

Алгебра

Саютин Дмитрий

11 декабря 2016 г.

Содержание

1. Введение	1
1.1 Основные обозначения и определения, функции	1
1.2 Бинарные отношения	3
1.3 Порядки и лемма Цорна	5
2. Группы. Введение	7
2.1 Группы и подобное. Определения	7
2.2 Симметрическая группа	9
2.3 Подгруппы	10
2.4 Гомоморфизм групп	12
3. Кольца	13
3.1 Введение	13
3.2 Свойства колец	14
3.3 Гомоморфизм колец	15
3.4 Фактор-кольцо	17
3.5 Поле многочленов	20
3.6 141116	23
3.7 Вторая пара 141116	25
3.8 211116, unsorted	28
4. Кольцо целых чисел, теория чисел	31
4.1 281116, вторая пара, unsorted	31
4.1.1 Тест ферма на простоту	32
4.2 Шифрование	33
4.2.1 Предисловие	33
4.2.2 RSA	33
4.3 Сравнения по модулю	34

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
\emptyset	$\forall x: x \notin \emptyset$	Пустое множество
\sqcup	$A \sqcup B = A \cup B$, при этом $A \cap B = \emptyset$	Дизъюнктивное 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 подчеркнуть 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 $f: X \rightarrow Y$ 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 $\text{Im } f$) 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 $f^{-1}(\hat{y}) = \bigcup_{y \in \hat{y}} f^{-1}(y)$.

Определение 1.8. Пусть $f: X \rightarrow Y$ 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 $f: X \rightarrow Y$, $g: Y \rightarrow Z$, определим композицию функций $g \circ f: X \rightarrow Z$:

$$(g \circ f)(x) := g(f(x))$$

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

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

Определение 1.12. Пусть $f: X \rightarrow Y$. Отображение $g: Y \rightarrow X$ 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 обратное к f слева и справа.

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

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

Определение 1.14. Функция f называется сюръекцией, если [образ функции](#) совпадает с [областью значений](#).

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

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

Теорема 1.1. Пусть $g: X \rightarrow Y$. Следующие условия эквивалентны:

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

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:

$$\text{Сюръективность} \iff \forall y: g^{-1}(y) \neq \emptyset \text{ (см 1.6).}$$

Покажем, что $g'(y) \in g^{-1}(y)$, тем самым последнее не пусто.

$$\text{И действительно } g(g'(y)) = (g \circ g')(y) = id_Y(y) = y. \quad \square$$

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 \leq .

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

Пример 4. График функции тоже является отношением.

Определение 1.17. Бинарное отношение на множестве M называется:

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

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 эквивалентности, классом эквивалентности элемента x называется множество элементов, состоящих с ним в отношении:

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

Лемма.

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

Доказательство.

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

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 $X = \bigcup_{x \in X} \bar{x}$ (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 $x \sim y$, 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 $a, b \in \mathbb{Z}, n \in \mathbb{N}$. $a \sim b := (a - b) \div n$.

Проверим определение отношения эквивалентности:

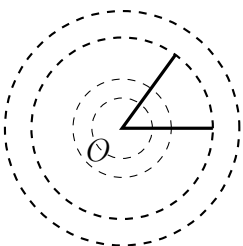
- Рефлексивность: $x - x = 0 \div n$.
- Симметричность: $(x - y) \div n \implies (y - x) \div n$.
- Транзитивность: $(x - y) \div n, (y - z) \div n \implies (x - y) + (y - z) \div n \implies (x - z) \div n$.

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

- $\bar{0} = \{m \in \mathbb{Z} \mid m \div n\}$
- $\bar{1} = \{m \in \mathbb{Z} \mid (m - 1) \div n\}$
- ...

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 \leq , 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 $\forall a, b: a \leq b$ или $b \leq a$.

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

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

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

- $\forall x: x \leq a$.

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 $a \leq b$ и $b \leq a$, то b совпадает с a ($b = a$).

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

Замечание 4. Если определён хотя бы один оператор " $<$ ", " \leq ", " $>$ ", " \geq ", 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 \leq .

