Алгебра

Саютин Дмитрий

13 января 2017 г.

Содержание

1. Введение

1.1. Основные обозначения и определения, функции

Символ	Определение	Описание
$\cap$	$A \cap B = \{x \mid x \in A \wedge x \in B\}$	Пересечение множеств
$\cup$	$A \cup B = \{x \mid x \in A \vee x \in B\}$	Объединение множеств
$\setminus$	$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$	Разность множеств
$\times$	$A \times B = \{(x, y) \mid x \in A, y \in B\}$	Произведение множеств
$\forall x:$	Выражение верно для любого (всех) x	Квантор всеобщности
$\exists x:$	Существует x, такой что	Квантор существования
$\exists!\, x:$	Существует ровно один x, такой что	Квантор существования
$\varnothing$	$\forall x: x \notin \varnothing$	Пустое множество
$\sqcup$	$A \sqcup B = A \cup B$, при этом $A \cap B = \varnothing$	Дизъюнктное объединение
$\subset$	$A \subset B \iff x \in A \implies x \in B$	A — подмножество B

Замечание. В данном конспекте $\subset$ и $\subseteq$ означают одно и то же, но иногда запись $\subset$ используется для того, чтобы подчеркнуть, что подмножество не совпадает со всем множеством (также как $\sqcup$ используется, чтобы подчеркнтуь пустоту пересечения у операндов).

***Определение* 1.1.** Множество — аксиоматическое понятие, не имеющее определения.

***Определение* 1.2.** Функция — это упорядоченная тройка (X, Y, Γ), где X, Y — множества, а Γ — подмножество $X \times Y$, такое что $\forall x \in X: \exists!\, y \in Y: (x, y) \in \Gamma$.

***Определение* 1.3.** Множество X из предыдущего определения называется областью определения функции, множество Y — **областью** значений, а Γ — графиком функции.

***Определение* 1.4.**

- Запись $f: X \to Y$ означает, что f — функция из X в Y.
- Запись $f(x) = y$, означает, что $(x, y) \in \Gamma_f$.

***Определение* 1.5.** Образом функции f (**множеством** значений, обозначается как $\operatorname{Im} f$) называется множество $y \in Y$, таких что $\exists x \in X: f(x) = y$.

***Определение* 1.6.** Прообразом точки y у отображения f (записывается как $f^{-1}(y)$) называется множество таких x, что $f(x) = y$.

***Определение* 1.7.** Прообразом множества $\hat{y}$ у отображения f (записывается как $f^{-1}(\hat{y})$ называется множество таких x, что $f(x) \in \hat{y}$.

Упражнение: Докажите, что $f^{-1}(\hat{y}) = \bigcup\limits_{y \in \hat{y}} f^{-1}(y)$.

***Определение* 1.8.** Пусть $f\colon X \to Y$ и $Z \subset X$. Тогда функцию f можно сузить на множество Z (записывается как $f|_Z$), где $f|_Z(x) := f(x)$.

***Определение* 1.9.** Пусть $f\colon X \to Y,\ g\colon Y \to Z$, определим композицию функций $g \circ f\colon X \to Z$: $(g \circ f)(x) := g(f(x))$

***Определение* 1.10.** Отображение id_X из X в X, такое что $\forall x\colon id_X(x) = x$ называется тождественным отображением.

***Определение* 1.11.** Две функции называются равными, если они равны на всей области определения.

***Определение* 1.12.** Пусть $f\colon X \to Y$. Отображение $y\colon Y \to X$ называется:

- Обратным к f слева, если $f \circ g = id_Y$
- Обратным к f справа, если $g \circ f = id_X$.
- Обратным к f, если оно обратно к f слева и справа.

***Определение* 1.13.** Функция f называется инъекцией (вложением), если

- $\forall x, y\colon f(x) = f(y) \implies x = y$

***Определение* 1.14.** Функция f называется сюръекцией, если образ функции совпадает с областью значений.

- $\forall y \in Y\colon \exists x \in X\colon f(x) = y$

***Определение* 1.15.** Функция называется биекцией, если она одновременно является и инъекцией, и сюръекцией.

Теорема 1.1. Пусть $g\colon X \to Y$. Следующие условия экивалентны:

1. g — биекция.
2. $\exists g'\colon Y \to X\colon g \circ g' = id_Y,\ g' \circ g = id_X$.
3. $\exists f, h\colon Y \to X\colon g \circ f = id_Y,\ h \circ g = id_X$.

Доказательство.

- “1” $\implies$ “2”. Рассмотрим функцию $g' = (Y,\ X,\ \Gamma_{g'})$, где $\Gamma_{g'} = \{(y,\ x) \mid (x,\ y) \in \Gamma_g\}$.

  Так как f — биекция, то график задан корректно: для каждого y найдётся (так как выполнена сюръекция) ровно один (так как выполнена биекция) x, такой что $(y,\ x) \in \Gamma_{g'}$

  Показать тождественность композиций остаётся в качестве упражнения для читателя.
- “2” $\implies$ “3”. Просто возьмём $f := g', h := g'$.
- “3” $\implies$ “2”. $f = id_X \circ f = (h \circ g) \circ f = h \circ (g \circ f) = h \circ id_Y = h$, тем самым $f = h$.
- “2” $\implies$ “1”:

– Верна инъективность:
$g(x) = g(y) \implies g'(g(x)) = g'(g(y)) \implies (g' \circ g)(x) = (g' \circ g)(y) \implies id_X(x) = id_X(y) \implies x = y$.

– Верна сюръективность:
Сюръективность $\iff \forall y \colon g^{-1}(y) \neq \varnothing$ (см 1.6).
Покажем, что $g'(y) \in g^{-1}(y)$, тем самым последнее не пусто.
И действительно $g(g'(y)) = (g \circ g')(y) = id_Y(y) = y$. □

Замечание. Тем самым мы показали, что функция является биекцией тогда и только тогда, когда она обратима (см пункты 1 и 2 теоремы).

1.2. Бинарные отношения

Пусть X, Y — множества, а $R \subseteq X \times Y$.

***Определение* 1.16.** R называется отношением между объектами из X и Y. Запись xRy означает, что $(x, y) \in R$.

Замечание. Как правило нас будут интересовать интересовать ситуация, когда $X = Y$, т.е. отношение между элементами одного множества. Такие отношения называются отношениями **на множестве** X.

Пример 1. $X = Y$, отношение равенства.

Пример 2. $X = Y = \mathbb{R}$, отношение $\leqslant$.

Пример 3. $X = Y = \mathbb{N}$, отношение кратности $\vdots$

Пример 4. График функции тоже является отношением.

***Определение* 1.17.** Бинарное отношение на множестве M называется:

- Рефлексивным, если $\forall x \in M \colon xRx$.
- Антирефлексивным, если $\forall x \in M \colon \neg(xRx)$.
- Симметричным, если $\forall x, y \in M \colon xRy \implies yRx$.
- Антисимметричным, если $\forall x, y \in M \colon xRy \wedge yRx \implies x = y$.
- Асимметричным, если $\forall x, y \in M \colon xRy \implies \neg(yRx)$.
- Транзитивным, если $\forall x, y, z \in M \colon xRy \wedge yRz \implies xRz$.

Замечание. Отношение асимметрично тогда и только тогда, когда оно антисимметрично и антирефлексивно.

***Определение* 1.18.** Отношение называется отношением эквивалентности, если оно рефлексивно, транзитивно, симметрично.

Замечание. Отношения эквивалентности часто обозначаются через $\sim$.

***Определение* 1.19.** Пусть $\sim$ — отношение эквивалености, классом эквивалентности элемента x называется множество элементов, состоящих с ним в отношении:

- $\bar{x} = \{y \mid x \sim y\}$

Лемма.

1. Классы экивалентности совпадают или не пересекаются.
2. Множество распадается на диъюнктное объединение ($\sqcup$) классов эквивалентности.
3. Всякое разбиение множества X на непересекающиеся подмножества есть разбиение на классы эквивалентности по этому признаку.

Доказательство.

1. Пусть $\bar{x} \cap \bar{y} \neq \varnothing \implies \exists z \in \bar{x} \cap \bar{y}$.

   Тогда $z \sim x, z \sim y \implies x \sim y \implies \bar{x} = \bar{y}$.

   Действительно, $t \in \bar{x} \iff t \in \bar{y}$, по определению отношения эквивалентности 1.18.

2. Заметим, что $X = \bigcup\limits_{x \in X} \bar{x}$ (каждый x входит хотя бы в свой класс эквивалентности).

   Но классы эквивалентности либо совпадают, либо не пересекаются, поэтому можно из объединения убрать совпадающие классы, оставив каждый только в одном экземпляре, и тем самым получить требуемое разбиение.

3. Определим $x\ y$, когда x лежит в том же подмножестве, что и y. Заметим, что:
   - Верна рефлексивность ($x \sim x$)
   - Верна симметричность ($x \sim y \implies y \sim x$).
   - Верна транзитивность ($x \sim y, y \sim z \implies x \sim z$). □

***Определение* 1.20.** Пусть X — множество, $\sim$ — отношение эквивалентности на X (1.18). Тогда $X/\sim$ — множество всех классов эквивалентности.

Пример 1. Отношение равенства является отношением эквивалентности.

Пример 2. Сравнимость по модулю является отношением эквивалентности:

Пусть $a, b \in \mathbb{Z}, n \in N$. $\quad a \sim b := (a - b) \vdots n$.

Проверим определение отношения эквивалентности:

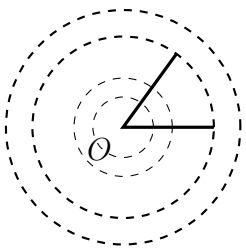
- Рефлексивность: $x - x = 0 \vdots n$.
- Симметричность: $(x - y) \vdots n \implies (y - x) \vdots n$.
- Транзитивность: $(x - y) \vdots n, (y - z) \vdots n \implies (x - y) + (y - z) \vdots n \implies (x - z) \vdots n$.

$\mathbb{Z}/\sim$ принято обозначать как $Z/n\mathbb{Z}$, подробнее об этом будет рассказано позднее, но уже сейчас можем понять как устроено это множество: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots \overline{n-1}\}$, где:

- $\overline{0} = \{m \in \mathbb{Z} \mid m \vdots n\}$
- $\overline{1} = \{m \in \mathbb{Z} \mid (m - 1) \vdots n\}$
- $\ldots$

Несложно понять, что эти классы непересекаются и в объединении дают всё множество $\mathbb{Z}$.

Пример 3. Множество точек на плоскости, точки эквивалентны, если находятся на одинаковом расстоянии от точки $(0,\ 0)$. Классы эквивалентности — все окружности с центром в O.



1.3. Порядки и лемма Цорна

***Определение* 1.21.** Бинарное отношение $\leqslant$, являющееся рефлексивным, транзитивным, антисимметричным (определение 1.17) называется отношением частичного порядка, а множество, на котором введён порядок называется частично упорядоченным.

***Определение* 1.22.** Линейным (также известен как полный порядок или цепь) называется частичный порядок, такой что $\forall a, b\colon a \leqslant b$ или $b \leqslant a$.

***Определение* 1.23.** Элемент a частично упорядоченого множества называется минимальным, если не существует элемента меньшего его.

- Иначе говоря $m \leqslant a \implies m = a$.

***Определение* 1.24.** Элемент a частично упорядоченного множества называется наименьшим, если он меньше или равен любого другого элемента.

- $\forall x\colon x \leqslant a$.

Замечание 1. Понятия наибольшего и максимального элемента вводятся аналогично.

Замечание 2. Обратите внимание, что $=$ имеет свой обычный смысл, а не смысл оператора сравнения. Т.е. если $a \leqslant b$ и $b \leqslant a$, то b совпадает с a $(b = a)$.

Замечание 3. Частичный порядок как правило вводится как оператор "$\leqslant$". Аналогично его можно ввести через оператор "$<$", такой порядок называется строгим частичным порядком.

Замечание 4. Если определён хотя бы один оператор "$<$", "$\leqslant$", "$>$", "$\geqslant$", то естественным образом можно доопределить остальные (чем мы, возможно, будем впоследствии пользоваться).

Замечание 5. Минимальных элементов может быть несколько, а вот наименьший элемент (если он существует) ровно один.

Упражнение: Приведите пример частично упорядоченного множества в котором несколько минимальных элементов.

Упражнение: Докажите последнее замечание (о том, что наименьших элементов не может быть несколько).

Пример 1. $\mathbb{R}$ является частично упорядоченным множеством с порядком $\leqslant$.

Пример 2. Множество $\mathbb{N}$, $a \leqslant b := b \vdots a$. ($\leqslant$ означает новый введённый порядок, а не обычное сравнение значений).

Пример 3. Множество всех подмножеств какого-то множества X (обозначается 2^X). $a \leqslant b := a \subseteq b$.

Упражнение: Покажите по определению, что все бинарные отношения из примеров являются отношениями порядка.

***Определение* 1.25.** Пусть X — частично упорядоченное множество, а Y — его подмножество. Тогда на Y можно ввести такой же порядок, как и на множестве X. Такой порядок называется индуцированным.

***Определение* 1.26.** Пусть X — частично упорядоченное множество, а Y — его подмножество, упорядоченное по индуцированному порядку, тогда элемент $x \in X$ называется вверхней гранью, если:

- $y \leqslant x\ \forall y \in Y$.

Замечание. Понятие нижней грани вводится аналогично.

Лемма (Цорна)**.** Частично упорядоченное множество, в котором любое линейно упорядоченное подмножество (по индуцированному порядку) имеет верхнюю грань, содержит максимальный элемент.

Доказательство. Даётся без доказательства.

В интернете есть несколько доказательств, но они используют сложные технологии, вроде трансфинитной индукции и ординалов.

- wikipedia(en)
- mccme(ru) □

2. Группы. Введение

2.1. Группы и подобное. Определения

Пусть X —множество с ведённой на нём операцией $*\colon X \times X \to X$.

Бинарная операция $*$ может обладать некоторыми свойствами:

#	Название	Определение
1	Ассоциативность	$\forall x, y, z \in X\colon (x * y) * z = x * (y * z)$
2	Существование нейтрального	$\exists e \in X\colon \forall x \in e\colon xe = ex = x$
3	Существование обратного	$\forall x \in X\colon \exists x^{-1}\colon x * x^{-1} = x^{-1} * x = e$
4	Коммутативность	$\forall x, y \in X\colon x * y = y * x$

***Определение* 2.1.** Множество с операцией $*$ на нём называется:

- Полугруппой, если верно (1).
- Моноидом, если верно (1, 2).
- Группой, если верное (1, 2, 3).
- Абелевой группой, если верно (1, 2, 3, 4).

Пример. Пусть Ω — множество всех отображений из X в X.

Определим операцию "$*$" как композицию отображений.

Тогда верны свойства 1 (по определению композиции) и 2 ($e = id_X$). Тем самым Ω — моноид.

Свойство 3 будет верно, если оставить только биекции (существование обратных обеспечивает теорема 1.1), свойство 4 неверно совсем.

Упражнение: приведите контр-пример к пункту 4.

Лемма. Если $*$ — ассоциативна и есть нейтральный элемент *[т.е. это моноид]*, то:

1. Нейтральный элемент единственный.
2. Обратный либо $\nexists$, либо $\exists!$
3. Если x и y обратимы, то $x * y$ обратим.
4. Множество обратимых элементов образует группу.

Доказательство.

