лемма 34 *Пусть* R *— область главных идеалов,* $a, b, c \in R$, *причем* c *— неприводимый. Тогда если* ab *делится на* c, *то* a *или* b *делится на* c. *Другими словами:* c *— неприводим* $\Longleftrightarrow$ *идеал* cR *— простой.*

Доказательство: Если ни a ни b не делятся на c, то по предыдущей лемме $aR + cR = bR + cR = R$, т.е. идеал cR взаимно прост с каждым из идеалов aR, bR. Но тогда cR взаимно прост с их произведением abR, т.е. $cR+abR = R$, откуда $ab \notin cR$. $\square$

Лемма 35 *Пусть* R *— область главных идеалов,* $I_1 \subseteq I_2 \subseteq \ldots$ *— возрастающая цепочка идеалов. Тогда* $I_n = I_{n+1} = \ldots$ *для некоторого* n*(иными словами кольцо главных идеалов является нетеровым).*

Доказательство: Так как все идеалы главные, $I_k = r_k R$ для некоторых $r_k \in R$. Нетрудно проверить, что $I = \cup I_k$ — идеал, поэтому $I = qR$, $q \in R$. По определению $q \in R_j R$ для некоторого j. Тогда $I = qR = r_j R$, откуда $r_l R = r_j R$ при $l \geqslant j$.$\square$

Лемма 36 *Если* R *— область главных идеалов, то каждый необратимый элемент раскладывается в произведение неприводимых.*

Доказательство: Пусть $r \in R \setminus R^*$. Идеал rR содержится в каком-то максимальном идеале $p_1 R$,(который, как и все идеалы является главным). Т.е. $r = p_1 r_1$, $r_1 \in R$. Так как $p_1 R$ максимальный, то он является простым, а значит p_1 — неприводим. Если r_1 обратим, то все доказано. Иначе $r_1 = p_2 r_2$, $p_2, r_2 \in R$, где p_2 неприводим. Продолжим процесс. Получим строго возрастающую цепочку идеалов $rR \subset r_1 R \subset r_2 R \subset \ldots$. По предыдущей лемме процесс конечен, т.е. на каком-то шаге получим обратимый элемент $r_k \in R^*$. $\square$

Лемма 37 *Пусть R — область целостности, в которой каждый неприводимый элемент порождает простой идеал. Если каждый необратимый элемент раскладывается в произведение неприводимых, то кольцо R факториально.*

Доказательство: Достаточно доказать единственность разложения на неприводимые элементы. Пусть

$$\varepsilon p_1 \dots p_n = \theta q_1 \dots q_m, \tag{2}$$

где все элементы p_k и q_k неприводимы, а ε, θ обратимы. Индукцией по $\min(m, n)$ докажем, что $m = n$ p_k ассоциирован с $q_{\sigma(k)}$ для некоторой перестановки $\sigma \in S_n$.

База индукции: если $m = 0$, то правая часть обратима, поэтому $n = 0$.

Индукционный переход. По условию идеал $p_n R$ простой, поэтому $q_l \in p_n R$ для некоторого $1 \leqslant l \leqslant m$. Т.к. q_l неприводим, то $q_l = \delta p_n$, где $\delta \in R^*$. Подставим это в равенство (2) и сокращая на p_n получим

$$\varepsilon p_1 \dots p_{n-1} = \theta\delta q_1 \dots q_{l-1} q_{l+1} \dots q_m.$$

По индукционному предположению $n - 1 = m - 1$ и существует биекция $\tau : \{1, \dots, n-1\} \longrightarrow \{1, \dots, m\} \setminus \{l\}$ такая, что p_k ассоциирован с $q_{\tau(k)}$ для всех $k \in \{1, \dots, n-1\}$. Положим $\sigma(k) = \begin{cases} \tau(k), & 1 \leqslant k \leqslant n-1 \\ l, & k = n. \end{cases}$. $\square$

Эта лемма завершает доказательство теоремы 14.

3.9 Евклидовы кольца

Определение 45 *Область целостности R называется евклидовым кольцом, если существует функция (евклидова норма)*

$$\nu : K \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\},$$

такая, что для всех $a, b \in R \setminus \{0\}$ выполняются свойства

$$\nu(ab) \geqslant \nu(a)$$
$$\exists q, r \in R : a = bq + r \text{ и либо } \nu(r) < \nu(b), \text{ либо } r = 0.$$

Элементы q и r называются, соответственно, неполным частным и остатком от деления a на b.

Примеры:

1. Кольцо $\mathbb{Z}$ с $|\cdot|$;

2. Кольцо многочленов с коэффициентами из поля $K[x]$ с нормой deg;

3. $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ с нормой $v(z+bi) = z^2+b^2$.

4. $\mathbb{Z}[\omega] = \mathbb{Z}[x]/(x^2+x+1)$ с нормой $v(a+bi) = a^2+b^2-ab$.

Теорема 15 *Евклидово кольцо является кольцом главных идеалов.*

Доказательство: (см. [1, глава 3]) Пусть I идеал в R и $I \neq \{0\}, I \neq R$. Возьмем элемент $b \in I$ с наименьшей возможной евклидовой нормой. Покажем, что $I = bR$. Пусть $a \in I$. Тогда существуют $q, r \in R$ такие, что $a = bq + r$ и если $r \neq 0$, то $\nu(r) < \nu(b)$. Элемент $r = a - bq$ принадлежит I, следовательно его норма не может быть меньше чем $\nu(b)$, а значит $r = 0$ и $a = bq$. Таким образом $I \subseteq bR$, обрвтное следует из того, что $b \in I$. □

□

Итого

евклидовы кольца ⊂ КГИ ⊂ факториальные ⊂ области целостности

3.9.1 НОД,НОК

Определение 46 *Пусть $a, b \in R$. Элемент $d \in R$ называется наибольшим общим делителем элементов a и b, если он делит и a и b, и делится на любой другой общий делитель a и b.*

Другими словами $d \in R$ наибольший общий делитель, если dR — наименьший главный идеал, содержащий a и b.

Замечание 17 *НОД определен с точностью до ассоциированности*

Теорема 16 *(о линейном представлении НОД)*
Пусть R — кольцо главных идеалов. Для любых $a, b \in R$ существуют $x, y \in R$ такие, что $ax + by = \gcd(a, b)$.

Доказательство. Идеал $aR + bR$ является минимальным идеалом, содержащим a и b ($aR + bR = (a, b)$), а по условию он является главным. Таким образом $aR + bR = dR$, и по определению НОД $d = \gcd(a, b)$. □

Определение 47 *Элементы a и b называются взаимно простыми, если у них нет необратимых общих делителей.*

Следствие 10 *Пусть R — кольцо главных идеалов. Идеалы aR и bR являются взаимно простыми тогда и только тогда, когда элементы a и b взаимно просты.*

Определение 48 *Пусть $a, b \in R$. Элемент $c \in R$ называется наименьшим общим кратным элементов a и b, если он делится на a и на b, и делит любое другое общее кратное a и b.*

Другими словами c наименьшее общее кратное , если R — наибольший главный идеал, содержащийся в $aR \cap bR$.