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

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

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 верхней гранью, если:

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

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 $*$: $X \times X \rightarrow X$.

Бинарная операция $*$ может обладать некоторыми свойствами:

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

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. $\forall x, y: x^{-1}$ лежит в множестве (так как у него есть обратный элемент $-x$), и $x * y$ лежит в множестве (см пункт 3). \square

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

Операцию также можно обозначить через $+$, тогда $\underbrace{x + x + \dots + x}_{n \text{ раз}} = nx$, 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 $M(X, G) = \{f: X \rightarrow G\}$ 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 $X = \{1, 2, \dots, n\}$ 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 : $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$, $\sigma(4) = 4$.

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 $X = \{1, 2, \dots, n\}$):

Рассмотрим последовательность $1, \sigma(1), \sigma^2(1) \dots$. 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 инверсий чётно. Аналогично вводится понятие нечётной перестановки.

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

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

Утверждение 2.1. Для любых двух перестановок σ_1, σ_2 :

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

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. $H \neq \emptyset$ - 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 . $x \in H \Rightarrow xx^{-1} \in H = e_H \in H \Rightarrow e_H x^{-1} \in H$

$$\begin{cases} x, y \in H \\ y^{-1} \in H \end{cases} \Rightarrow x(y^{-1})^{-1} = xy \in H \quad \square$$

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

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

Замечание. Еще есть централизатор и нормализатор подмножества. Их определения очень похожи на определения центра и централизатора группы.

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

Замечание. Обозначение: $\langle X \rangle$

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 $x_1 \cdot x_2 \cdot \dots \cdot x_n$, где каждый из элементов $x_i \in X \cup X^{-1}$

$\subset: X$ - наименьшая подгруппа $\Rightarrow H \geq \langle X \rangle$

$\supset: x_1 \dots x_n \in \langle X \rangle \Rightarrow H \leq \langle X \rangle$

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

Замечание. $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$

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

Замечание. Если все степени g^i , то $\langle g \rangle$ бесконечна.

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

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

Доказательство. $\langle g \rangle = \{g^0, g^1, g^2, \dots, g^{n-1}\}$

Важно заметить, что $g^n = e$

$g^{mn+k} = (g^n)^m \cdot g^k = e g^k = g^k$, где $k \in \{0, \dots, n-1\}$, так как k - это остаток. \square

2.4. Гомоморфизм групп

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

1. Функция $f : G \rightarrow H$ - 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 изоморфно H обозначается следующим образом: $G \cong H$

Определение 2.12. Ядро гомоморфизма : $Ker f = \{g \in G \mid f(g) = e_H\}$

Определение 2.13. Образ гомоморфизма : $Im f = f(G) = \{g \in G \mid f(g)\}$

Лемма. $f : G \rightarrow H$ - 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 $f^{-1}(h) = g \cdot Ker f$
4. Гомоморфизм f - инъективный (мономорфизм) $\iff Ker f = \{e_G\}$
5. $Ker f \leq G$

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. $gKer f = \{gx \mid x \in Ker f\} = f^{-1}(h)$
 \subset : $y \in gKer f \Rightarrow y = gx, x \in Ker f \Rightarrow f(y) = f(g)f(x) = he_x = h \Rightarrow y \in f^{-1}(h)$
 \supset : Пусть $y \in f^{-1}(h) \Rightarrow y = g(g^{-1}y) \in gKer f$
 $g^{-1}y \in Ker f$
 $f(g^{-1}y) = f(g^{-1})f(y) = (f(g))^{-1}f(y) = h^{-1}h = e_H \Rightarrow g^{-1}y \in Ker f$
4. f - инъективный гомоморфизм $\iff Ker f = \{e_G\}$ следует из 3 пункта, так как можно предъявить биекцию
5. а). $x \in Ker f \Rightarrow x^{-1} \in Ker f$
 $f(x) = e_H$
Знаем второе свойство, делаем так: $f(x^{-1}) = (f(x))^{-1} = e_H^{-1} = e_H \Rightarrow x^{-1} \in Ker f$
б). $x, y \in Ker f \Rightarrow xy \in Ker f$
 $f(x) = f(y) = e_H \Rightarrow f(xy) = f(x)f(y) = e_H e_H = e_H$