1. Пусть e_1, e_2 — нейтральные, тогда $e_1 = e_1 * e_2 = e_2$.
2. Пусть y_1, y_2 — обратные к x, тогда $y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2$.
3. Покажем, что $(y^{-1} * x^{-1})$ является обратным к $x * y$

- $(x * y) * (y^{-1}x^{-1}) = e$
- $(y^{-1}x^{-1}) * (x * y) = e$

4. В множестве обратимых элементов:
   - Ассоциативность верна, так как была верна для любых элементов моноида.
   - Есть нейтральный (так как нейтральный элемент обратим).
   - Любой элемент обратим (по определению этого множества).
   - Рассмотренная группа замкнута, т.е. $\forall x, y\colon\ x^{-1}$ лежит в множестве (так как у него есть обратный элемент — x), и $x * y$ лежит в множестве (см пункт 3). □

Замечание. В теории групп операцию на группе часто обозначают через умножение и применяют мультипликативную нотацию: $x * y$, или xy. $\underbrace{x * x * \ldots * x}_{n \text{ раз}} = x^n$. Обратный элемент записывается как x^{-1}.

Операцию также можно обозначить через $+$, тогда $\underbrace{x + x + \ldots + x}_{n \text{ раз}} = nx$, и обратный как $-x$.

Вторая (аддитивная) нотация как правило используется при работе с коммутативными (абелевыми) группами.

Пример 1. $\{-1, +1\}$, операция умножения.

Является абелевой группой.

Пример 2. Движения плоскости, оставляющие на месте заданную точку.

Операция композиции (сначала применить одно отображение, потом второе).

Является группой, но не абелевой.

Замечание. Все такие движения являются либо поворотами вокруг данной точки, либо отражением относительно прямой, проходящей через эту точку.

Пример 3. Кольцо вычетов или $\mathbb{Z}/_{n\mathbb{Z}}$, подробнее его, а также смысл этого обозначения мы будем обсуждать позже.

Пока можно считать, что это множество целых чисел от 0 до $n - 1$ и операция сложения по модулю.

Является абелевой группой.

Пример 4. Пусть G — группа, а X — множество.

Рассмотрим множество $M(X, G) = \{f\colon X \to G\}$ всех функций из X в G.

Тогда на данном множестве можно ввести операцию $*$:

$(f * h)(x) = f(x) * h(x)$.

Операция $*$:

Ассоциативна	$(f*(g*h))(x) = f(x)*(g*h)(x) = f(x)*g(x)*h(x) = (f*g)(x)*h(x) = ((f*g)*h)(x)$
Имеет нейтральный	Функция тождественно равная e_G
Имеет обратный	Отправим элемент в обратный элемент к результату исходной функции ($f^{-1}(x) = f(x)^{-1}$)

2.2. Симметрическая группа

Пример 5. Пусть X — множество из n элементов, рассмотрим S_X — множество всех биекций из X в X и операцию композиции.

Упражнение: Проверьте, что композиция двух биекций является биекцией (т.е. операция композиции замкнута), а также 3 свойства группы.

Замечание. Группу S_X для $X = \{1, 2, \ldots, n\}$ часто обозначают как S_n.

Элементы данной группы называются перестановками (перестановка переводит одни элементы в другие), их часто записывают в одной из двух форм:

$\sigma = (1\,2\,3)\,(4)$ — цикловая запись, $\sigma = [2\,3\,1\,4]$ — "обычная" запись.

В перестановке σ: $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$, $\sigma(4) = 1$.

Группу S_n также называют симметрической подгруппой порядка n.

Замечание. $|S_n| = n!$ (первый элемент можно перевести в любой, второй в любой из $n - 1$ оставшихся, и так далее).

Замечание. Цикловая запись существует у любой перестановки и единственна с точностью до порядка циклов.

Понять это можно следующим образом (на примере $X = \{1, 2, \ldots, n\}$):

Рассмотрим последовательность 1, $\sigma(1)$, $\sigma^2(1)$ .... Заметим, что рано или поздно последовательность повторится (требуем конечности X).

Так как σ — биекция, то мы не могли получить что-то отличное от 1 — иначе у повторившегося элемента есть два обратных — предыдущие элементы в той же последовательности у обоих вхождений.

Затем аналогичную последовательность можно рассмотреть от произвольного не рассмотренного элемента.

Несложно понять, что других цикловых записей не бывает (мы только что построили цикловую запись из соображений того, какая она должна быть, значит по-другому построить нельзя).

***Определение* 2.2.** Перестановка называется циклом, если в её цикловой записи один цикл.

***Определение* 2.3.** Транспозицией называется цикл длины 2

***Определение* 2.4.** Для $\sigma \in S_n$ инверсией называется такая пара i, j, что $i < j$ и $\sigma(i) > \sigma(j)$.

***Определение* 2.5.** Перестановка называется чётной, если число её инверсией чётно. Аналогично вводится понятие нечётной перестановки.

***Определение* 2.6.** Каждой перестановке можно сопоставить знак (число из $\{+1, -1\}$) по следующему правилу: $\operatorname{sign}\sigma = (-1)^{N(\sigma)}$, где $N(\sigma)$ — число инверсий.

Чётным перестановкам соответсвует знак $+1$, а нечётным — знак -1.

Утверждение 2.1. Для любых двух перестановок σ_1, σ_2:

$\operatorname{sign}(\sigma_1\sigma_2) = (\operatorname{sign}\sigma_1)(\operatorname{sign}\sigma_2)$.

Доказательство. **TODO: Дописать доказательство** □

Утверждение 2.2. Любая перестановка раскладывается в произведение транспозиций вида $(i, i + 1)$.

Доказательство. **TODO: Дописать доказательство** □

Утверждение 2.3. Любая перестановка раскладывается в произведение транспозиций вида (a, i), для фиксированного a и всех i.

Доказательство. **TODO: Дописать доказательство** □

Следствие. Цикл чётной длины является нечётной перестановкой, а нечётной длины — чётной.

Доказательство. Будет напрямую следовать из правила перемножения знаков и разложения цикла в транспозицию. □

2.3. Подгруппы

***Определение* 2.7.** Подмножество $H \subseteq G$ называется подгруппой в G, если оно само является группой относительно тех же операций. Иными словами, для того, чтобы H было подгруппой, необходимо выполнение следующих трех условий.

1. $h, g \in H \Rightarrow hg \in H$
2. $h \in H \Rightarrow h^{-1} \in H$
3. $e \in H$

Замечание. Подгруппа H всегда содержит нейтральный элемент из G и является группой относительно той же операции.

Замечание. Обозначение H - подгруппа G: $H \leq G$

Замечание. Для любой группы мы всегда сможем предъявить хотя бы две подгруппы: сама группа и множество из одного нейтрального элемента(если группа содержит только один элемент, то только одну, так как они совпадут).

Лемма. $H \neq 0$ - подгруппа $\iff \forall x, y \in H \; xy^{-1} \in H$

Доказательство. Необходимость $\Rightarrow$. H - подгруппа $\Rightarrow x \in H$ и так как $y \in H \Rightarrow y^{-1} \in H \Rightarrow xy^{-1} \in H$
Достаточность $\Leftarrow$. $x \in H \Rightarrow xx^{-1} \in H = e_H \in He_Hx^{-1} \in H$

$$\begin{cases} x, y \in H \\ y^{-1} \in H \end{cases}$$

$\Rightarrow x(y^{-1})^{-1} = xy \in H$ □

Пример. $4\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z}$

Пример. $\{e\} \leq G; \; G \leq G$

Пример. $A_n < S_n$
A_n - группа четных перестановок.

Существует две конструкции, позволяющие легко строить подгруппы в неабелевых группах.

1. Центр.

***Определение* 2.8.** Множество элементов, коммутирующих со всеми элементами G, называется цетром группы и обозначается $C(G)$

Группа G в том и только том случае абелева, когда $G = C(G)$. Группа G, для которой C(G) = 1, называется группой с тривиальным центром или, без затей, группой без центра. Например, центр неабелевой простой группы тривиален.

- $C(S_n) = 1$, при $n \geq 1$
- $C(A_n) = 1$, при $n \geq 4$

2. Централизатор элемента. Пусть $x \in G$. Определим централизатор элемента x в группе G следующим образом: $C_G(x) = \{g \in G \mid gx = xg\}$.

Замечание. $C_G(x) \leq G$

Лемма. Для любого $x \in G$ имеем $C_G(x) \leq G$

Доказательство. $x1 = x = 1x$, поэтому $C_G(x) \neq \varnothing$. Если $h, g \in C(G)$, то $(hg)x = h(gx) = h(xg) = (xh)g = x(hg)$, так что $hg \in C(G)$. С другой стороны, если $h \in C(G)$, то умножая равенство $hx = xh$ на h^{-1} справа и слева, получаем $xh^{-1} = h^{-1}x$, так что $h^{-1} \in C(G)$. Отсюда следует, что $C(G) \leq G$. □

Замечание. На самом деле $C(G) = \bigcap C_G(x)$, где пересечние берется по всем x.

Замечание. Еще есть цетрализатор и нормализатор подмножества. Их определения очень похожи на определения центра и цетрализатора группы.

***Определение* 2.9.** Подгруппа G, порожденная множеством X - это наименьшая подгруппа в G, содержащая множество X.

Замечание. Обозначение: $G = \langle X \rangle$

Замечание. $H_1 \leq G$, $H_2 \leq G$, то $H_1 \cap H_2 \leq G$

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

Лемма. $\langle X \rangle$ состоит из всех элементов вида $x_1 \cdot x_2 \ldots \cdot x_n$, где каждый из элементов $x_i \in X \cup X^{-1}$
$\subset$: X - наименьшая подгруппа $\Rightarrow$ $H \geq \langle X \rangle$
$\supset$: $x_1 \ldots x_n \in \langle X \rangle \Rightarrow H \leq \langle X \rangle$

***Определение* 2.10.** Подгруппа, порожденная одним элементом, называется циклической.

Замечание. $< g >= \{g^i | i \in Z\}$

Замечание. Порядок подгруппы, порожденной элементом g называется порядком элемента g.

Замечание. Если все степени g^i, то $< g >$ бесконечна.

Если степени g^i повторяются, то есть $\exists k, l \in N \; k > l \; g^k = g^a \iff g^{k-l} = e$

Утверждение 2.4. $ordg = \min\{n \in N \mid g^n = e\}$

Доказательство. $< g >= \{g^0, g^1, g^2, \ldots, g^{n-1}\}$
Важно заметить, что $g^n = e$
$g^{mn+k} = (g^n)^m \cdot g^k = eg^k = g^k$, где $k \in \{0, \ldots, n-1\}$, так как k - это остаток. □

2.4. Гомоморфизм групп

***Определение* 2.11.** Пусть $(G, *)$, $(H, \cdot)$ - группы:

1. Функция $f : G \to H$ - гомоморфизм групп, если $\forall x,\ y\ \in G\ f(x * y) = f(x) \cdot f(y)$
2. Инъективный гомоморфизм - мономорфизм
3. Сюръективный гомоморфизм - эпиморфизм
4. Биективный гомоморфизм - изоморфизм

Замечание. G изомофрно H обозначается следующим образом: $G \cong H$

***Определение* 2.12.** Ядро гомоморфизма : $Kerf = \{g \in G\ |f(g) = e_H\}$

***Определение* 2.13.** Образ гомоморфизма : $Imf = f(G) = \{g \in G\ |f(g)\}$

Лемма. $f : G \to H$ - гомоморфизм, тогда:

1. $f(e_G) = e_H$
2. $f(x^{-1}) = f^{-1}(x)$
3. Пусть $g \in G\ f(g) \cdot h$, тогда $f^{-1}(h) = g \cdot Kerf$
4. Гомоморфизм f - инъективный(мономорфизм) $\iff$ $Kerf = \{e_G\}$
5. $Kerf \leq G$

Доказательство.

1. $f(e_G) = f(e_G \cdot e_G) = f(e_G)f(e_G)$ домножим на $(f(e_G))^-1$
   $f(e_G)(f(e_G))^{-1} = f(e_G)f(e_G)(f(e_G))^{-1}$
   $e_H = f(e_G) * e_H = f(e_G)$
2. $f(x)f(x^{-1}) = f(xx^{-1}) = f(e_G) = e_H$
3. $gKerf = \{gx\ |x \in Kerf\} = f^{-1}(h)$
   $\subset$: $y \in gKerf \Rightarrow y = gx,\ x \in Kerf \Rightarrow f(y) = f(g)f(x) = he_x = h \Rightarrow y \in f^{-1}(h)$
   $\supset$: Пусть $y \in f^{-1}(h) \Rightarrow y = g(g^{-1}y) \in gKerf$
   $g^{-1}y \in Kerf$
   $f(g^{-1}y) = f(g^{-1})f(y) = (f(g))^{-1}f(y) = h^{-1}h = e_H \Rightarrow g^{-1}y \in Kerf$
4. f - инъективный гомоморфизм $\iff$ $Kerf = \{e_G\}$ следует из 3 пункта, так как можно предъявить биекцию
5. a). $x \in Kerf \Rightarrow x^{-1} \in Kerf$
   $f(x) = e_H$
   Знаем второе свойство, делаем так: $f(x^{-1}) = (f(x))^{-1} = e_H^{-1} = e_H \Rightarrow x^{-1}Kerf$
   b). $x, y \in Kerf \Rightarrow xy \in Kerf$
   $f(x) = f(y) = e_H \Rightarrow f(xy) = f(x)f(y) = e_He_H = e_H$

□

3. Кольца

3.1. Введение

***Определение* 3.1.** Множество R с операциями $+, \cdot$ на нём называется кольцом, если:

1. $(R, +)$ — абелева группа.
2. $\forall x,\, y,\, z \in R\colon \begin{matrix}(x+y)z = xz + yz \\ x(y+z) = xy + xz\end{matrix}$ (дистрибутивность)

***Определение* 3.2.** Кольцо называется ассоциативным, если $*$ — ассоциативна $(x(yz) = (xy)z)$.

***Определение* 3.3.** Кольцо называется коммутативным, если $*$ — коммутативна $(xy = yx)$.

***Определение* 3.4.** Кольцо называется кольцом с единицей, если $\exists 1\colon x \cdot 1 = 1 \cdot x = x\ \forall x \in R$.

***Определение* 3.5.** Ассоциативное кольцо с единицей, причём $1 \neq 0$, в котором всякий ненулевой элемент обратим [по умножению] называется телом.

***Определение* 3.6.** Коммутативное тело называется полем.

Пример 0. $2\mathbb{Z}$ —коммутативное, ассоциативное кольцо без 1.

Пример 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}/n\mathbb{Z}$

Пример 2. Пусть R — коммутативное, ассоциативное кольцо с единицей.

$R[x]$ — кольцо многочленов с коэффициентами из R.

$R[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid a_i \in R,\, n \in \mathbb{N}_0\}$

Пример 3. $R[[x]] = \{\sum\limits_{i=0}^{\infty} a_i x^i \mid a_i \in R\}$ — кольцо формальных степенных рядов.

***Определение* 3.7.** Если R — кольцо, то $(R, +)$ (также записывается как R^+) называется аддитивной группой кольца.

***Определение* 3.8.** Пусть R — ассоциативное кольцо с 1, тогда $(R, \cdot)$ — моноид.

Обозначим как R^* множество обратимых элементов моноида.

Пример (к множеству обратимых элементов). $\mathbb{Z}^* = \{+1, -1\},\ \mathbb{Q}^* = \mathbb{Q} \setminus \{0\},\ \mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Пример 4. X — множество, R — кольцо.

Введём структуру кольца на множестве отображений $X \to R$.