Лемма 38 *Пусть R — кольцо главных идеалов. $a, b \in R \setminus \{0\}$. Тогда* $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a,b)}$.

Доказательство.

$$d = \gcd(a, b),\ a = a'd,\ b = b'd.$$

По теореме о линейном представлении НОД существуют $x, y \in R$ такие, что $ax + by = d$. Так как R — область целостности, а $d \neq 0$, то можно сократить на d и получить равенство

$$a'x + b'y = 1.$$

Если $c \in aR \cap bR$, то $c = ca'x + cb'y \in ba'R + ab'R = a'b'dR$. Таким образом, $aR \cap bR \subseteq a'b'dR$, а обратное включение очевидно. Осталось заметить, что $a'b'd = \frac{ab}{\gcd(a,b)}$. □

3.9.2 Алгоритм Евклида

Пусть R — евклидово кольцо.

Лемма 39 *Для любых $a, b, c \in R$ имеет место равенство* $\gcd(a, b) = \gcd(a - bc, b)$.

Доказательство. Ясно, что $a - bc, b \in aR + bR$, поэтому $(a - bc)R + bR \subseteq aR + bR$. С другой стороны

$$a = (a - bc) + bc \in (a - bc)R + bR,$$

откуда следует обратное включение. Так как $(a - bc)R + bR = aR + bR$, то и наименьший главный идеал, содержащий эти идеалы, одинаковый. □

Алгоритм Евклида. Обозначим $r_0 = a$ и $r_1 = b$ и положим $i = 1$. Алгоритм Евклида:

1. Разделить r_{i-1} на r_i с остатком: $r_{i-1} = r_i q_i + r_{i+1}$.
2. Если $r_{i+1} \neq 0$, то увеличить i и вернуться к первому шагу.
3. Если $r_{k+1} = 0$, то $\gcd(a, b) = r_k$.

Действительно, т.к. $r_{i+1} = r_{i-1} - r_i q_i$, то по лемме $(r_{i-1}, r_i) = (r_{i+1}, r_i)$, а $(r_k, 0) = r_k$.

Для нахождения линейного представления НОДа используется обратный ход алгоритма Евклида.

3.10 Сравнения первой степени.

Пусть R — кольцо главных идеалов. Для наглядности сфомулируем утверждения в кольце $\mathbb{Z}$.

Лемма 40 *Пусть* $d = \gcd(a, m)$. *Тогда*

$$|\{x \in \mathbb{Z}/m\mathbb{Z} | ax = b \mod m\}| = \begin{cases} 0, & d \nmid b \\ d, & d \mid b \end{cases}$$

и если $d \mid b$, *то*

$$\{x \in \mathbb{Z}/m\mathbb{Z} | ax = b \mod m\} = \{x_0, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d}\}.$$

(см. [8, предложение 3.3.1])

3.10.1 Линейные диофантовы уравнения.

Лемма 41 *Пусть* $d = \gcd(a, b)$. *Тогда если* $d \nmid c$, *то уравнение*

$$ax + by = c \tag{3}$$

неразрешимо в целых числах, а если $d \mid d$, *то все решения уравнения (3) имеют вид* $\begin{cases} x = x_0 + n \cdot \frac{b}{d} \\ y = y_0 - n \cdot \frac{a}{d} \end{cases}$, *где* (x_0, y_0) — *частное решение уравнения (3).*

4 Теория чисел.

Вопросы, ответы на которые, будут получены в ближайшие лекции:

1. При каких n существуют первообразные корни по модулю n, т.е. когда группа $(\mathbb{Z}/n\mathbb{Z})^*$ циклическая?
2. Описание группы $(\mathbb{Z}/n\mathbb{Z})^*$
3. Некоторые обобщения малой теоремы Ферма (см. ниже).

4.1 Обратимые классы вычетов. Функция Эйлера. Явная формула для функции Эйлера. Теорема Эйлера, малая теорема Ферма, теорема Вильсона.

Функция Эйлера

Определение 49 *Порядок мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^*$ обозначается $\varphi(n)$. Функция $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ называется функцией Эйлера.*

Лемма 42 *Образ числа $m \in \mathbb{Z}$ обатим в $\mathbb{Z}/n\mathbb{Z}$, если и только если $\gcd(m, n) = 1$. Таким образом, $\varphi(n)$ равна количеству чисел от 0 до $n-1$, взаимно простых с n.*

Эта лемма следует из леммы 40.

Лемма 43 *Если кольцо R с единицей (не обязательно коммутативное) является прямой суммой колец $R_1 \bigoplus \ldots \bigoplus R_k$, то $R^* \cong R_1^* \times \ldots R_k^*$. Если R^* конечна, то $|R^*| = |R_1^*| \ldots |R_k^*|$.*

Теорема 17 *1. Если $\gcd(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.*

2. *Если p — простое, $k \in \mathbb{N}$, то $\varphi(p^k) = p^{k-1}(p-1)$.*
3. *Пусть $p_1, \ldots, p_l$ — различные простые числа, $k_1, \ldots, k_l \in \mathbb{N}$, $n = \prod_{i=1}^{l} p_i^{k_i}$. Тогда*

$$\varphi(n) = \prod_{i=1}^{l}(p_i^{k_i} - p_i^{k_i-1}) = n\prod_{i=1}^{l}\frac{p_i - 1}{p_i}.$$

Доказательство:

1. Следует из китайской теоремы об остатках и леммы 43.
2. Легко видеть, что числе которые меньще чем p^k и не взаимно просты с p^k ровно $\frac{p^k}{p} = p^{k-1}$.
3. Следует из предыдущих пунктов.

□

Теорема 18 *(теорема Эйлера). Если a взаимно просто с n, то $a^{\varphi(n)} \equiv 1 \mod n$.*

Следствие 11 *(малая теорема Ферма) Если p — простое число, a — целое число, не делящееся на p, то $a^{p-1} \equiv 1 \mod p$.*

Следствие 12 *(теорема Вильсона) Если p — простое число, то $(p-1)! \equiv -1 \mod p$.*

Доказательство: Заметим, сначала, над полем $\mathbb{Z}/p\mathbb{Z}$

$$x^{p-1} - 1 = (x-1)(x-2)\dots(x-(p-1)). \tag{4}$$

Действительно, разность этих многочленов — многочлен, степени строго меньшей, чем $p-1$, но при этом $1, \dots, p-1$ являются его корнями. Остается воспользоваться леммой 26. Для завершения доказательства остается подставить $x = 0$ в обе части равенства (4).