□

3. Кольца

3.1. Введение

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

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

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 .

$$R[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in R, n \in \mathbb{N}_0\}$$

Пример 3. $R[[x]] = \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in R\}$ — 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 $X \rightarrow R$.

$$\begin{aligned} (f + g)(x) &= f(x) + g(x) \\ (f \cdot g)(x) &= f(x) \cdot g(x) \end{aligned}$$

Определение 3.9. Функция из $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ 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 $\mathbb{R}^2 \rightarrow \mathbb{R}^2$.

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

Упражнение: кольцо ли?

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

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

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 $\forall r \in R: r = 1 * r = 0 * r = 0 \implies R = \{0\} \implies |R| = 1$. □

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 $\exists s \in R \setminus \{0\}: rs = 0$.

Определение 3.13. Пусть R — коммутативное кольцо.

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

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

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

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

“ \Rightarrow ”: Оставлено в качестве упражнения.

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

Доказательство. Утеряно в веках. □

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

3.3. Гомоморфизм колец

Определение 3.15. $f: A \rightarrow B$ называется гомоморфизмом колец, если:

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

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

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

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

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

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 $f: A \rightarrow B$ 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 $\forall a \in A: f(a) = f(1 * a) = f(1) f(a) = 0 f(a) = 0 \implies f$ — 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 $f: A \rightarrow B$ — гомоморфизм колец с единицей, то $\forall x \in A^*: f(x^{-1}) = f(x)^{-1}$

Доказательство. Сводится к утверждению из прошлой темы □

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

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

Действительно является гомоморфизмом (следствие дистрибутивности).

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

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

Определение 3.21. Непустое подмножество кольца R называется подкольцом, если

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

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

- Левым идеалом, если $\forall r \in R, \forall s \in I: rs \in I$ (иначе говоря, $RI \subseteq I$)
- Правым идеалом, если $\forall r \in R, \forall s \in I: rs \in I$ (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 $f: A \rightarrow B$ — гомоморфизм колец, то

$\text{Im } f$ — подкольцо B .

$\text{Ker } f$ — 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:

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

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 ($a \equiv b \pmod{I}$), 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. $m, l \in \mathbb{Z}$

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

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: $R/I: (r_1 + I)(r_2 + I) = r_1r_2 + I$.
- Проверим дистрибутивность слева: $(r_1 + I)(r_2 + I + r_3 + I) = r_1r_2 + I + r_1r_3$.
- **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, $f \in K[x]$.

Утверждение 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 $r = f, q = 0$.

- $f(x) = a_0 + a_1x + \dots + a_nx^n$, $g(x) = b_0 + b_1x + \dots + b_mx^m$, $a_n \neq 0, b_m \neq 0$.
- $f_1(x) = f(x) - g(x)\frac{a_n}{b_m}x^{n-m}$, здесь мы неявно пользуемся тем, что в поле можно делить.
- $\deg f_1 < n \xrightarrow{\text{по индукции}} \exists q_1, r_1: f_1 = q_1g + r_1$
- $g = g\frac{a_n}{b_m}x^{n-m} + f_1 = g\frac{a_n}{b_m}x^{n-m}q_1 + r_1 = g\left(\frac{a_n}{b_m}x^{n-m} + q_1\right) + r_1$

Покажем единственность

- Пусть есть разные разложения.
- $f = q_1g + r_1 = q_2g + r_2$, 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.

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

(см определение 3.8, также из последнего следует, что $b_k \neq 0$)

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

Доказательство. Аналогично предыдущему доказательству. (**TODO: Не понятно :(**) □

Теорема 3.5 (Теорема о гомоморфизме). Пусть f — гомоморфизм колец с 1. Тогда

$$A/\text{Ker } f \simeq \text{Im } f.$$

Доказательство. Из теоремы о гомоморфизме групп у нас есть: $\phi: A/\text{Ker } f \rightarrow \text{Im } f$

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: $(a, b) * (c, d) = (ac, bd)$.