$(f + g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = f(x) \cdot g(x)$

***Определение* 3.9.** Функция из $\mathbb{R}^2 \to \mathbb{R}^2$ называется линейной, если:

1. $f(x + y) = f(x) + f(y), \forall x, y \in \mathbb{R}^2$.
2. $f(cx) = cf(x), \forall c \in \mathbb{R}, \forall x \in \mathbb{R}^2$.

Пример 5. Множество линейных функций $\mathbb{R}^2 \to \mathbb{R}^2$.

- $f, g\colon \mathbb{R}^2 \to \mathbb{R}^2$
- $(f+g)(x) = f(x) + g(x)$
- $f \cdot g = f \circ g$

Упражнение: кольцо ли?

Пример 6. A — абелева группа, есть $+$, 0.

$x, y \in A\colon x \cdot y := 0$.

***Определение* 3.10.** Кольцо, в котором все произведения равны нулю, называется кольцом с нулевым умножением.

3.2. Свойства колец

Лемма. Пусть R - кольцо (ассоциативное), $r \in R$, тогда:

1. r * 0 = 0 * r = 0
2. Если R - кольцо с единицей, то $(-1) * r = -r$, где $(-x)$ означает обратный элемент по сложению.
3. Если $|R| \neq 1$, то $0 \neq 1$.

Доказательство.

1. - $r + 0 = r = 0 + r$.
   - $r(r+0) = r^2$
   - $r^2 + r * 0 = r^2$
   - $r * 0 = 0$.
   - Аналогично доказывается правое равенство.
2. Пользуемся дистрибутивностью кольца:
   $(-1) * r = (-r) \iff (-1)r + r = 0 \iff (-1)r + 1 * r = 0 \iff r(-1+1) = 0. \iff r * 0 = 0.$
3. Пусть $0 = 1$. Тогда $\forall r \in R\colon r = 1 * r = 0 * r = 0 \implies R = \{0\} \implies |R| = 1.$ □

***Определение* 3.11.** R^* (также обозначается как $R^\times$) – множество обратимых элементов кольца по умножению.

***Определение* 3.12.** Пусть R — коммутативное кольцо.

Элемент $r \in R \setminus \{0\}$ называется делителем нуля, если $\exists s \in R \setminus \{0\}\colon rs = 0$.

***Определение* 3.13.** Пусть R — коммутативное кольцо.

Элемент $r \in R \setminus \{0\}$ называется нильпотентным, если $\exists n \in \mathbb{N}\colon r^n = 0$

Замечание 1. Если $r \in R^*$, то r не делитель нуля.

Доказательство.

- $rs = 0$, если r — делитель нуля.

- $r^{-1} * r = 1$, если r — обратим.
- $s = r^{-1}rs = r^{-1} * 0 = 0$, если верны оба.
- Противоречие. □

Замечание 2. В $\mathbb{Z}/n\mathbb{Z}$ есть делители нуля $\iff$ n – составное.

- Если $n = ml$ $(m, l \geqslant 2)$, то и m и l - делители нуля.
- Если есть делители нуля, то $\exists m, l \geqslant 2,\ ml \vdots n$, что невозможно.

Замечание 3. В $\mathbb{Z}/n\mathbb{Z}$ нильпотенты $\iff$ n делится на какой-то квадрат.

" $\Longleftarrow$ ": Если n делится на квадрат ($n = m^2 l$, где $m > 1$), то $r = ml$ — нильпотент.

" $\Longrightarrow$ ": Оставлено в качестве упражнения.

Утверждение 3.1. Если в кольце R нет делителей нуля, то в $R[x]$ их тоже нет.

Доказательство. Пусть в $R[x]$ есть делители нуля, иначе говоря

$(a_t x^t + \ldots + a_1)(b_k x^k + \ldots + b_1) = 0.$

Потребуем, что $a_t \neq 0$ и $b_k \neq 0$, т.е. это старшие коэффициенты в соответствующих многочленах.

Заметим, что при степени x^{t+k} будет коэффициент $a_t b_k$. Но так как справа нулевой многочлен, то все коэффициенты произведения равны 0.

То есть $a_t b_k = 0$, но в R нет делителей нуля, противоречие. □

***Определение* 3.14.** Коммутативное ассоциативное кольцо с 1 без делителей нуля называется областью целостности (целостным кольцом).

3.3. Гомоморфизм колец

***Определение* 3.15.** $f\colon A \to B$ называется гомоморфизмом колец, если:

- A, B — кольца.
- $\forall a,\, b \in A\colon f(a + b) = f(a) + f(b)$.
- $\forall a,\, b \in A\colon f(ab) = f(a)f(b)$.

***Определение* 3.16.** $\operatorname{Ker} f = f^{-1}(0) = \{x \in A \mid f(x) = 0\}$

***Определение* 3.17.** $\operatorname{Im} f = \{f(x) \mid x \in A\}$.

Замечание. Если $f\colon A \to B$ — гомоморфизм колец, то:

1. $f(0_A) = 0_B$
2. $f(-r) = -f(r)$
3. Если $f(a) = b$, то $f^{-1}(b) = a + \operatorname{Ker} f$
4. f — инъективна $\iff$ $\operatorname{Ker} f = \{0\}$

Доказательство. Уже было доказано в теории групп. □

Замечание. Единица не всегда сохраняется, даже если она есть во втором кольце.

Упражнение: привести пример.

***Определение* 3.18.** Гомоморфизм нулевой, если он переводит все элементы в 0.

Утверждение 3.2. Если $f\colon A \to B$ ненулевой гомоморфизм колец. A — кольцо (ассоциативное, коммутативное) с 1. B — область целостности, то $f(1_A) = 1_B$.

Доказательство. $f(1_A) = f(1_A * 1_A) = f(1_A) * f(1_A)$

$f(1_A) - f(1_A) * f(1_A) = 0_B$

$f(1_A)(1_B - f(1_A)) = 0_B$.

Так как B — область целостности, то $f(1_A) = 0$ или $f(1_A) = 1_B$.

Если $f(1_A) = 0_B$, то $\forall a \in A\colon f(a) = f(1 * a) = f(1)\, f(a) = 0\, f(a) = 0 \implies f$ — нулевой.

Следовательно $f(1_A) = 1_B$. □

Замечание. Далее гомоморфизм колец с единицей означает гомоморфизм колец, обладающий свойством выше ($f(1_A) = 1_B$).

Лемма. Если $f\colon A \to B$ — гомоморфизм колец с единицей, то $\forall x \in A^*\colon f(a^{-1}) = f(a)^{-1}$

Доказательство. Сводится к утверждению из прошлой темы □

***Определение* 3.19.** Пусть R — кольцо с 1, введём *канонический гомоморфизм* $\phi : \mathbb{Z} \to R$:

$$\phi(n) = \begin{cases} 0 & n = 0 \\ \underbrace{1_R + 1_R + \ldots + 1_R}_{n \text{ раз}} & n > 0 \\ -\phi(-n) & n < 0 \end{cases}$$

Действительно является гомоморфизмом (следствие дистрибутивности).

***Определение* 3.20.** Если канонический гомоморфизм ϕ — инъективен ($\operatorname{Ker}\phi = \{0\}$), то характеристика ноль ($\operatorname{Char} R := 0$)

Иначе ядро нетривиально. Но в $\mathbb{Z}$ любое нетривиальное ядро имеет вид $n\mathbb{Z}$ (для некоторого $n \geqslant 1$), такое n и называется характеристикой кольца R ($\operatorname{Char} R = n$).

***Определение* 3.21.** Непустое подмножество кольца R называется подкольцом, если

- $\forall a, b \in A\colon a + b,\ -a,\ ab \in A$

***Определение* 3.22.** Аддитивная подгруппа $I \leqslant R^+$ называется:

- Левым идеалом, если $\forall r \in R, \forall s \in I\colon rs \in I$ (иначе говоря, $RI \subseteq I$)
- Правым идеалом, если $\forall r \in R, \forall s \in I\colon sr \in I$ (иначе говоря, $IR \subseteq I$).
- Двусторонним идеалом, если она и левый и правый идеал.

Пример 1. В $\mathbb{Z}$ все идеалы имеют вид $n\mathbb{Z}$. Просто из-за того, что все подгруппы $\mathbb{Z}$ имеют такой вид.

Замечание. В этих примерах не написано о каком именно идеале идёт речь, потому что в коммутативных кольцах все идеалы совпадают

Пример 2. Рассмотрим $\mathbb{R}[x]$ (множество многочленов с вещественными коэффициентами).

Примеры его идеалов:

- $\mathbb{R}[x]$
- $\{0\}$
- $I = \{f \in \mathbb{R}[x] \mid f(0) = 0\} = x\,\mathbb{R}[x]$ (свободный коэффициент нулевой, а значит можно поделить на x, что и записано в последнем равенстве).
- $I = P(x)\,\mathbb{R}[x]$, где $P(x) \in \mathbb{R}[x]$
- Первые три пункта тоже подходят под последний. На самом деле (факт без доказательства) все идеалы имеют такой вид.

Пример 3. Рассмотрим $\mathbb{Z}[x]$ (множество многочленов с целыми коэффициентами):

- $P(x)\mathbb{Z}[x]$, где $P(x) \in \mathbb{Z}[x]$
- Но не все идеалы имеют такой вид, например: $(x-3)\mathbb{Z}[x] + 2\mathbb{Z}[x]$.
- **Упражнение:** понять почему последнее действительно идеал.

Лемма. Если $f\colon A \to B$ — гомоморфизм колец, то

$\operatorname{Im} f$ — подкольцо B.

$\operatorname{Ker} f$ — двусторонний идеал A.

Доказательство. Оставлено в качестве упражнения. □

***Определение* 3.23.** R — кольцо, $X \subseteq R$. Идеалом (левым, правым, двусторонним), порождённым подмножеством X называется наименьший по включению идеал (левый, правый, двусторонний), содержащий X.

Упражнение: пересечение всех идеалов, содержащих данное множество X является идеалом, порождённым множеством X.

Замечание. Для правых идеалов:

$$\bigcap_{\substack{I \supseteq X \\ \text{I}-\text{идеал R}}} I = \sum_{x \in X} xR$$

3.4. Фактор-кольцо

Лемма. Подкольцо, порождённое множеством X, то есть наименьшее подкольцо, содержащее это множество, состоит из всех сумм из элементов $\pm x_1 x_2 x_3 \dots x_n$, где $x_i \in X$

Доказательство. Оставлено в качестве упражнения. □

***Определение* 3.24.**

- (X) — идеал, порождённый множеством X, в зависимости от ситуации левый, правый или двусторонний.
- (a) — идеал, порождённый элементом a, где $a \in R$, в зависимости от ситуации левый, правый или двусторонний.
- Идеал, порождённый одним элементом называется *Главным идеалом.*

Замечание. Для левых идеалов $(a) = Ra$.

Доказательство. Оставлено в качестве упражнения. □

Пример.

- $X = \{15, 20\}$, найти (X).
- (X) — идеал в $\mathbb{Z}$, а все идеалы в $\mathbb{Z}$ имеют вид $n\mathbb{Z}$, найти n.
- $(X) = \{15x + 20y \mid x, y \in \mathbb{Z}\} \subseteq 5\mathbb{Z}$
- Включение в другую сторону можно показать, получив gcd из 15 и 20.
- $n = \gcd(15, 20)$.
- **Упражнение:** доказать в произвольном случае.

Любой идеал I по определению является подгруппой аддитивной подгруппы кольца и задаёт разбиение кольца на смежные классы или классы вычетов по модулю I, о чём пойдёт речь дальше.

***Определение* 3.25.** a и b сравнимы по модулю I ($a \equiv b \mod I$), если $a - b = a + (-b) \in I$,

Где $a, b \in R$, I — идеал R (левый, правый, или двусторонний).

Лемма. Если I — двусторонний идеал, $a \equiv a' \pmod I$, $b \equiv b' \pmod I$, то

1. $a + b \equiv a + b' \equiv a' + b' \pmod I$.
2. $ab \equiv ab' \equiv a'b' \pmod I$

Доказательство.

1. Оставлено в качестве упражнения.
2. $ab - ab' = a(b - b') \in I$. (так как $b - b' \in I$, и I — идеал) □

Пример. $m, l \in \mathbb{Z}$

$m \equiv l \pmod{n\mathbb{Z}} \iff m - l \in n\mathbb{Z} \iff m - l \vdots n \iff m \equiv l \pmod n$.

***Определение* 3.26.** Пусть I — двусторонний идеал R.

- Фактор-кольцом по I называется множество смежных классов в сравнимости по модулю.
- Зададим сложение: R/I: $(r_1 + I) + (r_2 + I) = r_1 + r_2 + I$.
- Зададим умножение: R/I: $(r_1 + I)(r_2 + I) = r_1 r_2 + I$.
- Проверим дистрибутивность слева: $(r_1 + I)(r_2 + I + r_3 + I) = r_1 r_2 + I + r_1 r_3$.
- **Упражнение:** Проверить дистрибутивность справа.
- **Упражнение:** Доказать корректность (независимость результата сложения и умножения от выбора представителя).

Пример 1. $\mathbb{Z}/_{n\mathbb{Z}}$ теперь является не только фактор-группой, но и фактор-кольцом.

Пример 2. $K[x]/_{(f(x))}$, подробнее о нём поговорим позже.

K — поле, $f \in K[x]$.

Теорема 3.3. Пусть $f, g \in K[x]$, $g \neq 0$. Тогда $\exists!\, q, r \in K[x]$: $f = gq + r$, где $\deg r < \deg g$.

Доказательство.

Существование, индукция по степени f

- Если $\deg f < \deg g$, то $r = f, q = 0$.
- $f(x) = a_0 + a_1 x + \dots a_n x^n$, $g(x) = b_0 + b_1 x + \dots b_m x^m$, $a_n \neq 0, b_m \neq 0$.
  $f_1(x) := f(x) - g(x)\frac{a_n}{b_m} x^{n-m}$, здесь мы неявно пользуемся тем, что в поле можно делить.
  $\deg f_1 < n \overset{\text{по индукции}}{\Longrightarrow} \exists q_1, r_1 \colon f_1 = q_1 g + r_1$
  $f = g\frac{a_n}{b_m} x^{n-m} + f_1 = g\frac{a_n}{b_m} x^{n-m} + g q_1 + r_1 = g(\frac{a_n}{b_m} x^{n-m} + q_1) + r_1$

Покажем единственность

- Пусть есть разные разложения.
- $f = q_1 g + r_1 = q_2 g + r_2$, где $q_1, q_2, r_1, r_2 \in K[x]$, $\deg r_1, \deg r_2 < \deg g$.
- $(q_1 - q_2)g = r_2 - r_1$, степень слева строго больше степени справа.
- Противоречие. □

Утверждение 3.4. Пусть R — область целостности.

$\forall f, g \in R[x],\ g \neq 0,\ g = b_k x^k + b_{k-1} x^{k-1} + \dots + b_0,\ b_k \in R^* \cup \{0\}$.

(см определение 3.8)

Тогда $\exists q, r \in R[x] \colon f = gq + r$, такие что $\deg r < \deg g$.

Замечание. Обратите внимание, что достаточно обратимости только элемента b_k, так как мы всегда делим именно на него.

Доказательство. Аналогично предыдущему доказательству. □

Теорема 3.5 (Теорема о гомоморфизме)**.** Пусть f — гомоморфизм колец. Тогда

$A/_{\operatorname{Ker} f} \simeq \operatorname{Im} f$.