□

4.2 Строение группы $(\mathbb{Z}/n\mathbb{Z})^*$.

4.2.1 Экспонента группы

Определение 50 *Экспонента группы G — наименьшее натуральное число d такое, что $g^d = e$ для любого $g \in G$. Если такого d не существует, то говорят, что экспонента группы равна бесконечности.*

Нетрудно убедиться, что

1. если группа конечна, то ее экспонента делит ее порядок.

Лемма 44 *Пусть G — группа. $a, b \in G$, причем $\operatorname{ord} a, \operatorname{ord} b < \infty$, $\operatorname{ord} a$ и $\operatorname{ord} b$ взаимно просты, и $ab = ba$. Тогда $\operatorname{ord}(ab) = \operatorname{ord} a \operatorname{ord} b$.*

Доказательство: Пусть $m = \operatorname{ord} a$, $n = \operatorname{ord} b$. Так как элементы a и b коммутируют, то $(ab)^{mn} = a^{mn}b^{mn} = e$, поэтому $\operatorname{ord}(ab) | mn$. Далее, если $(ab)^k = e$, то

$$a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle.$$

Но порядки $\langle a \rangle$ и $\langle b \rangle$ взаимно просты, поэтому по теореме Лагранжа $\langle a \rangle \cap \langle b \rangle = \{e\}$. Отсюда $a^k = b^{-k} = e$ и, следовательно $n|k, n|k$, а значит и $mn|k$. □

Следствие 13 *Пусть G — абелева группа конечного порядка. Тогда*

1. *Экспонента группы G равна $m = \operatorname{lcm}\{\operatorname{ord} g | g \in G\}$.*
2. *Существует элемент $g \in G$ такой, что $\operatorname{ord} g = m$.*
3. *Конечная абелева группа является циклической тогда и только тогда, когда ее экспонента равна ее порядку.*

Доказательство:(см. [1])

1. Пусть d — экспонента группы G. Тогда для любого $g \in G$ $\operatorname{ord} g | d$, поэтому $m|d$. С другой стороны $\forall g \in G\ a^m = e$, поэтому $d \leqslant m$.

2. Пусть $d = p_1^{k_1} \dots p_l^{k_l}$, где $p_1, \dots, p_l$ — различные простые числа. Тогда существуют элементы $g_1, \dots, g_l \in G$ порядки которых делятся на $p_1^{k_1}, \dots, p_l^{k_l}$ соответственно. Возводя элементы $g_1, \dots, g_l$ в подходящие степени, можно считать, что $\operatorname{ord} g_i = p_i^{k_i}$ для всех $i = 1..l$. (Если $\operatorname{ord} g = mn$, то в силу леммы 12 $\operatorname{ord} g^m = n$). Теперь, воспользовавшись предшествующей леммой по индукции нетрудно получить, что $\operatorname{ord} g_1 \dots g_l = d$.

3. Следует из предыдущих двух.

□

Теорема 19 *Пусть R — область целостности, $G \leqslant R^*$ и $|G| < \infty$. Тогда группа G циклическая.*

Доказательство: Пусть $|G| = m$. В силу последнего следствия, достаточно показать, что экспонента группы G равна m. Пусть d — экспонента группы G. Тогда все элементы G являются корнями многочлена $x^d - 1$. Но по п.2 леммы 26 этот многочлен не может иметь более чем d корней, поэтому $m \leqslant d$.

□

Следствие 14 *Конечная подгруппа мультипликативной группы поля — циклическая.*

Следствие 15 $(\mathbb{Z}/p\mathbb{Z})^*$ *— циклическая группа порядка* $p - 1$, *т.е.* $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$.

Цикличность группы $(\mathbb{Z}/p^k\mathbb{Z})^*$. Пусть p — нечетное простое число.

Лемма 45 *Пусть $n, m \in \mathbb{N}$ и $2 \nmid n$. Тогда*

$$(n+1)^{n^{m-1}} - 1 \equiv n^m \mod n^{m+1}.$$

Доказательство: По индукции по m. Для $m = 1$ утверждение очевидно. Переход:

$$(n+1)^{n^m} - 1 = ((n+1)^{n^{m-1}})^n - 1 = ((n+1)^{n^{m-1}} - 1) \sum_{i=0}^{n-1} (((n+1)^{n^{m-1}})^i)$$

Осталось заметить, что по индукционному предположению $(n+1)^{n^{m-1}} - 1 \equiv n^m \mod n^{m+1}$, и т.к. $m > 1$, то $(n+1)^{in^{m-1}} \equiv 1 \mod n^2$, поэтому $\sum_{i=0}^{n-1} (((n+1)^{n^{m-1}})^i) \equiv \sum_{i=0}^{n-1} 1 = n \mod n^2$. В результате получаем

$$((n+1)^{n^{m-1}} - 1) \sum_{i=0}^{n-1} (((n+1)^{n^{m-1}})^i) \equiv n^{m+1} \mod n^{m+2}.$$

□

Пусть d — первообразный корень по модулю p (т.е. $\langle d \rangle = (\mathbb{Z}/p\mathbb{Z})^*$).

Лемма 46 *В группе* $(\mathbb{Z}/p^k\mathbb{Z})^*$

1. $\operatorname{ord}(p+1) = p^{k-1}$;
2. $\operatorname{ord} d^{p^{k-1}} = p-1$;
3. $(p+1)d^{p^{k-1}}$ — *первообразный корень по модулю* p^k, *тем самым группа* $(\mathbb{Z}/p^k\mathbb{Z})^*$ *циклическая.*

Доказательство:

1. Подставим $n = p, m = k$ в сравнение из предыдущей леммы и получим, что $\operatorname{ord}(p+1) \mid p^{k-1}$, откуда $\operatorname{ord}(p+1) = p^l$, где $l \leqslant k-1$. Но в силу того же сравнения $(p+1)^{p^{k-2}} \equiv 1 + p^{k-1} \mod p^k$, поэтому $l = k$.
2. Т.к. $|(\mathbb{Z}/p^k\mathbb{Z})^*| = p^{k-1}(p-1)$, то $\operatorname{ord} d^{p^{k-1}} \mid p-1$. С другой стороны сравнение $d^{p^{k-1}l} \equiv 1 \mod p^k$ влечет сравнение $d^{p^{k-1}l} \equiv 1 \mod p$, что в силу того, что d первообразный корень по модулю p означает, что $(p-1) \mid p^{k-1}l$, т.е. $(p-1) \mid l$.
3. Следует из предыдущих двух пунктов и леммы 44.□