Замечание. В данной конструкции много делителей нуля.

TODO: Дальше что-то на тему прямых сумм, но без комментариев.

- $H, F \leq G$
- $\phi: H \times F \rightarrow G, (h, f) \mapsto fh$ — изоморфизм
- $H \cap F = \{e\}$ — инъективность.
- $hf = fh \quad \forall f \in F, \forall h \in H$ — гомоморфизм.
- $G = HF$ — сюръективность.

Утверждение 3.6. Пусть $H_1, \dots, H_n \leq G$.

1. $\phi: H_1 \times \dots \times H_n \rightarrow G$, — изоморфизм.

2. (a) $H_i \cap (H_1 \dots H_{i-1} H_{i+1} \dots H_n) = \{e\} \forall i$
 (b) $h_i h_j = h_j h_i \forall h_i \in H_i, h_j \in H_j$
 (c) $G = H_1 \dots H_n$

Утверждение 3.7. G — абелева группа. $|G| < \infty$

$$(*) : \forall x \in G \exists n : \text{ord } x = p^n \\ \implies |G| = p^k.$$

Доказательство. Если $H \leq G$, то H тоже удовлетворяет (*). G/H тоже удовлетворяет (*)

$$x \in G/H \implies x = g + H, \text{ord } g = p^n.$$

$$p^n x = p^n(g + H) = p^n g + H = H = \bar{0} \implies p^n : \text{ord } x.$$

$$x \in G \setminus \{0\}$$

$$H = \langle x \rangle, |H| = p^n, n \neq 0 \text{ (для некоторого } n).$$

$$|G/H| < |G| \implies |G/H| = p^l$$

$$|G| = |G/H| |H| = p^{l+n} \quad \square$$

3.5. 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 $r_1, r_2, f \in K[x]$, и $r_1 \equiv r_2 \pmod{f(x)K[x]}$, то $r_1 = r_2 \iff \deg r_1 = \deg r_2$.

Доказательство. Следствие слева направо очевидно из определения идеала, докажем справа налево.

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

• Если $h(x) = 0$, то $r_1 = r_2$.

• Но если $h(x) \neq 0$, то $\deg(fh) \geq \deg(f)$, но $\deg(r_1 - r_2) < \deg(f)$. Противоречие. \square

Замечание. Неформально можно думать о факторе $K[x]/f(x)K[x]$ как о многочленах со степенью меньше 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 $f(\alpha_1) = g(\alpha_1), \dots, f(\alpha_{n+1}) = g(\alpha_{n+1})$. 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:

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

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

$$f(\alpha) = 0 + C \implies C = 0 \text{ (так как } \alpha - \text{ корень).}$$

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

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

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.

Определение 3.28. Пусть R_1, R_2, \dots, R_n — ассоциативные кольца с 1.

Определим $R = R_1 \times R_2 \dots \times R_n$:

- $(r_1, \dots, r_n) + (r'_1, \dots, r'_n) = (r_1 + r'_1, \dots, r_n + r'_n)$.
- $(r_1, \dots, r_n) * (r'_1, \dots, r'_n) = (r_1 * r'_1, \dots, r_n * r'_n)$.

TODO: Причём эта берёза? $(r_1, 0, 0, \dots)$ $(0, r_2, 0, \dots)$ **TODO:** /причём

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). \square

Определение 3.29. 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 I и J .

Иначе говоря, $I + J = (I \cup J)$

TODO: why?

Определение 3.30. Произведение идеалов $IJ = (\{ab \mid a \in I, b \in J\})$ — это идеал порождённый всеми попарными произведениями.

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

TODO: unsorted

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

$$n\mathbb{Z} \leftrightarrow \pm n.$$

Определение 3.31. 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 $\iff \exists x, y \in \mathbb{Z}: nx + my = 1$.

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

$$n\mathbb{Z} + m\mathbb{Z} \supseteq n\mathbb{Z}, m\mathbb{Z}. \text{ Следовательно } m : d, n : d.$$

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

\Leftarrow Содержит единицу, а значит всё кольцо. □

ТЕПЕРЬ ТРЕБУЕМ R иметь единицу.