Доказательство. Из теоремы о гомоморфизме групп у нас есть: $\phi \colon A/_{\operatorname{Ker} f} \to \operatorname{Im} f$

Нужно показать гомоморфизм умножения: $\phi(ab) = \phi(a)\,\phi(b)$.

Что оставляется как упражнение читателю. □

***Определение* 3.27.** Пусть R_1, R_2 — кольца.

Определим $R_1 \oplus R_2 = \{(r_1, r_2)\}$, кольцо.

Зададим сложение: $(a,\ b) + (c,\ d) = (a + b,\ c + d)$

Зададим умножение: $(a,\ b) * (c,\ d) = (ab, cd)$.

Замечание. Аналогично вводится прямая сумма для большего числа слагаемых.

Замечание. Иногда преподаватели алгебры применяют обозначение $\times$ вместо $\oplus$ (смотрите далее).

Замечание. В данной конструкции много делителей нуля.

Действительно, любой элемент вида $(r,\ 0)$ или $(0,\ r)$ (в случае двух колец) является делителем нуля.

3.5. Разложение группы в прямую сумму, абелевы группы

Замечание. Warning. Данная секции восстановлена частично по памяти, здравому смыслу и википедии.

Принимаются замечание и предложения.

Замечание. Вероятно эта часть логически должна существовать в другом месте, но тут уже претензии не ко мне :)

***Определение* 3.28.** Группа G раскладывается в прямую сумму подгрупп $H_1, H_2, \ldots, H_k$, если:

- H_i — нормальная подгруппа в G (для всех i)
- $H_i \cap \langle H_1, \ldots H_{i-1}, H_{i+1}, \ldots H_k \rangle = \{e\}$
- $G = \langle H_1, \ldots, H_k \rangle$ (иначе говоря, G порождается подгруппами H_i)

***Определение* 3.29.** Запись $G = H + F$ означает, что G раскладывается в прямую сумму подгрупп H, F.

(Запись, разумеется, обобщается и на произвольное число подгрупп).

Замечание. В прямой сумме может быть только конечное число слагаемых

Теорема 3.6. Если $G = \sum H_i$, то:

- $h_i h_j = h_j h_i$ (для всех $h_i \in H_i$, $h_j \in H_j$, при $i \neq j$)
- Для каждого $g \in G$ существует единственное разложение $g = \sum h_i$, где $h_i \in H_i$,

Доказательство. **TODO: Его нет** □

TODO: help

- Пусть $H, F \leqslant G$.
- $H \cap F = \{e\}$ – инъективность.
- $hf = fh \quad \forall f \in F, \forall h \in H$ — гомоморфизм.
- $G = HF$ — сюръективность.

Утверждение 3.7. Пусть $H_1, \ldots, H_n \leqslant G$.

1. $\phi : H_1 n \times \ldots \times H_n \to G$, — изоморфизм.
2. (a) $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_n) = \{e\} \ \forall i$
   (b) $h_i h_j = h_j h_i \forall\, h_i \in H_i, h_j \inf H_j$
   (c) $G = H_1 \ldots H_n$

Утверждение 3.8. Пусть G — конечная абелева группа, а p — простое число.

Пусть порядок каждого элемента в G есть p в какой-то степени.

Тогда порядок группы G тоже p в некоторой степени.

Доказательство. Если $H \leqslant G$, то:

1. В H порядок каждого элемента есть p в некоторой степени.
2. В $G/_H$ порядок каждого элемента тоже p в некоторой степени.

Доказательство пункта 2:

Рассмотрим $x \in G/_H$, $x = g + H$ для некоторого g, пусть $\operatorname{ord} g = p^t$

$p^t x = p^t(g + H) = p^t g + H = 0 + H = \bar{0}$, значит $p^n \vdots \operatorname{ord} x$.

Рассмотрим $x \in G$, $x \neq 0$.

$H := \langle x \rangle$, тогда $|H| = p^n, n > 0$ (для некоторого n, не $1 = p^0$, т.к. войдёт элемент x и 0)

$|G/_H| < |G| \implies |G/_H| = p^l$, видимо пользуемся индукцией.

$|G| = |G/_H||H| = p^{l+n}$ □

3.6. Поле многочленов

Как мы обсуждали выше, $K[x]$ является полем, если полем является K. При чём в этом поле все идеалы имеют вид $f(x)K[x]$, обозначим этот идеал как $I = f(x)K[x] = (f(x))$. (напомним, что запись в скобках означает идеал, порождённый элементом, см 3.24).

Также мы обсуждали, что многочлены можно делить с остатком:

Для любого $g(x)$ существуют единственные $q(x), r(x)$, такие что $g(x) = q(x)f(x) + r(x)$ и $\deg r < \deg f$

Замечание. $g(x) \equiv r(x) \pmod I$, просто по определению mod (см 3.25).

Замечание. Тем самым все многочлены, имеющие одинаковый остаток при делении на какой-то многочлен $f(x)$ сравнимы друг с другом по модулю.

Лемма. Если $r_1, r_2, f \in K[x]$, $r_1 \equiv r_2 \mod (f(x)K[x])$ и $\deg r_1, \deg r_2 < \deg f$, то $r_1 = r_2$

Доказательство.

$r_1 \equiv r_2 \pmod{f(x)K[x]} \implies r_1 - r_2 = fh$ для некоторой функции h.

- Если $h(x) = 0$, то $r_1 = r_2$.
- Но если $h(x) \neq 0$, то $\deg(fh) \geqslant \deg(f)$, но $\deg(r_1 - r_2) < \deg(f)$. Противоречие. □

Замечание. Неформально можно думать о факторе $K[x]/_{f(x)K[x]}$ как о многочленнах со степенью меньшей f. $K[x]/I \simeq \{r \in K[x] \mid \deg r < \deg f\}$.

Лемма. Пусть R — область целостности (как частный случай — поле), $f, g \in R[x]$, $\alpha \in R$

1. Если $f(\alpha) = 0$, то $f(x) = (x - \alpha)q(x)$, где $q(x) \in R[x]$, $\deg q = deg f - 1$.
2. Если $n = \deg f$, то f имеет не более n различных корней в R.
3. Если $\deg f = \deg g = n$ и $f(\alpha_1) = g(\alpha_1), \ldots, f(\alpha_{n+1}) = g(\alpha_{n+1})$. где $\alpha_i \in R$ и различны. Тогда многочлены равны (т.е. попарно равны все коэффициенты).

Доказательство.

1. Поделим f на $x - \alpha$ с остатком:

   $f(x) = (x - \alpha)q(x) + r$, $\deg r < deg(x - \alpha) = 1 \implies \deg r = 0 \implies r$ – константа.

   $f(x) = (x - \alpha)q(x) + C$.

   $f(\alpha) = 0 + C \implies C = 0$ (так как α — корень).

2. Индукция по n:

   База ($n = 1$). $f(x) = ax + b$ ($a \neq 0$) корней явно не более, чем один. Если a необратим, то вообще ноль.

   Переход. Пусть f имеет корни (иначе $0 \leqslant n$) и α — один из них.

   $f(x) = (x - \alpha)\, q(x)$, $\deg q = n - 1$

   q имеет не более чем $n - 1$ корень. Конец.

3. $h(x) = f(x) - g(x)$, $\deg h \leqslant n$, $h(\alpha_i) = 0$ для $n + 1$ альф.

   Но многочлен не может иметь более n корней, следовательно он нулевой. □

Замечание. Можно считать, что $\deg 0 = \infty$, тогда все равенства остаются верными и для этого случая.

Упражнение: Лемма выше верна только в области целостности, предлагается построить примеры колец (вне областей целостности), для которых это не будет верно.

3.7. Идеалы и их свойства. Китайская теорема об остатках

Здесь и далее в главе R означает коммутативное кольцо, а I, J – его идеалы.

Лемма. $I \cap J$ идеал.

Доказательство. Оставлено в качестве упражнения. Совет: воспользуйтесь определением идеала (3.22). □

***Определение* 3.30.** Определим $I + J = \{a + b \mid a \in I, b \in J\}$ как все возможные суммы.

Замечание. $I + J$ является идеалом, так как:

- $I + J$ несомненно образует подгруппу аддитивной группы кольца.
- **TODO: дописать вторую часть**

Замечание. $I + J$ наименьший идеал содержащий и I и J.

Иначе говоря, $I + J = (I \cup J)$, то есть идеал порождённый объединением.

***Определение* 3.31.** Произведение идеалов $IJ = (\{ab \mid a \in I, b \in J\})$ — это идеал порождёный всеми попарными произведениями.

Замечание. $IJ \neq \{ab \mid a \in I, b \in J\}$, так как полученное множество идеалом не является.

Замечание. На самом деле $IJ = \{\sum a_i b_j \mid a_i \in I, b_j \in J\}$ (все конечные суммы такого вида).

Мы знаем, что идеал, порождённый множеством — это пересечение всех идеалов, являющихся надмножеством данного.

Множество выше является идеалом (проверьте по определению) и надмножеством $\{ab \mid a \in I, b \in J\}$

Значит искомый идеал является подмножеством данного, но с другой стороны можно показать, что искомый идеал должен содержать все суммы, написанные выше.

$IJ = \{\sum a_i b_j \mid a_i \in I, b_j \in J\}$. $(ra)b$, $ra \in I$.

***Определение* 3.32.** Идеалы I, J называются взаимно простыми, если $I + J = R$.

Замечание. Рассмотрим $R = \mathbb{Z}$, идеалы $n\mathbb{Z}$ и $m\mathbb{Z}$ взаимно просты $\iff \exists x, y \in \mathbb{Z}\colon nx + my = 1$.

Доказательство. $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$.

$d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z} \supseteq n\mathbb{Z}, m\mathbb{Z}$. Следовательно $m \vdots d, n \vdots d$.

Взаимно просты $\iff d = 1$. "$\to$" $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$. $\{nx + my \mid x, y \in \mathbb{Z}\}$

"$\leftarrow$" Содержит единицу, а значит всё кольцо. □

Здесь и далее все кольца имеют единицу.

Лемма. Если I, J взаимно просты, то $IJ = I \cap J$

Доказательство.

- $IJ \subseteq I \cap J$.

  $\forall r \in IJ\colon r = \sum\limits_{i=1}^{N} a_i b_i$, где $a_i b_i \in I \cap J$ но это значит, что и их сумма лежит в пересечении.

- $IJ \supseteq I \cap J$.

  I и J — взаимно просты $\implies I + J = R \ni 1$.

  $\implies \exists a \in I, b \in J$ такие что $a + b = 1$ (см 3.30)

  $\forall x \in I \cap J\colon x = x * 1 = x * (a + b) = xa + xb$.

  $xa \in (I \cap J)I$, $xb \in (I \cap J)J$.

  $xa + xb \in IJ$. □

Замечание. Обратите внимание, что $IJ \subseteq I \cap J$ для всех идеалов I, J, так как в первой части леммы не пользуемся тем, что I, J — взаимно простые.

Теорема 3.9. Пусть R — коммутативное ассоциативное кольцо с 1, а I, J — взаимно простые идеалы.

Тогда $R/IJ \cong R/I \oplus R/J$

Замечание. В частном случае мы уже знаем это утверждение, если $(n, m) = 1$, то:

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$.

Доказательство. $f\colon R \to R/I \oplus R/J$.

Сопоставим объекту два его класса по модулям I, J: $f(r) := (r \mod I, r \mod J)$, где $r \mod I = r + I$.

Каждая проекция является гомоморфизмом, значит f тоже гомоморфизм.

Так как I и J взаимно просты $(I + J = R)$, то $1 = a + b$ для некоторых $a \in I$, $b \in J$.

Вычислим $f(a)$. $f(a) = (a + I, a + J) = (0 + I, a + b - b + B) = (0 + I, 1 + J)$, (пользуемся тем, что $a \in I$, $b \in J$)

Аналогично $f(b) = (1 + I, 0 + J)$.

Рассмотрим произвольный x, y: $f(xa + yb) = f(x)f(a) + f(y)f(b) = (x \mod I)(0, 1) + (y \mod I)(1, 0) = (x + I, y + J)$.

Тем самым можно получить любой элемент в области значений и f — сюръекция.

Заметим, что $\operatorname{Ker} f = \{r \in R \mid r \in I, r \in J\} = I \cap J = IJ$

По теореме о гомоморфизме колец (см 3.5) получаем требуемое. □

Лемма. Пусть R — ассоциативное коммутативное кольцо с 1.

Если идеал I взаимно прост с каждым из идеалов $J_1, \ldots, J_k$, то I взаимно прост с их произведением $J_1 J_2 \ldots J_k$

Доказательство. $R = I + J_1 = I + J_1 R = I + J_1(I + J_2) = I + J_1 I + J_1 J_2 \subset I + J_1 J_2$

И, видимо, так как $I + J_1 J_2 \subset R$ как идеал кольца, то в последнем переходе можно поставить равенство.

И так далее до любого конечного k:

$R = I + J_1 J_2 = I + J_1 J_2 R = I + J_1 J_2 (I + J_3) = \ldots = I + J_1 J_2 J_3$

Здесь мы пользуемся определением идеала (3.22), суммы идеалов (3.30), определением взаимной простоты (3.32). □

Теорема 3.10 (Китайская Теорема об Остатках)**.** Пусть $I_1, I_2, \ldots, I_n$ — попарно взаимнопростые идеалы в R.

Тогда $R/_{I_1 I_2 \ldots I_n} \cong R/_{I_1} \oplus R/_{I_2} \oplus \ldots \oplus R/_{I_n}$

Доказательство. Доказательство теоремы несложно получить из индукции, предыдущей леммы и теоремы 3.9. □

Замечание. Если R — кольцо целых чисел, то теорему можно сформулировать следующим образом:

Пусть $m_1, m_2, \ldots, m_k$ — попарно взаимнопростые целые числа, $n := m_1 m_2 \ldots m_k$.

Тогда $\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}/_{m_1\mathbb{Z}} \oplus \ldots \oplus \mathbb{Z}/_{m_k\mathbb{Z}}$

Теорема 3.11 (Решение систем сравнений в целых числах)**.**

Для любого набора остатков $r_1 \ldots r_k$ $\exists x \in \mathbb{Z}$, такой что:

$$\begin{cases} x \equiv r_1 \mod m_1 \\ x \equiv r_2 \mod m_2 \\ \ldots \\ x \equiv r_k \mod m_k \end{cases} \qquad (m_i, m_j) = 1 \text{ для } i \neq j.$$

Причём если x и y являются решениями этой системы, то $x \equiv y \pmod n$.

Доказательство.

Определим $n := m_1 m_2 \ldots m_k$, $n_i := n/m_i$.

Так как m_i и n_i взаимнопросты, то $\exists x_i, y_i \in \mathbb{Z}$: $m_i x_i + n_i y_i = r_i$

С практической точки зрения их можно найти, например, с помощью алгоритма Евклида.

Заметим, что

- $n_i y_i \equiv r_i \pmod{m_i}$
- $n_i y_i \equiv 0 \pmod{m_j}$ для $j \neq i$

Первое следует из $m_i x_i + n_i y_i = r_i$, второе из $n_i = n/m_i = m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k$.

Определим $x := \sum_{i=1}^{k} n_i y_i$.

Тогда $\forall i$: $x \equiv n_i y_i \equiv r_i \pmod{m_i}$.

Вторая часть доказательства проще:

Пусть x — решение системы.

- Если y — решение, то $y - x \vdots m_i$ (для всех i), значит $y - x \vdots n$.
- Если y таков, что $y - x \vdots n$, то $y = x + nt$, подставляем в систему, nt сокращается. □

3.8. Простые и максимальные идеалы, делимость

***Определение* 3.33.** Элемент b делит элемент a (записывается как $b \mid a$), если $a = bc$ для некоторого $c \in R$.

Утверждение 3.12.