Строение группы $(\mathbb{Z}/n\mathbb{Z})^*$. Пусть $n \in \mathbb{N}$ и $n = p_1^{k_1} \cdots p_l^{k_l}$, где $l \in \mathbb{N}_0$, $p_1, \ldots, p_l$ — попарно различные простые числа, $k_1, \ldots, k_l \in \mathbb{N}$. Из китайской теоремы об остатках и леммы 43 нам уже известно, что

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^* \times \ldots \times (\mathbb{Z}/p_l^{k_l}\mathbb{Z})^*.$$

Для всех простых p кроме 2 нам известно, что $(\mathbb{Z}/p^k\mathbb{Z})^* \cong C_{p^{k-1}(p-1)}$. В случае $p = 2$ имеется следующее утверждение:

Лемма 47 *1. Пусть* $m \in \mathbb{N} \setminus \{1\}$, *тогда* $5^{2^{m-2}} - 1 \equiv 2^m \mod 2^{m+1}$;

2. *Пусть* $k \in \mathbb{N} \setminus \{1\}$.
   (a) *В группе* $(\mathbb{Z}/2^k\mathbb{Z})^*$: $\operatorname{ord}(-1) = 2, \operatorname{ord}(5) = 2^{k-2}, \langle -1\rangle \cap \langle 5\rangle = \{1\}$;
   (b) $(\mathbb{Z}/2^k\mathbb{Z})^* \cong C_2 \times C_{2^{k-2}}$;

Теперь нам известно все о строении группы $(\mathbb{Z}/n\mathbb{Z})^*$. Результат можно сформулировать следующим образом.

Теорема 20 *Пусть* $n \in \mathbb{N}$ *и* $n = p_1^{k_1} \cdots p_l^{k_l}$, *где* $l \in \mathbb{N}_0$, $p_1, \ldots, p_l$ — *попарно различные простые числа,* $k_1, \ldots, k_l \in \mathbb{N}$, *причем если* $2|n$, *то* $p_1 = 2$. *Тогда группа* $(\mathbb{Z}/n\mathbb{Z})^*$ *изоморфна группе*

$$\begin{cases} C_{p_1^{l_1-1}(p_1-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)}, & \text{если } 2 \nmid n \text{ или } (4|n, \text{но } 8 \nmid n), \\ C_{p_2^{l_2-1}(p_2-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)}, & \text{если } 2 \mid n \text{ и } 4 \nmid n, \\ C_2 \times C_{2^{l_1-2}} \times C_{p_2^{l_2-1}(p_2-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)}, & \text{если } 8|n \end{cases}.$$

Критерий существования дискретного логарифма.

Предложение 8 *Группа $(\mathbb{Z}/n\mathbb{Z})^*$ циклическая тогда и только тогда, когда n имеет вид $2, 4, p^a$ или $2p^a$, где p — нечетное простое число.*

Обобщение малой теоремы Ферма. Определим функцию Кармайкла $\lambda : \mathbb{N} \longrightarrow \mathbb{N}$ как значение экспонены группы $(\mathbb{Z}/n\mathbb{Z})^*$. Из предыдущей теоремы легко следует следующая.

Теорема 21 *1. Если n не делится на 8, то $\lambda(n) = \mathrm{lcm}_{1\leqslant i\leqslant l}(p_i^{k_i-1}(p_i-1))$. Если $n = 2^k m$, где m нечетно, а $k \geqslant 3$, то $\lambda(n) = \mathrm{lcm}(\mathrm{lcm}_{1\leqslant i\leqslant l}(p_i^{k_i-1}(p_i-1)), 2^{k-2})$.*

2. Если a взаимно просто с n, то $a^{\lambda(n)} \equiv 1 \mod n$.

4.3 Тесты на простоту.

(см. [1, стр 26]) Для нечетного $n > 1$ определяется множество $T \subseteq \mathbb{Z}/n\mathbb{Z}\backslash\{0\}$, которое совпадает со всем множеством в случае простого n. Те числа n, для которых $|T| = \varphi(n)$ называются псевдопростыми для данного теста.

4.3.1 Тест Ферма

$T := \{a|a^{n-1} = 1\}$. Псевдопростые числа для теста Ферма существуют и называются числами Карлмайкла. Чисел Карлмайкла бесконечно много. Наименьшее из них — 561.

4.3.2 Тест Эйлера

$$T = \{a|a^{\frac{n-1}{2}} = 1\}$$

Псевдопростые есть: 1729, 2465

Следующие два теста будут рассмотрены несколько позже, т.к. для описания одного из них требуется понятие символя Якоби, который будет введен чуть позднее.

4.3.3 Тест Соловея-Штрассена

$$T := \{a \in (\mathbb{Z}/n\mathbb{Z})^*|a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}.$$

Пусть для k случайных значений a мы проверим выполнение условия $a \in T$. Следующее утверждение позволяет оценить с какой вероятностью число n

следует считать простым. Известное мне доказательство использует свойства квадратичных вычетов, которые мы пройдем несколько позже, поэтому пока приведу только формулировку.

Предложение 9 *Пусть n — нечетное составное число. Тогда $|T| < \frac{\varphi(n)}{2}$*

Таким образом если для k случайных значений $a \in (\mathbb{Z}/n\mathbb{Z})^*$ выполнено $a \in T$, то можно считать, что n простое с вероятностью, не меньшей чем $1 - \frac{1}{2^k}$.

4.3.4 Тест Миллера-Рабина

Пусть $n - 1 = 2^m k$, $2 \nmid k$.

$$T = \{a | a^k = 1 \text{ или } \exists j < m : a^{2^j k} = -1\}$$

Легко видеть, что если n простое, то $T = (\mathbb{Z}/n\mathbb{Z})^*$. (это следует из того, что в поле $\mathbb{Z}/n\mathbb{Z}$ уравнение $x^2 = 1$ имеет ровно 2 решения.)
К сведению.

Предложение 10 *Пусть n — нечетное составное число $3 \nmid n$ и $n - 1 = 2^m k$, $2 \nmid k$. Тогда $|T| \leqslant \frac{\varphi(n)}{4}$.*

Таким образом если для k случайных значений $a \in (\mathbb{Z}/n\mathbb{Z})^*$ выполнено $a \in T$, то можно считать, что n простое с вероятностью, не меньшей чем $1 - \frac{1}{4^k}$.

Если при фиксированном n число a проходит тест Миллера–Рабина и не показывает, что n составное, то оно проходит и тест Соловея-Штрассена с тем же результатом.

4.4 Криптография: начало.

Криптосистема

$$\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}.$$

- $\mathcal{P}$ — мн-во всевозможных элементов открытого текста;
- $\mathcal{C}$ — мн-во всевозможных элементов шифротекста;

Примеры: элементы сообщений — буквы N-буквенного алфавита $0, 1, \ldots, N - 1$. Аффинные преобразования.

[105] Классическая криптосистема — криптосистема, в которой имея информацию о преобразовании шифрования, можно реализовать преобразование дешифрования примерно за такое же время, что и преобразование шифрования.