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

Доказательство. $\subseteq. IJ \subseteq I \cap J$.

$$\forall r \in IJr = \sum_{i=1}^N a_i b_i, a_i b_i \in I \cap J \text{ а значит и их сумма лежит в пересечении.}$$

$$\supseteq, I \text{ и } J \text{ вз. просты } \implies I + J = R, 1 \in R.$$

$$\implies \exists a \in I, b \in J: a + b = 1.$$

$$\text{Пусть } x \in I \cap J, x = x * 1 = x * (a + b) = xa + xb.$$

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

$$xa + xb \in IJ. \quad \square$$

Замечание. Обратите внимание, что $IJ \subseteq I \cap J$ для всех идеалов I, J .

Теорема 3.8. Пусть R комм асс кольцо с 1, I, J вз простые идеалы.

$$\text{Тогда } R/IJ \cong R/I \oplus R/J$$

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

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

Доказательство. $f: R \rightarrow R/I \oplus R/J$.

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

Каждая проекция является гомоморфизмом, значит это тоже гомом.

$$\text{Ker } f = I \cap J = IJ.$$

$$\text{Ker } f = \{r \in R \mid r \in I, r \in J\} = I \cap J$$

По теорему о гомоморфизме колец получаем требуемое □

Лемма. R асс комм кольцо с 1. Если идеал I вз прост с каждым из идеалов J_1, \dots, J_k , то I вз прост с их произведением

Доказательство. $R = I + J_1 = I + J_1 R = I + J_1 (I + J_2) = I + J_1 I + J_1 J_2 \subset J + I_1 I_2$ И так далее.

$$\subset I + J_1 J_2 R = I + J_1 J_2 (I + J_3) \quad \square$$

Теорема 3.9. I_1, \dots, I_n попарно взаимно просты.

Замечание. $R = \mathbb{Z}$.

m_1, \dots, m_k — попарно взаимно простые целые числа.

$$n = m_1 m_2 \dots m_k.$$

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

Теорема 3.10 (Китайская теорема об остатках). Для любого набора остатков $r_1 \dots r_k$. $\exists x \in \mathbb{Z}$

$$x \equiv r_1 \pmod{m_1} \dots x \equiv r_k \pmod{m_k}$$

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

Доказательство. ? $x \equiv r_1 \pmod{m_1} \dots x \equiv r_k \pmod{m_k}$.

$$(m_i, m_j) = 1.$$

$$n = m_1 \dots m_k.$$

$$n_i = n/m_i.$$

$$(m_i, n_i) = 1 \implies \exists x_i, y_i \in \mathbb{Z}: m_i x_i + n_i y_i = 1.$$

$$n_i y_i \equiv 0 \pmod{m_j} \quad j \neq i \quad n_i y_i \equiv 1 \pmod{m_j} \quad j = i$$

$$l = \sum_{i=1}^k r_i n_i y_i.$$

$$\forall i: 1 \leq i \leq k:$$

$$l \equiv r_i n_i y_i \equiv r_i \pmod{m_i}.$$

□

3.6. 141116

TODO: 141116, unsorted

Определение 3.32. Элемент b делит элемент a (записывается как $b \mid a$), если $a = bc$ для некоторого $c \in R$.

Утверждение 3.11.

$$\bullet \quad b \mid a \iff a \in bR \iff aR \subseteq bR$$

$$\bullet \quad a \in R^* \iff aR = R$$

Доказательство. **TODO:**

□

§Простые и максимальные идеалы.

Определение 3.33. Пусть I — идеал, тогда I простой, если $\forall a, b \in R: ab \in I \implies a \in I \vee b \in I$.

Определение 3.34. I — максимальный, если для любого идеала $J: I \subsetneq J \subset R \implies J = R$.

link: tointro.

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

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

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

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

[?] $\forall r \in R, ra \in L_j \subseteq L$. □

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. $f: A \rightarrow B$, гомоморфизм колец, $I \subseteq B$, I — простой идеал.

Тогда $f^{-1}(I)$ — простой идеал в A .