1. $b \mid a \iff a \in bR \iff aR \subseteq bR$
2. $b \in R^* \iff bR = R$

Доказательство.

1. $b \mid a \iff a = bc \iff a \in bR \iff aR \subseteq bRR \iff aR \subseteq bR$
2. Следует из первого пункта:
   $b \in R^* \iff \exists c\colon bc = 1 \iff b \mid 1 \iff bR \subseteq R \iff bR = R$ □

***Определение* 3.34.** Пусть I — идеал, тогда I простой, если $\forall a, b \in R\colon ab \in I \implies a \in I \vee b \in I$.

***Определение* 3.35.** I — максимальный, если для любого идеала J: $I \subsetneq J \subset R \implies J = R$.

***Определение* 3.36.** Идеал, не совпадающий со всем кольцом называется собственным.

Замечание. В целых числах походу совпадает.

Лемма. Пусть I — идеал R, тогда $\exists J$ — идеал, $I \subseteq J \subseteq R$ и J максимальный.

Доказательство. Рассмотрим множество $X = \{K \mid K$ — идеал в$R, K \supseteq I, K \neq R\}$, введём на нём частичный порядок включения ($\subseteq$).

Покажем, что любое линейно упорядоченное подмножество X имеет верхнюю грань.

Пусть $\{L_i\}$ — произвольное линейно упорядоченное подмножество, $L := \bigcup L_i$.

Рассмотрим произвольные $a, b \in L$, тогда $a \in L_i, b \in L_j$ (для некоторых i, j).

Но множество линейно упорядоченно, значит одно лежит в другом (совпадение тоже допускается), без потери общности давайте считать, что $L_i \subseteq L_j$.

Следовательно $a, b \in L_j \implies a - b \in L_j \subseteq L$.

Также $\forall r \in R\colon ra \in L_j \subseteq L$.

Итого мы получаем по определению (3.22), что L — идеал. Значит любое линейное упорядоченное подмножество X имеет верхнюю грань, значит (по лемме Цорна) в множестве X есть максимальный элемент.

Соответственно этот максимальный элемент и является максимальным идеалом. □

Замечание. R — область целостности $\iff \{0\}$ — простой идеал.

Область целостности $\iff ab = 0 \implies a = 0 \vee b = 0$.

Идеал простой $\iff ab \in \{0\} \implies a \in \{0\} \vee b \in \{0\}$.

Упражнение: (от препода)

1. $f\colon A \to B$, гомоморфизм колец, $I \subseteq B$, I — простой идеал.
   Тогда $f^{-1}(I)$ — простой идеал в A.
2. $f\colon A \to B$, эпиморфизм колец, $I \subseteq B$, I — максимальный.
   Тогда $f^{-1}(I)$ — максимальный.

Утверждение 3.13. Пусть R — коммутативное ассоциативное кольцо с 1, I — идеал в R, тогда:

1. I — простой $\iff$ $R/_I$ — область целостности.
2. I — максимальный $\iff$ $R/_I$ — поле.
3. Если I — максимальный, то I — простой.

Доказательство.

"$\to$". (!) в $R/_I$ нет делителей нуля.
$(a+I)(b+I) = I \implies a \in I \vee b \in I$.
$(a+I)(b+I) = ab + I$
TODO: ....

"$\to$" $\forall r \notin I$ элемент $r+I$ обратим в $R/_I$.
I — максимальный, $r \notin I \implies I \subsetneq I + rR = R$ (равно R, так как I максимальный)
$\implies \exists x$.....
"$\leftarrow$". Пусть $I \subsetneq J \subseteq R$.
$\exists r \in J \setminus I$, $R/_I$ — поле, следовательно $\exists x \in R$: $xr \equiv 1 \mod I$. т.е. $I + rR = R$, и $I + rR \subseteq J$ $implies J = R$. □

Пример. $\mathbb{Q}[x,y]$ — многочлены от двух переменных. $\mathbb{Q}[x][y] = \{\sum a_{i,j}x^i y^j\}$
$I = (x,y) = x\mathbb{Q}[x,y] + y\mathbb{Q}[x,y]$, обратите внимание, что это не главный идеал.
$J = (x) = x\mathbb{Q}[x,y]$.
$Q[x,y]/_{x\mathbb{Q}[x,y]} \equiv \mathbb{Q}[y]$ — область целостности.
Не поле.
J — простой идеал, но не максимальный.

Далее R область целостности

Утверждение 3.14. Пусть R — кольцо главных идеалов, I — простой идеал, $I \neq \{0\}$.
Тогда I — максимальный.

Доказательство. $I = pR$, пусть $I \subsetneq J \subseteq R$, J — идеал.
R — КГИ $\implies J = qR$ $pR \subseteq qR \subseteq R$
$p = qr$, pR — простой $\implies (q \in pR \implies pR = qR) \vee (r \in pR \implies r = ps)$.
$p = qr = qspp(1-qs) = 0 \implies q \in R^* \iff qR = R$.
TODO: Дописать, там юзались КГИ и элемент делящий другой □

§Факториальные кольца.
Пусть R — область целостности.

***Определение* 3.37.** $a, b \in R$, a и b ассоциированные, если $aR = bR$.

(или, эквивалентно, $aR \subseteq bR$, $bR \subseteq aR \iff a|b, b|a$).

Пример 1. В $\mathbb{Z}$ n и m ассоциированы, если $n = m$ или $n = -m$.

Пример 2. В $K[x]$ (где K — поле) f и g ассоциированы, если $f(x) = cg(x)$, $c \in K[x] \setminus \{0\}$.

Пусть $a \sim b$, если a ассоциирован с b.

***Определение* 3.38.** Пусть $a \in R \setminus R^*$. Элемент a неприводим, если $a = bc \implies a \sim b \vee a \sim c$.

Замечание. Ассоциированость является отношением эквивалентности.

Лемма. Пусть $a, b \in R \setminus \{0\}$, тогда:

1. $a \sim b \iff a = b\varepsilon$, где $\varepsilon \in R^*$.
2. a — неприводим $\iff (a = cd \implies c \in R^* \vee d \in R^*)$.

Доказательство.

1. - “$\implies$”

     $a \sim b \iff \begin{cases} b|a \implies a = b\varepsilon \implies a = a\delta\varepsilon \implies a(1 - \delta\varepsilon) = 0 \implies \delta\varepsilon = 1 \implies \varepsilon \in R^* \\ a|b \implies b = a\delta \end{cases}$

     Пользуемся тем, что мы в области целостности, а также тем, что $a \neq 0$.
   - “$\impliedby$”

     a и b ассоциированные $\iff a \mid b, b \mid a$.

     $a = b\varepsilon$, $b = a\varepsilon^{-1}$ (пользуемся коммутативностью, обратимостью ε).

     После этого делимость очевидна по определению (см 3.33)
2. $a = bc \implies (a \sim b \vee a \sim c)$

   Пусть б.п.о. $a \sim b \implies a = b\varepsilon, \varepsilon \in R^* \implies b\varepsilon = bc \implies b(\varepsilon - c) = 0 \implies c = \varepsilon$. $a = bc$

□

3.9. Неприводимые элементы. Факториальные кольца

***Определение* 3.39.** R — область целостности. R — факториально, если любой элемент единственным образом раскладывается в произведение неприводимых.

Единственность вплоть до порядка и ассоциированости:

Если $\varepsilon p_1 p_2 \dots p_n \sim \Theta q_1 q_2 \dots q_m$ (где p_i, q_j неприводимы, $\varepsilon, \Theta \in R^*$), то $n = m$ и $\exists \sigma \in S_n \colon p_i \sim q_{\sigma(i)}$

Теорема 3.15. Если R — кольцо главных идеалов, то R факториально.

Доказательство состоит из нескольких лемм:

Лемма (1)**.** R — кольцо главных идеалов, $a, c \in R, c$ — неприводим, $\neg c|a \implies aR + cR = R$

Доказательство. R — кольцо главных идеалов $\implies aR + cR = bR \implies c \in bR \implies c = bd$.

Так как c неприводим, то $c \sim b$ или $b \in R^*$.

Но $c \sim b \iff cR = bR$, но тогда $a \in bR = cR$, т.е. $c|a$, но это ложь.

$b \in R^* \iff bR = R$, что мы и хотели. □

Лемма (2)**.** R — кольцо главных идеалов, $a, b, c \in R$, c неприводим.

Тогда $(c|ab \implies c|a \vee c|b)$

Иначе говоря, cR простой: $ab \in cR \implies a \in cR \vee b \in cR$

TODO: В обе стороны

Доказательство. $c|ab$, пусть $\neg c|a$ и $\neg c|b$.

Тогда по предыдущей лемме $cR + aR = R$ и $cr + bR = R$, из чего по какой-то лемме из китайской теоремы об остатках следует, что cR взаимно прост с $(aR)(bR) = abR$.

Итого: $cR + abR = R$ и $ab \in cR$.

Но $cR + abR = cR$ (так как $c|ab$), следовательно $cR = c$, что возможно $\iff$ обратим.

Но c неприводим, противоречие. □

***Определение* 3.40.** Кольцо R называется нётеровым, если для любой последовательности идеалов I_n в R, такой что $I_1 \leqslant I_2 \leqslant I_3 \leqslant \ldots$, все идеалы начиная с некоторого места совпадают.

Лемма (3)**.** Если R — кольцо главных идеалов, то R нётерево.

Доказательство. Так как R — кольцо главных идеалов, то каждый идеал $I_k = r_k R$ для некоторого r_k.

Докажем, что $I := \bigcup\limits_{i=1}^{\infty} I_i$ идеал:

- $a, b \in I \implies a, b \in I_i \implies a - b \in I_i \implies a - b \in I$
- $a \in I \implies a \in I_i \implies \forall r \colon ra \in I_i \implies \forall r \colon ra \in I$

(Первое условие гарантирует, что I — является подгруппой аддитивной группы кольца, хотя это немного не очевидно сходу. Hint: a может быть равно 0).

Следовательно $I = qR$, для некоторого $q \in R$ (так как мы в кольце главных идеалов).

Значит $q \in I$, а значит $\exists n$, такое что $q \in I_n$.

Но из $q \in I_n$ следует, что $I \subseteq I_n$, но по определению $I_n \subseteq I$, значит $I = I_n$.

Аналогично $I_k = I$ для любого $k \geqslant n$ (т.к. $I_n \subseteq I \implies q \in I_k$, после чего применим доказательство выше). □

Лемма (4)**.** Пусть R — кольцо главных идеалов. Тогда любой ненулевой необратимый элемент раскладывается в произведение неприводимых.

Доказательство. $r \in R \setminus R^*, r \neq 0$.

rR содержится в некотором максимальном идеале M.

$M = p_1 R, rR \subseteq p_1 R \iff r = p_1 r_1, r_1 \in R$

$p_1 R$ — max $\implies$ $p_1 R$ — простой $\implies (ab \vdots p_1 \implies a \vdots p_1 \vee b \vdots p_1$

$p_1 = ab \implies a \sim p_1 \vee b \sim p_1$

И из всего этого следует, что p_1 неприводим, т.е.

$r = p_1 r_1$, p_1 неприводим.

Если $r_1 \in R^*$, то $r = p_1 r_1$ — искомое разложение. Хз.

Если $r_1 \notin R^*$, то $r_1 R \neq R$, поэтому $r_1 R \subseteq p_2 R$ — максимальный. $r = p_1 p_2 r_2$.

И так далее можно продолжать раскладывать.

Либо $r_k \in R^*$, тогда успех.

$$r_1 = p_2 r_2, r_1 R \subseteq r_2 R \quad (1)$$
$$r_2 = p_3 r_3, r_2 R \subseteq r_3 R \quad (2)$$

$\Longrightarrow$ $r_1 R \subsetneq r_2 R \subsetneq r_3 R \ldots$, далее всё хорошо по лемме 3. □

Лемма. Если:
- R — область целостности.
- $\forall$ неприводимого элемента его идеал прост.
- $\forall$ ненулевого необратимого элемента есть разложение в произведение

То R — факториально.

Доказательство. Достаточно доказать единственность разложения, воспользуемся индукцией по $\min(n, m)$

TODO: дописать

$\min(n, m) = 0$, пусть $n = 0$, тогда он обратим. Тогда и другой обратим. Значит они ассоциированы.

Переход: $n > 0 p_n$ — неприводим $\Longrightarrow$ $p_n R$ — прост.

$q_1 q_2 \ldots q_m \in p_1$??????????? $\exists l \colon 1 \leqslant l \leqslant m, q_l \in p_n R, q_l \vdots p_n$.

a) q_l — неприводим, $q_l = p_n \delta, \delta \in R^*$ $\Longrightarrow$ $q_l \sim p_n$.

b) Также $\varepsilon p_1 \ldots p_n \sim \Theta q_1 \ldots q_m$

(a), (b) $\Longrightarrow$ $\varepsilon p_1 \ldots p_{n-1} \sim \Theta q_1 \ldots q_{l-1} q_{l+1} \ldots q_m$.

По предположению индукции $n - 1 = m - 1$ $\Longrightarrow$ $n = m$

$\exists$ биекция $t \colon \{1, \ldots, n-1\} \to \{1, \ldots l-1, l+1, \ldots m\}$, $p_i \sim q_{t(i)}$.

$$\sigma \in S_n \colon \sigma(i) = \begin{cases} t(i) & i \leqslant n-1 \\ l & i = n \end{cases}$$ □

Замечание. Из всего вышесказанного следует теорема о факториальности кольца главных идеалов.

3.10. Евклидовы кольца

***Определение* 3.41.** Пусть R — область целостности, назовём R евклидовым, если $\exists \nu \colon R \setminus \{0\} \to \mathbb{N} \sqcup \{0\}$:

$\forall a, b \in R \setminus \{0\}$:

1) $\nu(ab) \geqslant \nu(a)$

2) $\exists q, r \in R \colon a = bq + r$ и $r = 0 \vee \nu(r) < \nu(b)$

Функция ν называется евклидовой нормой.

Пример 1. $\mathbb{Z}$, $\nu(x) = |x|$.

Пример 2. K — поле, рассмотрим $K[x]$: $\nu(f) = \deg f$.

Пример 3. $\mathbb{Z}[i] := \mathbb{Z}[x]/_{(x^2+1)}, \nu(a + bx) = a^2 + b^2$

Утверждение 3.16. Евклидовы кольца $\subset$ кольца главных идеалов $\subset$ факториальные $\subset$ области целостности.

Доказательство. Покажем, что R — евклидово кольцо, то R — кольцо главных идеалов.

Рассмотрим произвольный нетривиальный идеал I в R (если $I = \{0\}$, то $I = 0R$)

Рассмотрим элемент $b \in I$ с минимальной нормой: $\nu(b) = \min\limits_{r \in I} \nu(r)$, покажем, что $bR = I$.

Пусть $a \in I$, тогда $\exists q, r \colon a = bq + r$, при чём $r = 0 \vee \nu(r) < \nu(b)$.

Но $r = a - bq \in I$, так как $a \in I, bq \in I$.

Так как b имеет минимальную норму, то $r = 0$ или $\nu(r) \geqslant \nu(b)$, следовательно $r = 0$, $a = bq$.

Так как выбрать a можно произвольно, получаем, что идеал I главный ($I = bR$) □

***Определение* 3.42.** $d = \gcd(a, b)$, если $d|a$, $d|b$, и из $c|a$, $c|b$, следует $c|d$.

Замечание 1. gcd определён с точностью до ассоциированности.

