Алгебра

Саютин Дмитрий

9 ноября 2016 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
$\varnothing$	$\forall x\colon x \notin \varnothing$	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 $\forall x \in X\colon \exists!\, y \in Y\colon (x, y) \in \Gamma$.

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

***Определение* 1.4.**

- Запись $f\colon X \to Y$ 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 $\mathrm{Im} f$) называется множество $y \in Y$, таких что $\exists x \in X\colon f(x) = y$.

***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:

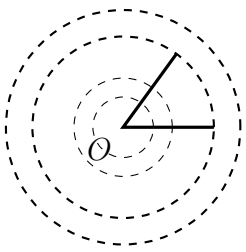
- Рефлексивность: $x - x = 0 \vdots n$.
- Симметричность: $(x - y) \vdots n \implies (y - x) \vdots n$.
- Транзитивность: $(x - y) \vdots n, (y - z) \vdots n \implies (x - y) + (y - z) \vdots n \implies (x - z) \vdots n$.

$\mathbb{Z}/\sim$ 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 наибольшим, 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:

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

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 — $-x$.

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

Пример 1. -1, $+1$, операция перемножения.

Является абелевой группой.

TODO: more coming soon

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.

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

R^* — множество обратимых элементов моноида.

$\mathbb{Z}^* = \{+1, -1\}, \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

Пример 4. X — множество, R — кольцо.

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

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

***Определение* 3.8.** 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* 3.9.** 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* 3.10.** R^* (также обозначается как $R^\times$) – множество обратимых элементов кольца по умножению.

***Определение* 3.11.** Пусть R — коммутативное кольцо.

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

***Определение* 3.12.** 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 ($n = m^2l$, 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. Утеряно в веках. □

***Определение* 3.13.** Коммутативное ассоциативное кольцо с 1 без делителей нуля называется областью целостности (целостным кольцом).

3.3. Гомоморфизм колец

***Определение* 3.14.** $f\colon A \to B$ 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* 3.15.** $\mathrm{Ker} f = f^{-1}(0) = \{x \in A \mid f(x) = 0\}$

***Определение* 3.16.** $\mathrm{Im} f = \{f(x) \mid x \in A\}$.

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 $f^{-1}(b) = a + \mathrm{Ker} f$
4. f — инъективна $\iff$ $\mathrm{Ker} f = \{0\}$

Доказательство. Уже было доказано в теории групп. □

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

Упражнение: привести пример.

***Определение* 3.17.** 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* 3.18.** 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* 3.19.** Если канонический гомоморфизм ϕ — инъективен ($\mathrm{Ker}\phi = \{0\}$), то характеристика ноль ($\mathrm{Char}R := 0$)

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 ($\mathrm{Char}R = n$).

***Определение* 3.20.** Непустое подмножество кольца R называется подкольцом, если

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

***Определение* 3.21.** 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 $\forall r \in R, \forall s \in I\colon rs \in I$ (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 $f\colon A \to B$ — гомоморфизм колец, то

$\mathrm{Im} f$ — подкольцо B.

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

Доказательство. Оставлено в качестве упражнения. □

***Определение* 3.22.** 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, тоесть 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* 3.23.**

- (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* 3.24.** 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, $a \equiv a' \mod I$, $b \equiv b' \mod I$, то

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

Доказательство.

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

Пример. $m, l \in \mathbb{Z}$

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

***Определение* 3.25.** 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, $f \in K[x]$.

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 $r = f, q = 0$.

- $f(x) = a_0 + a_1x + \dots a_nx^n$, $g(x) = b_0 + b_1x + \dots b_mx^m$, $a_n, b_m \neq 0$.
  $f_1(x) = f(x) - g(x)\frac{a_n}{b_m}x^{n-m}$, здесь мы неявно пользуемся тем, что в поле можно делить.
  $\deg f_1 < n \overset{\text{по индукции}}{\Longrightarrow} \exists q_1, r_1 \colon f_1 = q_1g + r_1$
  $g = g\frac{a_n}{b_m}x^{n-m} + f_1 = g\frac{a_n}{b_m}x^{n-m}gq_1 + r_1 = g(\frac{a_n}{b_m}x^{n-m} + q_1) + r_1$

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 справа.
- Противоречие. □

Теорема 3.4 (Теорема о гомоморфизме)**.** Пусть f — гомоморфизм колец с 1. Тогда $A/\mathrm{Ker}f \simeq \mathrm{Im}f$.

Доказательство. Из теоремы о гомоморфизме групп у нас есть: $\phi \colon A \,/\, \mathrm{Ker}f \to \mathrm{Im}f$
Нужно показать гомоморфизм умножения: $\phi(ab) = \phi(a)\,\phi(b)$.
Что оставляется как упражнение читателю. □

***Определение* 3.26.** 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. В данной конструкции много делителей нуля.