2. $f: A \rightarrow B$, эпиморфизм колец, $I \subseteq B$, I — максимальный.

Тогда $f^{-1}(I)$ — максимальный.

Утверждение 3.12. 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.

“ \rightarrow ”. (!) 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:

“ \rightarrow ” $\forall r \notin I$ элемент $r + I$ обратим в R/I .

I — максимальный, $r \notin I \implies I \subsetneq I + rR = R$ (равно R , так как I максимальный)

$$\implies \exists x \dots \dots \dots$$

“ \leftarrow ”. Пусть $I \subsetneq J \subseteq R$.

$\exists r \in J \setminus I$, R/I — поле, следовательно $\exists x \in R: xr \equiv 1 \pmod I$. 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.

$J = (x) = x\mathbb{Q}[x, y]$.

$\mathbb{Q}[x, y]/x\mathbb{Q}[x, y] \cong \mathbb{Q}[y]$ — область целостности.

Не поле.

J — простой идеал, но не максимальный.

Далее R область целостности

Утверждение 3.13. R — кольцо главных идеалов.

$I \neq \{0\}$, I — простой идеал. $=(\dots$

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 $\implies (q \in pR \implies pR = qR) \vee (r \in pR \implies r = ps)$.

$p = qr = qspp(1 - qs) = 0 \implies q \in R^* \iff qR = R.$ □

§Факториальные кольца.

Пусть R — область целостности.

Определение 3.35. $a, b \in R$, 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 3.36. $a \in R \setminus R^*$. a неприводим, если $a = bc \implies a \sim b \vee a \sim c$.

Замечание. Ассоциированность 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. “ \rightarrow ”

$$a \sim b \iff \begin{matrix} b|a \\ a|b \end{matrix} \implies a = b\varepsilon = aad\varepsilon \implies a(1 - d\varepsilon) = 0 \implies \varepsilon \in R^* \tag{1}$$

$$\implies b = a\varepsilon \tag{2}$$

$$\tag{3}$$

“ \leftarrow ” Quite Sad.

2) $a = bc \implies (a \sim b \vee a \sim c)$

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

3.7. Вторая пара 141116

Определение 3.37. R — область целостности. R — факториально, если любой элемент единственным образом раскладывается в произведение неприводимых.

Единственность вплоть до порядка и ассоциированности:

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 $\exists \sigma \in S_n: p_i \sim q_{\sigma(i)}$

Теорема 3.14. 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 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. R — кольцо главных идеалов, $a, b, c \in R$, c неприводим.

Тогда $(c|ab \implies c|a \vee c|b)$

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

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 3.38. Кольцо называется нётеровым, если $I_1 \leq I_2 \leq \dots \leq I_{228}$ — идеалы R , то $I_n = I_{n+1} = \dots$

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

Доказательство. R — кольцо главных идеалов $\implies I_k = r_k R$.

$I = \bigcap_{i=1}^{\infty} I_i$ идеал:

$a, b \in I \implies a, b \in I_i \implies a - b \in I_i, ra \in I_i \quad \forall k, \forall r \in R$.

Следовательно $I = qR$, для некоторого $q \in R$. Следовательно $\exists n: q \in I_n = r_n R$

$q \in I_{n+1} = r_{n+1} R \implies qR \subseteq I_{n+1}$, но $qR \supseteq I_{n+1} \implies qR = I_{n+1}$. □

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 .

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

$p_1 R$ — макс $\implies p_1 R$ — простой $\implies (ab : p_1 \implies a : p_1 \vee b : p_1$

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

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.

$$r_1 = p_2 r_2, r_1 R \subseteq r_2 R \tag{4}$$

$$r_2 = p_3 r_3, r_2 R \subseteq r_3 R \tag{5}$$

$\implies r_1 R \subsetneq r_2 R \subsetneq r_3 R \dots$, 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 $\min(n, m)$

$n = 0, \dots$

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

$q_1 q_2 \dots q_m \in p_1 \dots p_n \implies \exists l: 1 \leq l \leq m, q_l \in p_n R, q_l \sim p_n$.