Замечание 1.5. Заметим, что идеал, порождённый a и b — это в точности gcd: $(a, b) = aR + bR$.

Замечание 2. R — кольцо главных идеалов, $aR + bR = dR$, $d = \gcd(a, b)$.

3.11. 211116, unsorted

P.s. R — область целостность.

***Определение* 3.43.** $a, b \in R$, $d = \gcd(a, b)$, если $d \mid a$, $d \mid b$ и $\forall c \colon c \mid a, c \mid b \implies c \mid d$.

Замечание. 1. $d = gcd(a, b) \iff dR$ — наименьший главный идеал, содержащий и a и b. $(aR + bR)$.

2. gcd Определён с точностью до ассоциативности.

Теорема 3.17. Пусть R — кольцо главных идеалов.

$a, b \in R$, тогда $\exists x, y \in R \colon ax + by = gcd(a, b)$.

Доказательство. R — кольцо главных идеалов $\implies aR + bR = dR$ и $d = gcd(a, b0$,

$d \mid a \iff aR \subseteq dR$

$d \in aR + bR = \{ax + by \mid x, y \in R\}$. □

***Определение* 3.44.** a, b — взаимно простые, если у них нет необратимых общих делителей.

Утверждение 3.18. R — кольцо главных идеалов, $a, b \in R$. Тогда a,b — взаимно простые $\iff$ aR, bR — взаимно простые.

Доказательство. a, b — взаимно простые $\iff 1 = gcd(a, b) \iff 1 = ax + by \iff R = aR + bR \iff aR$, bR — взаимно простые. □

***Определение* 3.45.** $a, b \in R, l = \operatorname{lcm}(a, b)$, если $a \mid l$, $b \mid l$, и если $a \mid c, b \mid c \implies l \mid c$.

Замечание. $l = \operatorname{lcm}(a, b) \iff lR$ — наибольший главный идеал, содержащийся в $aR \cap bR$.

Замечание. $a|b \iff bR \subseteq aR$.

Теорема 3.19. a, b — кольцо главных идеалов, $a, b \in R \setminus \{0\}$, тогда $\operatorname{lcm}(a, b) = ab/gcd(a, b)$.

При этом последнее равенство верно с точностью до ассоциированности.

Доказательство. $d = \gcd(a, b)$.

$a = a'd$, $b = b'd$, $a', b' \in R$.

$d = ax + by \implies 1 = a'x + b'y$, более формально:

$d(1 - a'x - b'y) = 0$, но $d \neq 0$ а R — область целостности, следовательно $1 - a'x - b'y = 0$.

(side note) $\operatorname{lcm}(a, b)R = aR \cap bR$.

(side note) $ab/d = a'b'd$.

$c \in aR \cap bR$

$c = c * 1 = ca'x + cb'y \in a'b'dR$.

$c \in bR, ca' \in ba'R = a'b'dR$.

$\operatorname{lcm}(a, b)R = aR \cap bR \subseteq a'b'dR = \frac{ab}{d}R$

"$\supseteq$",

$$a'b'd = ab' \in aR \tag{3}$$
$$a'b'd = ba' \in bR \tag{4}$$

$a'b'd \in aR \cap bR \implies a'b'dR \subseteq aR \cap bR$. □

§,

Далее мы требуем Евклидовости кольца.

Лемма. $\forall a, b, c \in R\colon \gcd(a, b) = \gcd(a - bc, b)$.

$\gcd(a, b)R =^{?} \gcd(a - bc, b)R$.

Доказательство.

$\gcd(a, b)R = aR + bR$, $\gcd(a - bc, b)R = (a - bc)R + bR$.

"$\supseteq$" $a - bc \in aR + bR, b \in aR + bR$.

"$\subseteq$" $b \in bR \subseteq (a - bc)R + bR$, $a = (a - bc) + bc \in (a - bc)R + bR$. □

Лемма. $\gcd(a, 0) = a$

Замечание. $\gcd(a, b)R = aR + bR = (a,\ b)$, где последнее означает идеал, порождённый a и b.

Поэтому часто наибольший общий делитель обозначают через $(a,\ b)$.

Алгоритм:

TODO: Вёрстка

$a, b \in R, \nu$ — евклидова норма.

$a = bq_0 + r_0$ $b = r_0q_1 + r_1$

$\dots$

$r_i = r_{i+1}q_{i+2} + 0$

Утверждается, что $r_{i+1} = (a, b)$.

$r_0 = 0 \vee \nu(r_0) < \nu(b)$, $(a, b) = (a - bq_0,\ b) = (r_0,\ b) = (b,\ r_0)$

$r_1 = 0 \vee \nu(r_1) < \nu(r_0)$, $(b,\ r_0) = (r_0,\ r_1)$

§

Лемма. $|\{x \in \mathbb{Z}/_{m\mathbb{Z}} \mid ax = b\}| = \begin{cases} 0 & \neg d \mid b \\ |d| & d \mid b \end{cases}$

Если $d \mid b$, то $\{x \in \mathbb{Z}/_{m\mathbb{Z}} \mid ax = b\} = \{x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}\}$.

Доказательство. 1. Пусть $\neg d \mid b$.

Если x_0 — решение, $ax_0 - b = mk$, где $k \in \mathbb{Z}$.

$d \mid a, d \mid m$, $b = ax_0 - mk \implies d \mid b$

$a = da'$, $m = dm'$.

2. ** Что-то уехавшее далеко и надолго **

3. а) Если x_0 — решение, то $x_0 + k\frac{m}{d}$

б) Пусть x_1 — решение, т.е. $ax_1 \equiv b \pmod m$, $ax_0 \equiv b \pmod m \implies a(x_1 - x_0) \equiv 0 \pmod m$

$\frac{a}{d}(x_1 - x_0) \equiv 0 \pmod{\frac{m}{d}}$ □

Замечание. $\gcd(a, b) = d = ax + my \implies 1 = \frac{a}{d}x + \frac{m}{d}y \iff \frac{a}{d}, \frac{m}{d}$ — взаимно простые.

$\frac{a}{d}(x_1 - x_0) \vdots \frac{m}{d}$

$x_1 - x_0 \equiv 0 \pmod{\frac{m}{d}}$

$x_1 = x_0 + l\frac{m}{d}$.

§Диофантовы уравнения в целых числах (?)

Лемма. $d = \gcd(a, b)$

Тогда если $\neg d \mid c$, то "$ax + by = c$" неразрешимо в $\mathbb{Z}$

А если $d \mid c$, то "$ax + by = c$" разрешимо и все решения имеют вид:

$x = x_0 + \frac{b}{d}k, y = y_0 - \frac{a}{d}k$, $k \in \mathbb{Z}$.

Доказательство. 1) Если $x_0, y_0 \in \mathbb{Z}$, $ax_0 + by_0 = c$, то $d \mid a$, $d \mid b$, $d \mid (ax_0 + by_0)$, т.е $d \mid c$.

2) Если $d \mid c$, то $c = dc'$

$d = \gcd(a, b) \implies ax + by = d$, $x, y \in \mathbb{Z}$.

$axc' + byc' = dc' = c \implies x_0 = xc', y_0 = yc'$.

3) Если $ax_1 + by_1 = c$, $ax_0 + by_0 = c \implies a(x_1 - x_0) + b(y_1 - y_0) = 0$.

$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0)$.

$d = (a, b) \implies \frac{a}{d}, \frac{b}{d}$ — взаимно простые.

$x_1 - x_0 \vdots \frac{b}{d} \implies x_1 - x_0 = k\frac{b}{d}, y_1 - y_0 = -k\frac{a}{d}$, где $k \in \mathbb{Z}$. □

4. Кольцо целых чисел, теория чисел

4.1. Введение в теорию чисел, Эйлер, Ферма

***Определение* 4.1.** Функция эйлера — это $\varphi(n) :=$ порядок группы $(\mathbb{Z}/_{n\mathbb{Z}})^*$

Замечание. Напоминание, "$*$" означает обратимую часть моноида, в данном случае.

Лемма. Класс элемента m обратим в $(\mathbb{Z}/_{n\mathbb{Z}})^* \iff \gcd(m,n) = 1$.

Доказательство. Нужно решить $mx = 1 \pmod n$

Это тоже самое, что решать $mx + tn = 1$, найти m, t.

Расширенный алгоритм Евклида вам в помощь. □

Следствие. $\varphi(n) =$ количество чисел от 1 до $n-1$ взаимнопростые с n

Лемма. Пусть R — кольцо с 1, $R = \bigoplus\limits_{i=1}^{n} R_i$.

Тогда $R^* \cong \times_{i=1}^{n} R_i^*$

Доказательство. **TODO: Закончить доказательство**

У нас уже есть $R \cong \bigoplus_{i=1}^{n} R_i$ и соответсвующий изоморфизм ψ.

Давайте покажем, что если $r \in R^*$, то ему соответствует сумма обратимых элементов.

Пусть $\psi(r) = a_1 + \ldots + a_n$, а также $\psi(r^{-1}) = b_1 + \ldots + b_n$.

Рассмотрим $\psi(1) = \psi(rr^{-1}) = (a_1 + \ldots + a_n)(b_1 + \ldots + b_n)$.

□

Теорема 4.1.

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. Если $\prod\limits_i p_i^{k_i}$, то $\varphi(n) = \prod\limits_i p_i^{k_i-1}(p_i - 1) = n \prod\limits_i \frac{p_i - 1}{p_i}$

Доказательство.

1. По китайской теореме об остатков $\mathbb{Z}/_{ab\mathbb{Z}} \cong \mathbb{Z}/_{a\mathbb{Z}} \oplus \mathbb{Z}/_{b\mathbb{Z}}$.
   Применим лемму, $(\mathbb{Z}/_{ab\mathbb{Z}})^* \cong (\mathbb{Z}/_{a\mathbb{Z}})^* \times (\mathbb{Z}/_{b\mathbb{Z}})^*$
   $\varphi(ab) = |(\mathbb{Z}/_{a\mathbb{Z}})^* \times (\mathbb{Z}/_{b\mathbb{Z}})^*| = \varphi(a)\varphi(b)$
2. $\varphi(a) = p^k - \frac{p^k}{p} = p^{k-1}(p-1)$
   Среди всех чисел от 0 до $p^k - 1$ подойдут все, кроме $\vdots\, p$. Доказательство? Попробуйте обратить элемент через расширенный алгоритм Евклида.
3. Следует из индукции, и первых двух пунктов. □

Теорема 4.2 (Эйлера)**.** Если $\gcd(a,\, n) = 1$, то $a^{\varphi(n)} = 1 \pmod n$

Замечание (Формулировка в теории групп). Если $\gcd(a,\, n) = 1$, то $\bar{a}^{\varphi(n)} = 1$ в $(\mathbb{Z}/_{n\mathbb{Z}})^*$, где $\bar{a}$ — класс числа a.

Доказательство. Рассмотрим $x \in (\mathbb{Z}/_{n\mathbb{Z}})^*$, по теореме лагранжа порядок элемента x делит порядок группы.

Иначе говоря, $x^s = 1$, где $s = |(\mathbb{Z}/_{n\mathbb{Z}})^*|$, но $s = \varphi(n)$ по определению. □

Следствие (Малая теорема Ферма). Если p — простое, и $\gcd(a,\, p) = 1$, то $a^{p-1} \equiv 1 \pmod p$

Теорема 4.3 (Вильсона)**.** Если p — простое, то $(p-1)! \equiv -1 \pmod p$.

Доказательство. Рассмотрим поле $Z/_{p\mathbb{Z}}$ (так как p — простое, то всё обратимо, см леммы выше).

$f(x) := x^{p-1} - 1$, $g(x) := (x-1)(x-2)\dots(x-(p-1))$.

Заметим, что $f(x) = g(x) = 0$ для всех $x \neq 0$, $x \in \mathbb{Z}/_{p\mathbb{Z}}$.

Рассмотрим $h(x) := f(x) - g(x)$, моном x^{p-1} сократится, значит в разности получится многочлен степени $\leqslant p-2$.

Но у него есть $p-1$ корень — 1, 2, …, $p-1$, по вот по этой лемме

$h(x) = 0$ — нулевой многочлен. Значит $f(x) = g(x)$ (как многочлены).

Значит $-1 = f(0) = g(0) = (p-1)! * (-1)^{p-1} = (p-1)!$ □

4.2. Экспонента группы

***Определение* 4.2.** Пусть G — группа. Экспонентой G называется минимальное $d \in \mathbb{N}$, такое что $g^d = e$ (для всех $g \in G$).

Упражнение: Если G конечна, то экспонента делит $|G|$ (**TODO: почему?**).

4.3. 281116, вторая пара, unsorted

Как написано выше $|(\mathbb{Z}/_{p^k\mathbb{Z}})^*| = \phi(p^k) = p^{k-1}(p-1)$

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

1. $\operatorname{ord}(p+1) = p^{k-1}$
2. Пусть $\langle d \rangle = (\mathbb{Z}/_{p\mathbb{Z}})*$
   Тогда $\operatorname{ord} d^{p^{k-1}} = p-1$
3. $(p+1)d^{p^{k-1}}$ — первообразный корень по модулю p^k, т.е:
   $(\mathbb{Z}/_{p^k\mathbb{Z}})$ — циклическая.

Доказательство.
1) (по лемме **TODO: ?**) $n = p, m = k$.

$(p+1)^{p^{k-1}} \equiv 1 + p^k \pmod{p^{k+1}}$
$(p+1)^{p^{k-1}} \equiv 1 \pmod{p^k} \implies \operatorname{ord}(p+1) \mid p^{k-1}$
Если $\operatorname{ord}(p+1) < p^{k-1}$, то $\operatorname{ord}(p+1) \mid p^{k-2}$.

Но по лемме $(n = p,\ m = k-1)$ $(p+1)^{p^{k-2}} \equiv 1 + p^{k-1} \pmod{p^k}$

2) $d^{p^{k-1}(p-1)} = 1$ (в $\mathbb{Z}/_{p\mathbb{Z}}$).

$(d,\ p) = 1, d \in (Z/_{p\mathbb{Z}})^*$, предыдущее верно по теореме эйлера(**TODO: ?**)

$\Longrightarrow \operatorname{ord} d^{p^{k-1}} \mid p-1$

$(d^{p^{k-1}})^l = q \iff d^{p^{k-1}l} \equiv 1 \pmod{p^k} \implies d^{p^{k-1}l} \equiv 1 \pmod{p}$

$\Longrightarrow p^{k-1}l \vdots (p-1) \iff l \vdots (p-1) \implies \operatorname{ord}(d^{p^{k-1}}) = p-1$

3) $\operatorname{ord}((p+1)d^{p^{k-1}}) =$ (по лемме) $= (p-1)p^{k-1} = |(\mathbb{Z}/_{p^k\mathbb{Z}})^*|$ □

Обсудим частный случай $p = 2$.

$|(\mathbb{Z}/_{2^k\mathbb{Z}})^*| = \phi(2^k) = 2^{k-1}$.

Если $k = 1$, то $(\mathbb{Z}/_{2\mathbb{Z}})^* = \{1\}$

Если $k = 2$, то $(\mathbb{Z}/_{4\mathbb{Z}})^* \simeq C_2$ (просто по тому, что любая группа такого порядка циклическая).