4.4.1 Открытый ключ.

4.4.2 Алгоритм RSA.

(Rivest, Sgamir, Adleman)

Каждый пользователь выбирает два очень больших числа p и q и вычисляет $n = pq$. Нетрудно вычислить $\varphi(n) = (p-1)(q-1) = n+1-p-q$. Затем пользователь выбирает случайное число $e : 1 \leqslant e \leqslant \varphi(n)$, которое взаимно просто с $\varphi(n)$. Итого каждый пользователь A выбрал два простых числа p_A и q_A, а вслед за этим — случайное число e_A такое, что $(e_A, (p_A-1)(q_A-1)) = 1$. Далее A вычисляет $n_A = p_A q_A$, $\varphi(n_A) = n_A + 1 - p_A - q_A$ и $d_A \equiv e_A^{-1} \mod \varphi(n_A)$.

4.5 Сравнения высших степеней.

Пусть $f(x) \in \mathbb{Z}[x]$. В силу китайской теоремы об остатках сравнение $f(x) \equiv 0 \mod n$ может быть сведено к набору сравнений вида $f(x) \equiv 0 \mod p_i^{k_i}$, где p_i — различные простые числа. Напомню, что сравнения первой степени были полностью изучены в 3.10.

4.5.1 Лемма Хенселя.

Лемма 48 *$f(x) \in \mathbb{Z}[x]$. $m, k \in \mathbb{N}$, $m \leqslant k$. Если $f(a) \equiv 0 \mod p^k$ и $f'(a) \neq 0 \mod p$, то $\exists s \in \mathbb{Z}$ такое, что* $\begin{cases} f(s) \equiv 0 \mod p^{k+m} \\ r \equiv s \mod p^k. \end{cases}$ *Причем такой s единственный по $\mod p^{k+m}$.*

Доказательство.

$$f(x) = g(x-a) = \sum_{l=0}^{n} \frac{f^{(l)}(a)}{l!}(x-a)^l$$

$$s = a + tp^k$$

$$f(a+tp^k) = \sum_{l=0}^{n} \frac{f^{(l)}(a)}{l!}(tp^k)^l \equiv [m \leqslant k] \equiv f(a) + f'(a)tp^k \equiv [f(a) = zp^k] \equiv$$

$$\equiv (z + f'(a)t)p^k.$$

$$f(a+tp^k) \equiv 0 \mod p^{k+m} \iff z + f'(a)t \equiv 0 \mod p^m$$

Последнее сравнение в силу того, что $f'(a) \neq 0 \mod p$ имеет единственное решение. □

4.6 Квадратичные сравнения. Символ Лежандра, символ Якоби. Квадратичный закон взаимности.

4.6.1 о квадратичных сравнениях.

сведение к виду $x^2 \equiv a \mod b$

$$ax^2 + bx + c \equiv 0 \mod p$$

$$x^2 + a^{-1}bx + a^{-1}c \equiv 0 \mod p \; p \neq 2$$

$$(x + \frac{a^{-1}b}{2})^2 \equiv -a^{-1}c + \frac{a^{-2}b^2}{4} \mod p$$

4.6.2 Квадратичные вычеты. Символ Лежандра

Определение 51 *Пусть* $(a, m) = 1$. *Тогда* a – - *квадратичный вычет по модулю* m, *если разрешимо сравнение* $x^2 \equiv a \mod m$. *Если же оно неразрешимо, то* a — *квадратичный невычет по модулю* m.

Примеры: (см. [1, глава 3 п.10])

Предложение 11 *Пусть* p — *нечетное простое число и* $\mathbb{F}_p$ — *конечное поле порядка* p. *Положим* $(\mathbb{F}_p^*)^2 = \{x^2 | x \in \mathbb{F}_p^*\}$. *Очевидно, что* $(\mathbb{F}_p^*)^2 < \mathbb{F}_p^*$.

1. $|\mathbb{F}_p^* : (\mathbb{F}_p^*)^2| = 2$;
2. *Для любого* $x \in \mathbb{F}_p^*$ *имеем* $x^{\frac{q-1}{2}} = \pm 1$;
3. *Пусть* $x \in \mathbb{F}_p^*$. *Тогда* $x \in (\mathbb{F}_p^*)^2 \iff x^{\frac{p-1}{2}} = 1$.

Доказательство: Рассмотрим гомоморфизм групп

$$f : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$$
$$x \mapsto x^2.$$

Заметим, что $\operatorname{Ker} f = \{x | x^2 = 1\} = \{\pm 1\}$, т.к. $\mathbb{F}_p^*$ — поле. Отсюда $(\mathbb{F}_p^*)^2 = \operatorname{Im} f = (\mathbb{F}_p^*)/\operatorname{Ker} f$ и, значит $|\mathbb{F}_p^* : (\mathbb{F}_p^*)^2| = |\operatorname{Ker} f| = 2$. Далее, легко видеть, что $x^{\frac{p-1}{2}} \in \operatorname{Ker} f = \{\pm 1\}$.

Докажем последний пункт. Ясно, что $\{x | x^{\frac{p-1}{2}} = 1\} \supseteq (\mathbb{F}_p^*)^2$. Обратное включение следует из того, что, как показано выше, $|(\mathbb{F}_p^*)^2| = \frac{p-1}{2}$. $\square$

Определение 52 *Пусть* p — *нечетное простое число,* $a \in \mathbb{N}$ *не делится на* p. *Символ Лежандра* $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a \in (\mathbb{F}_p^*)^2 \\ -1, & \text{иначе.} \end{cases}$. *символ Якоби*

Другими словами $\left(\frac{a}{p}\right) = \pm 1$ и $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$.

Лемма 49 *Если сравнение* $x^2 \equiv a \mod 8$ *разрешимо, то сравнение* $x^2 \equiv a \mod 2^k$ *разрешимо для всех натуральных* k.

Предложение 12 *Пусть* $m = 2^k p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$, *где* p_i — *различные нечетные простые числа, и пусть* $(a, m) = 1$. *Тогда сравнение* $x^2 \equiv a \mod m$ *разрешимо в том и только в том случае, когда выполняются следующие условия:*

1. *Если* $k = 2$, *то* $a \equiv 1 \mod 4$; *если* $k \geqslant 3$, *то* $a \equiv 1 \mod 8$.
2. *Для каждого* i *имеем* $a^{\frac{p_i - 1}{2}} \equiv 1 \mod p_i$.