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

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

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

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

\exists биекция $t: \{1, \dots, n - 1\} \rightarrow \{1, \dots, l - 1, l + 1, \dots, m\}, p_i \sim q_{t(i)}$.

$$\sigma \in S_n: \sigma(i) = \begin{cases} t(i) & i \leq n - 1 \\ l & i = n \end{cases} \tag{6}$$

□

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

Определение 3.39. Пусть R — область целостности, назовём R евклидовым, если $\exists \nu: R \setminus \{0\} \rightarrow \mathbb{N} \sqcup \{0\}$:

$\forall a, b \in R:$

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

2) $\exists q, r \in R: a = bq + r$ 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 3.15. Евклидовы кольца \subset кольца главных идеалов \subset факториальные \subset области целостности.

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

Пусть I — его идеал, если $I = \{0\}$, то $I = 0R$.

Рассмотрим $b \in I$, выберем элемент с мин нормой $\nu(b) = \min_{r \in I} \nu(r)$, покажем, что $bR = I$.

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

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

Следовательно $r = 0 \vee \nu(r) \geq \nu(b)$, следовательно $r = 0, a = bq$. □

Определение 3.40. $d = \gcd(a, b)$, если $d|a, d|b$, и из $c|a, c|b$, то $c|d$.

Замечание 1. \gcd определён с точностью до ассоциированности.

TODO: Непонял при чём здесь эта борода . $(a, b) = aR + bR$.

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

3.8. 211116, unsorted

P.s. R — область целостности.

Определение 3.41. $a, b \in R, d = \gcd(a, b)$, если $d|a, d|b$ и $\forall c: c|a, c|b \implies c|d$.

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

2. \gcd Определён с точностью до ассоциативности.

Теорема 3.16. Пусть R — кольцо главных идеалов.

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

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

$d|a \iff aR \subseteq dR$

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

Определение 3.42. a, b — взаимно простые, если у них нет необратимых общих делителей.

Утверждение 3.17. 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 3.43. $a, b \in R, l = \text{lcm}(a, b)$, если $a|l, b|l$, и если $a|c, b|c \implies l|c$.

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

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

Теорема 3.18. a, b — кольцо главных идеалов, $a, b \in R \setminus \{0\}$, тогда $\text{lcm}(a, b) = ab/\gcd(a, b)$.

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

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

$c \in aR \cap bR$

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

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

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

“ \supseteq ”,

$$a'b'd = ab' \in aR \tag{6}$$

$$a'b'd = ba' \in bR \tag{7}$$

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

§,

Далее мы требуем Евклидовости кольца.

Лемма. $\forall a, b, c \in R: \text{gcd}(a, b) = \text{gcd}(a - bc, b).$

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

Доказательство.

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

$$\text{“}\supseteq\text{” } a - bc \in aR + bR, b \in aR + bR.$$

$$\text{“}\subseteq\text{” } b \in bR \subseteq (a - bc)R + bR, a = (a - bc) + bc \in (a - bc)R + bR. \quad \square$$

Лемма. $\text{gcd}(a, 0) = a$

Замечание. $\text{gcd}(a, b)R = aR + bR = (a, b)$, 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.

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

...

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

Утверждается, что $r_{i+1} = (a, b)$.

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

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

§

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

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

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.

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

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

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

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

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

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

$$x_1 - x_0 \div \frac{b}{d} \implies x_1 - x_0 = k\frac{b}{d}, y_1 - y_0 = -k\frac{a}{d}, \text{ где } k \in \mathbb{Z}. \quad \square$$

4. Кольцо целых чисел, теория чисел

4.1. 281116, вторая пара, unsorted

Как обсуждалось ранее $|(\mathbb{Z}/p^k\mathbb{Z})^*| = \phi(p^k) = p^{k-1}(p-1)$

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

1. $\text{ord}(p+1) = p^{k-1}$
2. Пусть $\langle d \rangle = (\mathbb{Z}/p\mathbb{Z})^*$
Тогда $\text{ord } d^{p^{k-1}} = p-1$
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: ?**) $n = p, m = k$.

$$(p+1)^{p^{k-1}} \equiv 1 + p^k \pmod{p^{k+1}}$$

$$(p+1)^{p^{k-1}} \equiv 1 \pmod{p^k} \implies \text{ord}(p+1) \mid p^{k-1}$$

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

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 $\mathbb{Z}/p\mathbb{Z}$).