Лемма. В группе $(\mathbb{Z}/_{p^k\mathbb{Z}})^*$, при $k \geqslant 2$:

1. $m \in \mathbb{N} \setminus \{1\} \implies 5^{2^{m-2}} - 1 \equiv 2^m \pmod{2^{m+1}}$
2. В $(\mathbb{Z}/_{2^k\mathbb{Z}})*$:
   (a) $\operatorname{ord}(-1) = 2, \operatorname{ord}(5) = 2^{k-2}$
   (b) $\langle -1\rangle \cap \langle 5\rangle = \{1\}$
3. $(\mathbb{Z}/_{2^k\mathbb{Z}})^* \simeq C_2 \times C_{2^{k-1}}$.

Доказательство. Оставлено в качестве сами-знаете-чего. □

Теорема 4.4. Пусть $n \in \mathbb{N}$, $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$, где p_i — различны.

Причём если $n \vdots 2$, то $p_1 = 2$.

Тогда:

$$(\mathbb{Z}/_{n\mathbb{Z}})^* \simeq \begin{cases} C_{p_1^{k_1-1}(p_1-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)} & n \not\vdots 2 \vee n \vdots 4, n \not\vdots 8 \\ C_{p_2^{k_2-1}(p_2-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)} & n \vdots 2, n \not\vdots 4 \\ C_2 \times C_{2^{k_1-2}} \times C_{p_2^{k_2-1}(p_2-1)} \times \ldots \times C_{p_l^{k_l-1}(p_l-1)} & n \vdots 8 \end{cases}$$

Доказательство. **TODO: Не указано...** □

Теорема 4.5. $(\mathbb{Z}/_{n\mathbb{Z}})^*$ циклическая $\iff$ выполнено одно из:

- $n = p^k$, p — простое, $p \neq 2$
- $n = 2p^k$, p — **TODO: простое ли** , $k \in \mathbb{N} \sqcap \{0\}$.
- $n = 4$

TODO: ..

$(a,\ n) = 1$. $a^{\phi(n)=1} \equiv 1 \pmod{n}$

***Определение* 4.3.** Функция Карлмайка $\lambda\colon \mathbb{N} \to \mathbb{N}$.

λ — экспонента группы $(Z/_{n\mathbb{Z}})^*$

$\lambda(n) \mid \phi(n)$, Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$

Теорема 4.6.

1. Если $n \not\vdots 8$, то $\lambda(n) = \operatorname{lcm}\limits_{1 \leqslant i \leqslant l}(p_i^{k_i-1}(p_i-1))$
2. Если $n = 2^k m$, где $k \geqslant 3$, а $m \not\vdots 2$, то $\lambda(n) = \operatorname{lcm}(\operatorname{lcm}\limits_{1 \leqslant i \leqslant l}(p_i^{k_i-1}(p_i-1)), 2^{k-2})$
3. Если $\gcd(a,\, n) = 1$, то $a^{\lambda(n)} \equiv 1 \pmod{n}$.

Доказательство. Его, предположительно, нет. □

4.3.1. Тест ферма на простоту

n — простое $\implies a^{n-1} \equiv 1 \pmod{n}$ $((a,\, n) = 1,\, 1 < a < n)$.

$T \subseteq \mathbb{Z}/_{n\mathbb{Z}} \setminus \{0\}$ — множество тех a, для которых тест пройден.

1) Если n — простое, то $T = (\mathbb{Z}/_{n\mathbb{Z}})$

2) $|T|/\phi(n)$ —?

Тест Ферма $T = \{a \mid a^{n-1} \equiv 1 \pmod{n}\}$

***Определение* 4.4.** Составные числа n, такие что $|T_n| = \phi(n)$ называются псевдо-простыми для данного теста.

***Определение* 4.5.** Числа Карлмайкла — псевдопростые числа для теста ферма.

Наименьшее число Карлмайкла — это 561.

Тест Эйлера:

Незачем тестировать чётные числа с ними и так всё ясно. Давайте тестировать только нечётные.

$T = \{a \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\}$

Увы тоже есть псевдопростые. Пример: 1729

$\sup \frac{T}{\phi(n)} \leqslant \frac{1}{k}$

Если составное, то вероятность детектирования через 10 запусков: $1 - \frac{1}{k^10}$

4.4. Шифрование

4.4.1. Предисловие

$P \to fC \to f^{-1}P$.

Где P, C — последовательности из символов какого-то алфавита (пусть $Z/_{n\mathbb{Z}}$)

Пример очень простого шифрования:
- $x \mapsto fx + b$
- $y \mapsto f^{-1}y - b$.

Где b — это секретный ключ.

Вообще так себе шифрование, потому что:

- Можно просто перебрать b (не так уж и много комбинаций).
- Частотный анализ (некоторые буквы встречаются чаще чем другие, тем самым можно перебирать только очень малое число гипотез).

Вторая попытка:

- $x \mapsto fax + b$, где a обратим (что верно $\iff \gcd(a, n) = 1$).
- $y \mapsto f^{-1}a^{-1}(y - b)$, где a^{-1} можно найти как $a^{\phi(N)-1}$ или алгоритм Евклида $1 = xN + ay$, $\gcd(N, y) = 1$.

Если знаем куда переходят две буквы (скажем из того же частотного анализа), то тоже конец шифру:

$$\begin{cases} ax_1 + b = y_1 \\ ax_2 + b = y_2 \end{cases},$$

решаем и получаем ответ.

Идея: давайте найдём такую функцию f, что её несложно вычислить, но сложно найти обратную не зная какого-то "секрета".

4.4.2. RSA

Два человека (скажем Алиса и Боб) хотят безопасно обмениваться информацией.

Рассмотрим следующий алгоритм (RSA):

- Алиса выбирает большое простое число p, а Боб выбирает большое простое число $q \neq p$ (как это сделать см в предыдущих сериях),
- Определим $N = pq$, заметим, что $\phi(N) = (p-1)(q-1) = N-p-q+1$, что легко вычисляется Алисой и Бобом, знающими p, q и сложно вычисляемо остальными.
- Алиса и Боб выбирает некое e: $1 \leqslant e \leqslant \phi(N)$, $\gcd(e, \phi(N)) = 1$.
- Определим функцию шифрования: $f(x) := x^e$
- Находим $d \in \mathbb{Z}$, такое что $de \equiv q \pmod{\phi(N)}$.
- Определим $f^{-1}(y) = y^d$. Тогда $f^{-1} \circ f = x^{de} = x^{1+k\phi(N)} = x$, так как $x^{\phi(N)} = 1$.
- Итог: любой, знающий N, e может шифровать, но только знающие p, q могут быстро сделать дешифровку.

4.5. Сравнения по модулю

$f(x) \equiv 0 \pmod{N} \iff f(x) \equiv 0 \pmod{p_i^{k_i}}$, где $n = p_1^{k_1} * \ldots * p_t^{k_t}$.

$ax^2 + bx + c \equiv 0 \pmod{p}$

$x^2 + a^{-1}bx + a^{-1}c \equiv 0$

Если $p \neq 2$, то уравнение выше эквивалентно:

$\left(x + \frac{a^{-1}b}{2}\right)^2 \equiv a^{-1}c + ?\frac{q^{-2}b^2}{4} \pmod{p}$.

Вопрос по поводу $p = 2$ замнём.

***Определение* 4.6.** Пусть $(a, m) = 1$. a — квадратный вычет по модулю m, если сравнение $x^2 \equiv a \pmod{m}$ — разрешимо.

Замечание. Аналогично вводится понятие квадратного невычета.

***Определение* 4.7.** Пусть p — простое число $\geqslant 3$.

$F_p := \mathbb{Z}/_{p\mathbb{Z}}$.

Замечание. Как впоследствии будет показано, любое поле порядка p (p простое, $\geqslant 3$) изоморфно $\mathbb{Z}/_{p\mathbb{Z}}$.

***Определение* 4.8.** $(F_p^*)^2 := \{x^2 \mid x \in F_p^*\}$

Лемма. $0\ (F_p^*)^2 \leqslant F_p^*$

1 $|F_p^* : (F_p^*)^2| = 2$

2 $\forall x \in F_p^*$: $x^{(p-1)/2} = \pm 1$.

3 Если $x \in F_p^*$, то $x \in (F_p^*)^2 \iff x^{(p-1)/2} = 1$.

Доказательство. Пункт 0 остаётся в качестве упражнения на определения.

Пусть $f\colon F_p^* \to F_p^*$, где $x \mapsto x^2$.

$\operatorname{Ker} f = \{x \in F_p^* \mid x^2 = 1\} = \{\pm 1\}$, это например следует из того, что многочлен в поле не может иметь больше корней, чем его степень.

$(F_p^*)^2 = \operatorname{Im} f \simeq F_p^*/_{\operatorname{Ker} f}$

$|F_p^*| = p - 1$, $|\operatorname{Ker} f| = 2$, следовательно $|(F_p^*)^2| = (p-1)/2$, пункт (1) доказан.

2. $x^{p-1} = 1$ в $F_p^* \implies x^{(p-1)/2} \in \operatorname{Ker} f = \{\pm 1\}$, что верно $\forall x \in F_p^*$ **TODO: ...**

3. “$\implies$”. $x = y^2$, значит $x^{(p-1)/2} = y^{p-1} = 1$.

“$\impliedby$”. **TODO: ...** , соображения касательно порядков. □

***Определение* 4.9.** Пусть p — простое $\geqslant 3$, $a \in \mathbb{N}$, $\gcd(a, p) = 1$.

Символ Лежандра это $\left(\frac{a}{p}\right) = \begin{cases} 1 & a \in (F_p^*)^2 \\ -1 & \text{иначе} \end{cases}$

Замечание. Так как мы определили символ Лежандра только для простых $p \geqslant 3$, то везде далее подразумевается это ограничение на p

Утверждение 4.7.

1. $\left(\frac{a}{b}\right) =\equiv a^{(p-1)/2} \pmod p$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. Если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

Доказательство. Пока что замяли. □

Теорема 4.8. Пусть p, q — простые, $\geqslant 3$.

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

Доказательство. Видимо замяли. □

***Определение* 4.10.** $n = p_1 \dots p_m$, где p_i — простые $\geqslant 3$, $\gcd(a, n) = 1$.

Тогда $\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_m}\right)$ — символ Якоби.

Теорема 4.9. $n \not\vdots 2 \implies \left(\frac{1}{n}\right) = -1, \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}, \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$

Теорема 4.10. $\gcd(a, n) = 1$, a, n — нечётные. $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{n-1}{2}\frac{a-1}{2}}$.

5. Поле комлексных чисел

5.1. Определения

5.1.1. Простое определение

Обычно под комплексными числами понимают множество $\mathbb{R}\times\mathbb{R}$ с операциями, определённым следующим образом:

- $(x,\, y) + (z,\, w) := (x + y,\, z + w)$
- $(x,\, y) * (z,\, w) := (x * z - y * w,\, x * w + y * z)$

Проверить дистрибутивность умножения остаётся как упражнение.

$i := (0, 1)$.

Можно записывать $(x,\, 0)$ как просто x, тем самым часто можно встретить запись вида $10-3i$, под этим понимается число $(10,\, -3)$.

Замечание 1. $i^2 = -1$ (это не определение, это следует из $i = (0, 1)$)

На самом деле из этого соотношения (и дистрибутивности) и выводится та формула умножения:

$(x + iy)(z + iw) = xz + xiw + iyz + i^2yw = xz - yw + i(xw + yz)$.

Замечание 2. Элемент 1 (или $(1,\, 0)$) является нейтральным по умножению.

Замечание 3. Деление комплексных чисел выводится из умножения:

$\frac{x+yi}{z+wi} = \frac{(x+yi)(z-wi)}{(z+wi)(z-wi)} = \frac{xz+yw+i(yz-xw)}{z^2+w^2}$

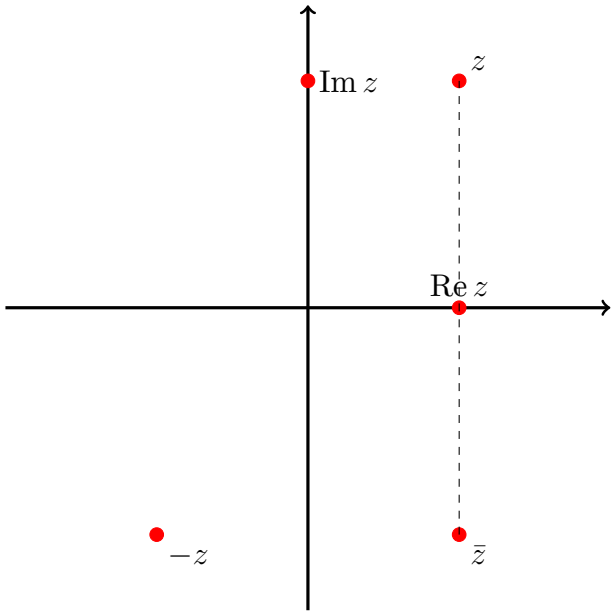
В практическом смысле лучше запоминать не формулу, а то, откуда она получается (домножение на сопряжённое).

5.1.2. Связанные определения и свойства

***Определение* 5.1.** Пусть $z = x + iy$, тогда:

- $\operatorname{Re} z := x$ — действительная часть z.
- $\operatorname{Im} z := x$ — мнимая часть z.
- $\bar{z} := x - iy$ — сопряжённое число к z.

Если интерпретировать комплексные числа как точки на плоскости (с некоторым операциями), то введённые определения можно проиллюстрировать картинкой: (действительная часть числа по оси Ox, мнимая по оси Oy):



Простейшие свойства:

- $z \in \mathbb{R} \iff z = \bar{z}$
- $z\bar{z}$, $z + \bar{z} \in \mathbb{R}$
- $\operatorname{Re} z = (z + \bar{z})/2$
- $\operatorname{Im} z = (z - \bar{z})/(2i)$
- $f(z) = \bar{z}$ — автоморфизм $\mathbb{C}$.

Первые 4 свойства следуют непосредственно из определений и должны быть очевидны.

По поводу последнего надо сказать следующее: i является решением уравнения $x^2 = -1$, но на самом деле решений у этого уравнения два: i, $-i$. Но откуда вы знаете какое же из них взять как i? Соответсвенно выбор противоположного решения и задаёт соответствующий автоморфизм.

Более формально это можно показать доказав отдельно гомоморфизм и биективность.

5.1.3. Определение через многочлены

В предыдущем параграфе мы определили комплексные числа как пары действительных чисел, сейчас же давайте скажем, что комплексные числа это многочлен степени не больше единицы, т.е. $ax + b$.

Давайте скажем, что b это действительная часть, а a — мнимая. Со сложением нет проблемы, но при умножении получится многочлен степени большей или равной двум:

$(ax + b)(cx + d) = acx^2 + \ldots$, поэтому было бы неплохо, если $x^2 = -1$, тогда мы получим в точности формулы выше, хотя и в многочленной форме.

Но давайте добавим это соотношение, иначе говоря, $\mathbb{C} := \mathbb{R}[x]/_{(x^2+1)}$. В каждом классе есть ровно один многочлен степени $\leqslant 1$, остальные же ему эквивалентны.

Можно проверить, что полученное поле изоморфно полю, которое было определено выше.

TODO: Доделать комплексные числа

5.1.4. Тригонометрическая запись

Несколько форм записи комплексного числа.

- $a + bi$ — “обычная”.

- $r(\cos(\phi) + i\sin(\phi))$ — "тригонометрическая".

Заметим, что $z \cdot w = |z| \cdot |w| \cdot (\cos(\arg z + \arg w) + i\sin(\arg z + \arg w))$.

Замечание. Если зафиксировать $w \in \mathbb{C}$, то можно рассмотреть функцию $f\colon \mathbb{C} \to \mathbb{C}$:

$f(z) := zw$.