Доказательство. Из китайской теоремы об остатках сравнение $x^2 \equiv a \mod m$ эквивалентно системе

$$\begin{cases} x^2 \equiv a \mod 2^k, \\ x^2 \equiv a \mod p_1^{k_1}, \\ \dots \\ x^2 \equiv a \mod p_l^{k_l} \end{cases}$$

Рассмотрим сравнение $x^2 \equiv a \mod 2^k$. Легко проверить, что 1 — единственный квадратичный вычет по модулю 4, как и по модулю 8. Поэтому при $k \in \{2,3\}$ сравнение разрешимо только при $a \equiv 1 \mod 2^k$. Если $k \geqslant 3$, то в силу леммы 49 рассматриваемое сравнение эквивалентно сравнению $x^2 \equiv a \mod 8$, которое разрешимо тогда и только тогда, когда $a \equiv 1 \mod 8$.

По лемме Хензеля сравнение $x^2 \equiv a \mod p_i^{k_i}$ разрешимо тогда и только тогда, когда $x^2 \equiv a \mod p_i$ разрешимо. А последнее разрешимо тогда и только тогда, когда $a^{\frac{p_i-1}{2}} \equiv 1 \mod p$. □

Предложение 13 *1.* $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

3. Если $a \equiv b \mod p$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(1)- уже доказано, (2) следует из (1).

Теорема 22 *(квадратичный закон взаимности) Пусть p и q — нечетные простые числа, тогда*

1. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

3. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

4.6.3 Символ Лежандра, символ Якоби.

Определение 53 *Пусть $n = p_1 \dots p_m$, где p_k — нечетные простые числа (не обязательно различные), $a \in \mathbb{N}$ взаимно просто с n. Символом Якоби называется число* $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_m}\right)$.

Предложение 14 *Пусть n — нечетное число, тогда*

$$\left(\frac{1}{n}\right) = 1,\ \left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}},\ \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

Теорема 23 *a и n взаимно простые нечетные числа, тогда*

$$\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}}.$$

Тесты на простоту: продолжение (повторение, но на лекции было в этот момент)

4.6.4 Тест Соловея-Штрассена

$$T := \{a \in (\mathbb{Z}/n\mathbb{Z})^* | a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}.$$

Пусть для k случайных значений a мы проверим выполнение условия $a \in T$. Следующее утверждение позволяет оценить с какой вероятностью число n следует считать простым. Известное мне доказательство использует свойства квадратичных вычетов, которые мы пройдем несколько позже, поэтому пока приведу только формулировку.

Предложение 15 *Пусть n — нечетное составное число. Тогда $|T| < \frac{\varphi(n)}{2}$*

Таким образом если для k случайных значений $a \in (\mathbb{Z}/n\mathbb{Z})^*$ выполнено $a \in T$, то можно считать, что n простое с вероятностью, не меньшей чем $1 - \frac{1}{2^k}$.

4.6.5 Тест Миллера-Рабина

Пусть $n - 1 = 2^m k$, $2 \nmid k$.

$$T = \{a | a^k = 1 \text{ или } \exists j < m : a^{2^j k} = -1\}$$

Легко видеть, что если n простое, то $T = (\mathbb{Z}/n\mathbb{Z})^*$. (это следует из того, что в поле $\mathbb{Z}/n\mathbb{Z}$ уравнение $x^2 = 1$ имеет ровно 2 решения.)
К сведению.

Предложение 16 *Пусть n — нечетное составное число $3 \nmid n$ и $n - 1 = 2^m k$, $2 \nmid k$. Тогда $|T| \leqslant \frac{\varphi(n)}{4}$.*

Таким образом если для k случайных значений $a \in (\mathbb{Z}/n\mathbb{Z})^*$ выполнено $a \in T$, то можно считать, что n простое с вероятностью, не меньшей чем $1 - \frac{1}{4^k}$.

Если при фиксированном n число a проходит тест Миллера–Рабина и не показывает, что n составное, то оно проходит и тест Соловея-Штрассена с тем же результатом.

4.7 Классы вычетов. Поля. Конечные поля. Поле $\mathbb{C}$.

4.8 Поле $\mathbb{C}$

(практически дословно см. [1]) Так как многочлен x^2+1 неприводим в кольце $\mathbb{R}[x]$, а $\mathbb{R}[x]$ — кольцо главных идеалов, то идеал $(x^2 + 1)\mathbb{R}[x]$ максимален. Следовательно, факторкольцо $\mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$ является полем.

Определение 54 *Поле $\mathbb{C} := \mathbb{R}[x]/(x^2 + 1)\mathbb{R}[x]$ называется полем комплексных чисел.*

Имеется естественное вложение (мономорфизм) $\mathbb{R} \hookrightarrow \mathbb{C}$ заданный с помощью композиции отображений

$$\mathbb{R} \hookrightarrow \mathbb{R}[x] \twoheadrightarrow \mathbb{C}.$$

Будем отождествлять элементы поля $\mathbb{R}$ с их образами под действием этого мономорфизма и считать, что $\mathbb{R}$ подполе в $\mathbb{C}$.

Обозначим через i смежный класс $x+(x^2+1)\mathbb{R}[x]$. Заметим, что $i^2+1 = 0$, откуда $i^2 = -1$. Так как в любом смежном классе $p(x) + (x^2 + 1)\mathbb{R}[x]$ есть единственный многочлен степени $\leqslant 1$, то любое комплексное число можно однозначно представить в виде $a+bi$, $a, b \in \mathbb{R}$. Ясно, что сложение и умножение определены по правилам:

$$(a + bi) + (c + di) = (a + c) + (b + d)i$$
$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Пусть $z = x + iy$, $x, y \in \mathbb{R}$. Тогда $\operatorname{Re} z := x$, $\operatorname{Im} z := y$. Число $\bar{z} = x - iy$ называется комплексно сопряженным к z. Из определения сразу следует, что

- $z \in \mathbb{R} \iff z = \bar{z}$;
- $\operatorname{Re} z = \frac{z+\bar{z}}{2}$, $\operatorname{Im} z = \frac{z-\bar{z}}{2i}$;
- $z + \bar{z}, z\bar{z} \in \mathbb{R}$.

Кроме того, нетрудно проверить следующие утверждения:

1. Отображение $\mathbb{C} \longrightarrow \mathbb{C}$ переводящее z в $\bar{z}$ является автоморфизмом поля $\mathbb{C}$.
2. Для многочлена $g \in \mathbb{C}[x]$ обозначим через $\bar{g}$ многочлен, коэффициенты которого сопряжены с коэффициентами многочлена g. Пусть $w \in \mathbb{C}$. Тогда
   (a) $g(\bar{w}) = \bar{g}(\bar{w})$.
   (b) Если $g \in \mathbb{R}[x]$, то $\bar{g} = g$.
   (c) Пусть $g \in \mathbb{R}[x]$ и $g(w) = 0$. Тогда $g(\bar{w}) = 0$. Более того кратности w и $\bar{w}$ равны.