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

$$\implies \text{ord } d^{p^{k-1}} \mid p-1$$

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

$$\implies p^{k-1}l \mid (p-1) \iff l \mid (p-1) \implies \text{ord}(d^{p^{k-1}}) = p-1$$

3) $\text{ord}((p+1)d^{p^{k-1}}) =$ (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 $k \geq 2$:

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) $\text{ord}(-1) = 2, \text{ord}(5) = 2^{k-2}$
 - (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 4.1. Пусть $n \in \mathbb{N}$, $n = p_1^{k_1} \cdot \dots \cdot p_l^{k_l}$, где p_i — различны.

Причём если $n \div 2$, то $p_1 = 2$.

Тогда:

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

Доказательство. TODO: Не указано... □

Теорема 4.2. $(\mathbb{Z}/n\mathbb{Z})^*$ циклическая \iff выполнено одно из:

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

TODO: ..

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

Определение 4.1. Функция Карлмайка $\lambda: \mathbb{N} \rightarrow \mathbb{N}$.

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

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

Теорема 4.3.

1) Если $n \not\equiv 1$, то $\lambda(n) = \text{lcm}_{1 \leq i \leq l} (p_i^{k_i} (p_i - 1))$

TODO: шта?

$$n = 2^k m, k \geq 3, m \not\equiv 2$$

2) $(a, n) = 1, a^{\lambda(n)} \equiv 1 \pmod{n}$

4.1.1. 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) $|T|/\phi(n) \text{ — ?}$

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

Определение 4.2. Составные числа n , такие что $|T_n| = \phi(n)$ называются псевдо-простыми для данного теста.

Определение 4.3. 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

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

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

4.2. Шифрование

4.2.1. Предисловие

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

Где P, C — последовательности из символов какого-то алфавита (пусть Z/nZ)

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”.

4.2.2. 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, знаящими p, q и сложно вычисляемо остальными.
- Алиса и Боб выбирает некое $e: 1 \leq e \leq \phi(N)$, $\gcd(e, \phi(N)) = 1$.
- Определим функцию шифрования: $f(x) := x^e$
- Находим $d \in \mathbb{Z}$, такое что $de \equiv 1 \pmod{\phi(N)}$.
- 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, знаящий N , e может шифровать, но только знающие p, q могут быстро сделать дешифровку.

4.3. Сравнения по модулю

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

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

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

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

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

Вопрос по поводу $p = 2$ замнём.

Определение 4.4. 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 4.5. Пусть p — простое число ≥ 3 .

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

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

Определение 4.6. $(F_p^*)^2 := \{x^2 \mid x \in F_p^*\}$

Лемма. $0 \in (F_p^*)^2 \leq F_p^*$

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

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

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

Доказательство. Пункт 0 остаётся в качестве упражнения на определения.

Пусть $f: F_p^* \rightarrow F_p^*$, где $x \mapsto x^2$.

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

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

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

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

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

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

Определение 4.7. Пусть p — простое ≥ 3 , $a \in \mathbb{N}$, $\text{gcd}(a, p) = 1$.

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

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

Утверждение 4.4.

$$1. \quad \left(\frac{a}{b}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

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

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

Доказательство. Пока что замаяли. □

Теорема 4.5. Пусть p, q — простые, ≥ 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 замаяли. □

Определение 4.8. $n = p_1 \dots p_m$, где p_i — простые ≥ 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 4.6. $n \not\equiv 2 \pmod{4} \implies \left(\frac{1}{n}\right) = -1, \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}, \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$

Теорема 4.7. $\gcd(a, n) = 1, a, n$ — нечётные. $\left(\frac{a}{n}\right) \left(\frac{n}{a}\right) = (-1)^{\frac{n-1}{2} \frac{a-1}{2}}$.