Если интерпретировать $\mathbb{C}$ как плоскость, то мы только что получили некоторую гомотетию, то есть отображение, сохраняющее подобие.

Несложно увидеть, что данное отображение можно интерпретировать как растяжение и поворот относительно 0, из чего следует утверждение выше.

Лемма (формула Муавра)**.** $z^n = |z|^n(\cos(n\arg z) + i\sin(n\arg z))$, для $n \in \mathbb{N}$.

***Определение* 5.2.** $re^{i\phi} := r(\cos(\phi) + i\sin(\phi))$

Замечание 1. Вообще следует из матанализа, но пока будем принимать это как определение.

Замечание 2. Приятным бонусом является сохранение свойств степенной функции:

Если $z = re^{i\phi}$, $w = te^{i\psi}$, то $zw = rte^{i(\psi+\phi)}$. Просто раскрыть по предыдущему определению.

Также $z^n = (re^{i\phi})^n = r^n e^{in\phi}$. (формула Муавра)

Лемма (1)**.** $C^* \equiv \mathbb{R}^*_{>0} \times \mathbb{R}/_{2\pi\mathbb{Z}}$

Лемма (2)**.** $C^* \equiv \mathbb{R} \times \mathbb{R}/_{2\pi\mathbb{Z}}$

Лемма (3)**.** $C^* \equiv \mathbb{R} \times \mathbb{R}/_{\mathbb{Z}}$

Замечание. $\mathbb{C}^*$ нужно воспринимать как обратимую группу кольца $\mathbb{C}$ относительно умножения, $\mathbb{R}^*_{>0}$ тоже,

$\mathbb{R}$ и $\mathbb{Z}$ подразумеваются относительно операции сложения.

Доказательство. 1. $z \mapsto (|z|, \arg z)$.

Гомоморфность очевидна, инъективность и сюръективность несложно показываются.

2. Чтобы получить вторую лемму пропустим первую компоненту предыдущего произведения через следующий изоморфизм:

   $\ln\colon \mathbb{R}^*_{>0} \to \mathbb{R}$, $\ln(ab) = \ln(a) + \ln(b)$, сюръективность с инъективностью очевидны.

3. Теперь пропустим вторую часть через изоморфизм домножения на константу:

   $f\colon \mathbb{R}/_{2\pi\mathbb{Z}} \to \mathbb{R}/_{\mathbb{Z}}$, $x \mapsto 2\pi x$

□

5.2. Уравнения деления круга

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

Перейдём в экспоненциальную запись: $w = se^{i\psi}$, $s \in \mathbb{R}_{>0}$, $\psi \in \mathbb{R}$.

Аналогично $z = re^{i\phi}$, $z^n = re^{in\phi} = se^{i\psi}$.

Тогда $r^n = s$, или $r = \sqrt[n]{s}$.

А также $n\phi - \psi \vdots 2\pi$, из чего $\phi = \frac{\psi+2\pi k}{n}$, где $k \in \mathbb{Z}$.

Сами корни выглядят как $z_k = \sqrt[n]{s}\exp(i\frac{\psi+2\pi k}{n})$.

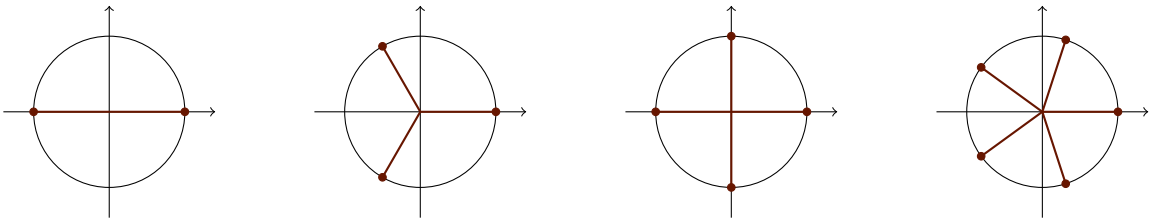
Замечание. Заметим, что $\phi(k)$ повторяются каждые n раз, поэтому достаточно рассмотреть только

$k \in \{0, 1, \ldots, n-1\}$ или любое другое множество, содержащее все остатки по делению на n.

Замечание. Случай $w = 0$ является вырожденным. Отметим, что в общем случае будет ровно n решений, но при $w = 0$ только один 0.

***Определение* 5.3.** Под $\sqrt[n]{w}$ понимается соответствующее *множество* z_i.

(a) $\sqrt[2]{1}$ (b) $\sqrt[3]{1}$ (c) $\sqrt[4]{1}$ (d) $\sqrt[5]{1}$



Аналогично для $w \neq 1$ мы тоже получим круг, но растянутый и/или повёрнутый.

5.3. Кольцо гауссовых целых чисел

Гауссовы целые числа — это множество комплексных чисел, у которых и действительная, и мнимая часть — целые числа.

Гауссовы целые числа обозначаются как $\mathbb{Z}[i]$.

6. “пока неясно”

6.1. Многочлены на полем

Краткое содержание предыдущих серий:

- $K[x]$ — поле многочленов.
- $K[x]$ — евклидово с нормой deg.
- Многочлены можно делить с остатком.
- Остаток от деления многочлена p на $(x-\alpha)$ есть $p(\alpha)$.

***Определение* 6.1.** Для многочлена $f(x) = a_n x^n + \dots a_1 x + a_0$:

$f'(x) = n a_n x^{n-1} + \dots + a_1$

Под $f^{(k)}(x)$ понимается как производная взятая $k \in \mathbb{N} \sqcup \{0\}$ раз, (причём $f^{(0)}(x) := f(x)$).

Замечание. Многочлены и производные мы понимаем как формальное выражение, в частности многочлен это конечная(!) последовательность коэффициентов, записывающаяся особым образом, а производная — это функция из множества многочленов в его же самого.

Лемма. 1. $(p \pm q)' = p' + q'$

2. $(pq)' = p'q + pq'$
3. $(\alpha p)' = \alpha p'$
4. $(p \circ q)' = (p' \circ q)q'$.

Замечание. Нужно отметить, что эти утверждения НЕ следуют из соответствующих утверждений математического анализа, например по тому, что здесь производная определяется другим образом.

Более того, если рассмотреть $K = \mathbb{Z}/_{p\mathbb{Z}}$, то многочлены $x^p - x$ и 0 — это разные многочлены, хотя если рассмотреть их как функции, то они обе тождественно равны 0.

Доказательство. Оставлено в качестве упражнения. □

Лемма (5)**.** $f(x) = \sum\limits_{i=0}^{n} \frac{f^{(i)}(a)}{l!}(x-a)^l$

Доказательство. Оставлено в качестве упражнения. □

Лемма (Лемма Хензеля)**.** Пусть $f \in \mathbb{Z}[x]$, $m, k \in \mathbb{N}$, $m \leqslant k$, p — простое.

Если $f(a) \equiv 0 \pmod{p^k}$ и $f'(a) \not\equiv 0 \pmod{p}$,

То $\exists! s \in \mathbb{Z}$, $f(s) \equiv 0 \pmod{p^{k+m}}$ и $s \equiv a \pmod{p^k}$,

TODO: непонятно что (3 фразы впереди):

$x^l \equiv b \pmod{p^l}$, $a^p \equiv a \pmod{p}$.

$f(x) = x^k - b$, $\neg p \mid h$, $\neg p \mid b$.

$f'(x) = k x^{k-1}$.

Доказательство. **TODO: непонятно**

$n := \deg f$, $f(x) = \sum\limits_{l=0}^{n} \frac{f^{(l)}(a)}{l!}(x-a)^l$.

$s = a + tp^k$

$f(s) = \sum\limits_{l=0}^{n} \frac{f^{(l)}(a)}{l!} t^l p^{kl} \equiv f(a) + f'(a)tp^k \equiv (z \cdot p^k + f'(a)tp^k \equiv p^k(z + f'(a)t) \pmod{p^{k+m}}$

$f'(a)x = -z \pmod{p^m}$ имеет единственное решение t.

$f(s) \equiv p^k(z + f'(a)t) \equiv 0 \pmod{p^{k+m}}$. □

Теорема 6.1. Пусть $t_0, \ldots, t_n \in K$, причём различны.

Пусть $y_0, \ldots y_n \in K$.

Тогда $\exists! p \in K[x]$, такой что $\deg p \leqslant n$, $p(t_i) = y_i$.

Доказательство. **TODO: fix formula**

$p(x) = \sum\limits_{i=0}^{n} y_i \frac{(x-t_j)I!=J}{(x-t_j)I!=J}$

Можно подставить и проверить.

Покажем единственность: пусть f, g подходят, $h(x) := f(x) - g(x)$.

$\forall$: $h(t_i) = 0$, $\deg h \leqslant n$, значит (по теореме о делении многочленов с остатком 3.3) $h = 0$ □

6.2. Кольцо частных

6.2.1. Вводные примеры

Замечание. Здесь и далее “$\rightsquigarrow$” используется для обозначения мономорфизма (?).

Пример 1. Из целых чисел есть мономорфизм в дробные:

$\mathbb{Z} \rightsquigarrow \mathbb{Q}$, $a \mapsto \frac{a}{1}$

Вот так можно, например, определить $\mathbb{Q}$:

$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/_\sim$

$\frac{a}{b} \sim \frac{c}{d} \iff ad = bc$

Пример 2. Расширение предыдущего примера, $R \rightsquigarrow \operatorname{Qout} R$ (мономорфизм в $R \times (R \setminus \{0\})/_\sim$)

Пример 3. $\mathbb{Z} \rightsquigarrow \mathbb{R}$

TODO: wtf?

$R \rightsquigarrow \psi G$, последнее — поле.

Существует поле F: $R \rightsquigarrow \phi F \rightsquigarrow \Theta G$.

6.2.2. Теорема

Теорема 6.2. Пусть R — область целостности (и, видимо, коммутативная).

Тогда существует поле F и мономорфизм $\phi\colon R \to F$, такие что для любого поля G и мономорфизма $\psi\colon R \to G$ $\exists!\Theta\colon F \to G$ гомоморфизм, т.ч. $\psi = \Theta \circ \phi$

TODO: Возможно здесь уместна картинка

Доказательство. $R \times (R \setminus \{0\})$

Определим $\sim$: $(a,\, b) \sim (c,\, d)$ если $ad = bc$, заметим, что оно является отношением эквивалентности: **Упражнение:** . Доказать это, не забудьте, что работаете в коммутативной области целостности.

Рассмотрим $F := R \times (R \setminus \{0\})/_\sim$.

Обозначим за $\frac{a}{b}$ — класс $(a,\, b)$

$\frac{a}{b}\frac{c}{d} := \frac{ac}{bd}$, $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$

Упражнение:

1. Докажите корректность определений операций $*$,$+$ (независимость от выбора элемента в классе эквивалентности)
2. Проверьте, что F — кольцо, причём единице соответствует класс элемента $\frac{1}{1}$, а нулю $\frac{0}{1}$
3. Проверьте, что F — поле, причём $(\frac{a}{b})^{-1} = \frac{b}{a}$
4. Докажите существование мономорфизма $\phi\colon R \to F$, $x \mapsto \frac{x}{1}$ (можно доказать гомоморфность и тривиальность ядра ϕ)

$\Theta(\frac{a}{b}) := \psi(a)\psi(b)^{-1}$

1. Корректность
2. Гомоморфность $+$: $\Theta(\frac{a}{b} + \frac{c}{d}) = \Theta(\frac{a}{b}) + \Theta(\frac{c}{d})$
3. Гомоморфность $*$: $\Theta(\frac{a}{b} * \frac{c}{d}) = \Theta(\frac{a}{b}) * \Theta(\frac{c}{d})$
4. Мономорфизм, ядро отображения является идеалом и либо тривильно либо совпадает со всем F, что соответсвует нулевому гомоморфизму (и неправда для $R \neq \{0\}$, что верно для областей целостности **TODO: факт-чек**).

То ли TODO, то ли упражнение.

$\psi = \Theta \circ \phi$: $\forall a \in R\ \Theta(\phi(a)) = \Theta(\frac{a}{1}) = \psi(a)\psi(1)^{-1} = \psi(a)$ □

***Определение* 6.2.** Построенное поле F называется полем частных кольца R и обозначается $\mathrm{Qout}\, R$ (или $\mathrm{Frac}R$)

Замечание. Докажем единственность F. $R \rightsquigarrow F$, $R \rightsquigarrow F_1$, в силу теоремы есть мономорфизм из F в F_1, и из F_1 в F, поэтому F изоморфно F_1. (рассмотрим композицию отображений, получим ненулевой автоморфизм, значит ядро тривиально)

***Определение* 6.3.** Пусть K — поле, Определеим поле дробно-рациональных функций: $K(x) := \{\frac{f(x)}{g(x)} \mid f, g \in K(x), g \neq 0\}$.

Замечание. $K(x) = \mathrm{Qout}(K[x])$

6.2.3. ?

Пусть R — кольцо главных идеалов.

Утверждение 6.3. $\forall \frac{a}{b} \in \mathrm{Qout}\, R$ можно представить в виде

$\frac{a}{b} = \frac{a_1}{r_1^{k_1}} + \ldots + \frac{a_s}{r_s^{k_s}}$, где r_i неприводимы.

Доказательство. $b = b_1 b_2$, где $(b_1,\, b_2) = 1$

$\frac{a}{b_1 b_2} = \frac{ay}{b_1} + \frac{ax}{b_2}$, $\exists x, y \in R$: $1 = b_1 x + b_2 y$, а значит $a = b_1 a x + b_2 a y$.

Доказательство состоит из индукции по s, при чём первый пункт является как базой (для $s = 2$, $s = 1$ очевидно), так и переходом $s \to s + 1$ □

Пусть R евклидово кольцо с евклидовой нормой ν

***Определение* 6.4.** $\frac{a}{r^k} \in \operatorname{Qout} R$, $\frac{a}{r^k}$ простейшая, если $\nu(a) < \nu(r)$

Утверждение 6.4. $\forall \frac{a}{b} \in \operatorname{Qout} R$ $\frac{a}{b} =$ элемент из R $+ \sum$ простейших

Доказательство. 1. По предыдущему утверждению достаточно рассмотреть только $\frac{a}{r^k}$, где r неприводимый.

2. $a = qr + r_0$, $\nu(r_0) < \nu(r)$ или $r_0 = 0$

   $\frac{a}{r^k} = \frac{q}{r^{k-1}} + \frac{r_0}{r^k}$, где второе слагаемое неприводимо, а первое можно разложить индукцией по k.

□

6.2.4. ?

TODO: ?

$\mathbb{R}(x) = \operatorname{Qout} R[x]$, $Q(x) = cMULT(x - x_i)^{k_i} MULT(x^2 + q_j x + r_j)^{l_j}$

$\frac{P(x)}{Q(x)} = \ldots + \frac{A_i}{(x-x_i)^2} + \ldots + \frac{B_j x + C_j}{(x^2+q_j+r_j)^{b_j}}$

P, Q — многочлены

6.2.5. Заключительные замечания

Если R — область целостности, то можно построить поле $\operatorname{Qout} R$, “насильно” обратив все элементы.

$R \rightsquigarrow \operatorname{Qout} R$

Если есть делители нуля, то так сделать нельзя, но можно в качестве знаменателей взять только некоторое обратимое подмножество $S \subset R$:

$R \rightsquigarrow S^{-1}R$

$a, b \in S \implies ab \in S$, и $0 \notin S$.

На самом деле это достаточные условия на S.