Для нахождения обратного элемента (по умножению) удобно воспользоваться равенством:

$$\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i.$$

Определение 55 *Поле F называется алгебраически замкнутым, если любой многочлен из $F[x]$ степени $\geqslant 1$ имеет хотя бы один корень в F.*

Лемма 50 *Если F алгебраически замкнуто, то любой многочлен из $F[x]$ раскладывается на множители степени 1.*

Теорема 24 *(Основная теорема алгебры). Поле $\mathbb{C}$ алгебраически замкнуто.*

Следствие 16 *Любой многочлен степени $\geqslant 3$ из кольца $\mathbb{R}[x]$ приводим. Следовательно, любой многочлен над $\mathbb{R}$ раскладывается на множители степени $\leqslant 2$.*

Доказательство: см [1, гл3 следствие 9.7] $\square$

4.8.1 Тригонометрическая форма комплексного числа.

Назовем модулем комплексного числа длину вектора, который его изображает, а его аргументом — тригонометрический угол между положительным

направлением вещественной оси и этим вектором. Другими словами,

$$|a+bi| = \sqrt{a^2+b^2}, \qquad \operatorname{Arg}(a+bi) = \arg(a+bi) + 2\pi\mathbb{Z}, \text{ где}$$

$$\arg(a+bi) = \begin{cases} \operatorname{arctg}\frac{b}{a}, & a > 0 \\ \operatorname{arctg}\frac{b}{a} + \pi, & a < 0 \\ \frac{\pi}{2}, & a = 0, b > 0 \\ -\frac{\pi}{2}, & a = 0, b < 0 \end{cases}$$

Пусть $r = |a+bi|, \varphi = \operatorname{Arg}(a+bi)$. Из определения синуча и косинуса следует, что

$$a + bi = r(\cos\varphi + i\sin\varphi).$$

правая часть последнего равенства называется тригонометрической формой комплексного числа.

Нетрудно проверить следующие формулы:

$$zw = |z| \cdot |w|(\cos(\operatorname{Arg} z + \operatorname{Arg} w) + i\sin(\operatorname{Arg} z + \operatorname{Arg} w)).$$

Другими словами, при перемножении комплексных чисел их модули перемножаются, а аргументы складываются. Отсюда следует, что для целого n имеем:

$$z^n = |z|^n(\cos(n\operatorname{Arg} z) + i\sin(n\operatorname{Arg} z)).$$

Последняя формула называется формулой Муавра.

Для сокращения записи будем использовать обозначение $e^{i\varphi} = r(\cos\varphi + i\sin\varphi)$. Смысл левой части выражения будет разъяснен позже в курсе математического анализа. Небольшую справку на эту тему можно найти в [1].

Единственность представления комплексного числа в тригонометрической форме и формулу для произведения в тригонометрической форме можно выразить следующим образом:

$$\mathbb{C}^* \cong \mathbb{R}^*_{>0} \times \mathbb{R}/2\pi\mathbb{Z}.$$

Учитывая изоморфизм $\ln : \mathbb{R}^*_{>0} \longrightarrow \mathbb{R}$, получим следующий результат:

$$\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/2\pi\mathbb{Z}$$
$$z \mapsto (\ln|z|, \operatorname{Arg} z)$$
$$e^r(\cos\varphi + i\sin\varphi) \longleftarrow (r, \varphi).$$

Так как $\mathbb{R}/\mathbb{Z} \cong \mathbb{R}/2\pi\mathbb{Z}$, можно получить более короткую запись $\mathbb{C}^* \cong \mathbb{R} \times \mathbb{R}/\mathbb{Z}$, но она менее интуитивна.

4.8.2 Уравнение деления круга. Корни из единицы.

Уравнение

$$z^n = w, \text{ где } w \in \mathbb{C}$$

называется уравнением деления круга. Найдем все его решения в поле $\mathbb{C}$. Пусть $w = se^{i\psi}$, $s \in \mathbb{R}_{>0}, \psi \in \mathbb{R}/2\pi\mathbb{Z}$. Будем искать z в тригонометрической форме $z = re^{i\varphi}$. Используя формулу Муавра, получаем $\begin{cases} r^n = s \\ n\varphi \equiv \psi \mod 2\pi\mathbb{Z}. \end{cases}$ Что эквивалентно

$$\begin{cases} r = \sqrt[n]{s} \\ \varphi = \frac{\psi}{n} + \frac{2\pi k}{n},\ k \in \mathbb{Z}. \end{cases}$$

Т.е.

$$z = \sqrt[n]{|w|}e^{i\frac{\psi+2\pi k}{n}},\ k \in \mathbb{Z}/n\mathbb{Z}.$$

Решения уравнения деления круга называются корнями из w. Символ $\sqrt[n]{w}$ обозначает множество всех корней из w. В частности, если $w = 1$, то $\sqrt[n]{1}$ является множеством всех корней их 1.

4.9 Целые гауссовы числа

В пункте 3.9 был рассмотрен пример кольца $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$ с нормой $v(a+bi) = a^2+b^2$. Это кольцо называется кольцом целых гауссовых чисел. Его элементы можно записывать в виде $a+bi$, $a, b \in \mathbb{Z}$. Иммеется вложение $\mathbb{Z}[i] \hookrightarrow \mathbb{C}$, при этом целым гауссовым числам соответствуют точки целочисленной решетки плоскости.

Рекомендуется в качестве упражнения доказать, что кольцо $\mathbb{Z}[i]$ евклидово (в пункте 3.9 это не было аккуратно доказано).

5 Многочлены

1. Кольцо многочленов $k[x]$ над полем k является евклидовым кольцом с евклидовой нормой deg.
2. Пусть $\alpha \in k$, $p(x) \in k[x]$, k — поле.
   (a) Остаток от деления многочлена $p(x)$ на $x-\alpha$ равен $p(\alpha)$.
   (b) Элемент α является корнем многочлена p тогда и только тогда, когда $p(x)$ делится на $x-\alpha$.
   (c) Многочлен степени n не может иметь больше, чем n корней.

5.0.1 Лемма Хензеля.

Лемма 51 *$f(x) \in \mathbb{Z}[x]$. $m, k \in \mathbb{N}$, $m \leqslant k$. Если $f(a) \equiv 0 \mod p^k$ и $f'(a) \neq 0 \mod p$, то $\exists s \in \mathbb{Z}$ такое, что $\begin{cases} f(s) \equiv 0 \mod p^{k+m} \\ r \equiv s \mod p^k. \end{cases}$ Причем такой s единственный по $\mod p^{k+m}$.*

Доказательство.

$$f(x) = g(x-a) = \sum_{l=0}^{n} \frac{f^{(l)}(a)}{l!}(x-a)^l$$

$$s = a + tp^k$$

$$f(a+tp^k) = \sum_{l=0}^{n} \frac{f^{(l)}(a)}{l!}(tp^k)^l \equiv [m \leqslant k] \equiv f(a) + f'(a)tp^k \equiv [f(a) = zp^k] \equiv$$

$$\equiv (z + f'(a)t)p^k.$$

$$f(a+tp^k) \equiv 0 \mod p^{k+m} \iff z + f'(a)t \equiv 0 \mod p^m$$

Последнее сравнение в силу того, что $f'(a) \neq 0 \mod p$ имеет единственное решение. $\square$

5.1 Разложение многочленов на неприводимые множители. Лемма Гаусса. Критерий Эйзенштейна

5.2 Формальные производные многочленов и число корней, конечные разности. Интерполяционные многочлены.

Теорема 25 *Пусть $t_0, y_0, \ldots, t_n, y_n \in K$, причем $t_i \neq t_j$ при $i \neq j$. Существует единственный многочлен $p(x) \in k[x]$ степени не выше n, удовлетворяющий условиям $p(t_i) = y_i$ для любого $i = 0, \ldots, n$. Этот многочлен можно найти по формуле*

$$p(x) = \sum_{i=0}^{n} y_i \frac{\Pi_{j \neq i}(x - t_j)}{\Pi_{j \neq i}(t_i - t_j)}.$$

Определение 56 *формальная производная*

Лемма 52 *Для любых $p, q \in R[x]$ и $\alpha \in R$ имеют место равенства:*

1. $(p+q)' = p' + q'$, $(\alpha p)' = \alpha p'$;
2. $(pq)' = p'q + pq'$;
3. $(p \circ q)' = (p' \circ q) \cdot q'$.

кратные корни

5.3 Поле частных, разложение на простейшие, локализация.

Лемма 53 *Пусть R — область целостности. Тогда существует поле F и мономорфизм $\lambda : R \hookrightarrow F$, обладающий следующим универсальным свойством: для любого поля K и мономорфизма $\varphi : R \hookrightarrow K$ существует единственный мономорфизм $\psi : F \hookrightarrow K$ такой, что $\varphi = \psi \circ \lambda$.*

Определение 57 *поле частных*

5.3.1 разложение на простейшие.

Определение 58 *простейшая дробь*

Теорема 26 *Пусть R — евклидово кольцо, а F — его поле частных. Любой элемент из F представим в виде суммы элемента из R и простейших дробей.*

Поле рациональных функций. Разложение рациональных функций на простейшие.

II семестр:

6 Линейная алгебра.

7 Кольцо многочленов.

Многочлены от многих переменных: выражение симметрических многочленов через элементарные симметрические. Формальные производные многочленов и число корней, конечные разности. Интерполяционные многочлены.

Неприводимые многочлены над полями - эффективная конструкция.

7.1 Алгоритм Берлекампа разложения многочлена на множители.(2-й семестр)

Алгоритм Берлекампа разложения многочлена на множители. (уже известны: конечные поля, о простых и неприводимых элементах кольца, уже нужна линейная алгебра и размерность пр-ва решений системы линейных уравнений)

Теорема 27 *Пусть $f \in \mathbb{F}_p[x]$ — многочлен положительной степени n со старшим коэффициентом 1.*

1. *Если многочлен $h \in \mathbb{F}_p[x]$ удовлетворяет соотношению $h^p \equiv h \mod f$, то*
$$f(x) = \prod_{a \in \mathbb{F}_p} (f(x), h(x) - a).$$

2. *Пусть $f = f_1 \dots f_k$, где f_i — попарно различные неприводимые многочлены со старшим коэффициентом 1. В таком случае многочлен h удовлетворяет соотношению $h^p \equiv h \mod f$ тогда и только тогда, когда $h(x) \equiv a_i \mod f_i$, где $a_i \in \mathbb{F}_p$. При этом каждому набору $(a_1, \dots, a_k)$ соответствует ровно один многочлен h, степень которого меньше степени многочлена f.*

7.2

Оценка числа неприводимых многочленов над конечным полем.

7.3 Теорема Гильберта о нулях, о базисе, базисы Гребнера и их использование в компьютерной алгебре.

7.4 Многочлены от многих переменных: выражение симметрических многочленов через элементарные симметрические.

Многочлены от многих переменных

Определение 59 *Многочлен $f(x_1, \dots, x_n)$ называется симметрическим, если для любой подстановки $\sigma \in S_n$ выполняется равенство*
$$f(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = f(x_1, \dots, x_n).$$

Основным примером симметрических многочленов служат элементарные симметрические многочлены $\sigma_k(x_1, \dots, x_n) = \sum_{i_1 < \dots < i_k} x_{i_1} \cdots x_{i_k}$, где $1 \leqslant k \leqslant n$; Положим $\sigma_0 = 1$, $\sigma_k(x_1, \dots, x_n) = 0$ при $k > n$.

Элементарные симметрические многочлены можно задавать с помощью производящей функции
$$\sigma(t) = \sum_{k=0}^{\infty} \sigma_k t^k = \Pi_{i=1}^{\infty}(1 + tx_i).$$

Если $x_1, \dots, x_n$ — корни многочлена $x^n + a_{n-1}x^{n-1} + \dots + a_0$, то $\sigma_k(x_1, \dots, x_n) = (-1)^k a_{n-k}$.

Теорема 28 *Пусть $f(x_1, \dots, x_n)$ — симметрический многочлен. Тогда существует единственный многочлен $g(y_1, \dots, y_n)$, что $f(x_1, \dots, x_n) = g(\sigma_1, \dots, \sigma_n)$.*

8 Поля.

Конечные поля, их порядок, существование и конструкции. Поле частных. Разложение рациональных функций на простейшие. Какие-нибудь представления про расширения полей(было выше)

9 Элементы теории Галуа.

10 Обозначения

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

Список литературы

[1] http://alexei.stepanov.spb.ru/students/temp/conspect.pdf

[2] Кострикин А.И. "Введение в алгебру". Основы алгебры: Учебник для вузов. — М.: Физматлит. 1994.— 320 с. — ISBN 5-02-014644-7.

[3] Кострикин А.И. "Введение в алгебру". Часть III. Основные структуры: Учебник для вузов.— 3-е изд. — М.: ФИЗМАТЛИТ, 2004.— 272 с. — ISBN 5-9221-0489-6.

[4] Алексеев В.Б. "теорема Абеля в задачах и решениях— М.: МЦНМО, 2001.

[5] А.Л.Городенцев. Алгебра. Учебник для студентов-математиков. Часть I. "МЦ НМО 2013

[6] http://alexei.stepanov.spb.ru/students/algebra3/Berns

[7] Н.А. Вавилов "Конкретная теория групп"

[8] К. Айерленд М.Роузен "Классическое введение в современную теорию чисел"

[9] Н. Коблиц "Курс теории чисел и криптографии"Москва: Научное изд-во ТВП, 2001, x+254 с.