TODO: Дальше что-то странное, страшное, непонятное..

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

Утверждение 3.5. Пусть $H_1, \dots, H_n \leqslant G$.

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

Утверждение 3.6. G — абелева группа. $|G| < \infty$
(*): $\forall x \in G\ \exists n \colon \mathrm{ord}x = p^n$
$\Longrightarrow |G| = p^k$.

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

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

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

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

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

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

$|G| = |G/H|\,|H| = p^{l+n}$ □

TODO: Live capture. Никаких гарантий

$K[x]$– поле.

$K[x]/f(x)K[x]$, все идеалы имеют вид $f(x)K[x]$, можно пофакторизовать.

$(f(x)) = f(x)K[x] = I$.

Для всех $g(x)$ сущест единственные: $g(x) = q(x)f(x) + r(x)$, $DEG(r) < DEGf$.

$g(x) \equiv r(x) \mod I$.

Можно думать об этом факторе, как о многочленах со степенью меньшей f.

$r_1, r_2 \colon degr_1, degr_2 < degf$.

$r_1 - r_2 = f(x)h(x)$, если $r_1 \equiv r_2 \mod I$.

$deg(f(x)h(x)) \geqslant degf$, если не нули.

Слева $< deg(f)$.

Поэтому противоречие, справа ноль, а $r_1 = r_2$.

$K[x]/I = \{r \in K[x] \mid DEG(r) < degf\}$.

Предложение. R — область целостности $\forall f \in R[x]$. $\forall g \in R[X], g \neq 0, g = b_k x^k + b_{k-1}x^{k-1} + \ldots b_0$.

$b_k \neq 0$, требуем $b_k \in R*$.

Тогда $\exists q, r \in R[x] \colon f = gq + r$, что $\deg r < \deg q$, доказательство как в прошлой теореме делимосте.

Лемма. Пусть R — область целостности (как частный случай — поле), $f, g \in R[x], \alpha \in R$. Тогда
- Если $f(\alpha) = 0$, то $f(x) = (x-\alpha)q(x)$, где $q(x) \in R[x]$, $\deg q = degf - 1$.
- Если $n = \deg f$, то f имеет не более f различных корней в R.
- 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) $f(x) = (x-\alpha)q(x) + r, \deg r < deg(x-\alpha) = 1 \implies \deg r = 0 \implies r$ – константа. $f(x) = (x-\alpha) + C$. $x = \alpha \colon 0 = 0 + C \implies C = 0$.

2) Индукция по n. $n = 1$, $f(x) = ax + b$ $(a \neq 0)$ явно не более, чем один. Возможно a необратим, тогда ваще ноль.

Переход. Пусть f имеет корни. Пусть $\alpha \colon f(\alpha) = 0$. $f(x) = (x-\alpha)q(x)$, $\deg q = n - 1$

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 вырожд случая.

Пример. Важно, что оц. Иначе эти три факта неверны, к чему предлагается построить примеры.

Опр $R_1, R_2, \dots R_n$ - кольца (ассоциативные, с 1).

$R = R_1 \times R_2 \dots \times R_n$.

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

$(r_1, 0, 0, \dots)$ $(0, r_2, 0, \dots)$

Пусть R комм кольцо навсегда, а I, J – идеалы R.

$I \cap J$ идеал.

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

Правда ли, что $I + J$ идеал? Подгруппа ад группы кольца + ???.

$I + J$ наименьший идеал содержащий и I и J. $I + J = (I \cup J)$

Хочется определить $IJ = \{ab \mid a \in I, b \in J\}$, но вот упс, это не идеал (УПР).

$IJ = (\{ab \mid a \in I, b \in J\})$, идеал порождённый всеми попарными произведениями.

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

$n\mathbb{Z} < - > \pm n$.

***Определение* 3.27.** 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. $n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$.

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

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

$<=$ Содержит единицу, а значит всё кольцо. □

ТЕПЕРЬ ТРЕБУЕМ R иметь единицу.

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

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

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

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

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

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

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

$xa + xb \in IJ$. □

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

Теорема 3.7. Пусть R комм асс кольцо с 1, I, J вз простые идеалы.

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

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

Каждая проекция является гомоморфизмом, значит это тоже гомом.

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

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

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.
$\subset I + J_1 J_2 R = I + J_1 J_2 (I + J_3)$ □

Теорема 3.8. $I_1, ..I_n$ попарно вз просты.,,,,,,,,,,,,,,,,,,,,,,

Замечание. $R = \mathbb{Z}$.

$m_1, \dots m_k$ – попарно вз пр целые числа.

$n = m_1 m_2 ... m_k$.

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

Теорема 3.9 (Китайская теорема об остатках)**.** Для любого набора остатков $r_1 \dots r_k$. $\exists x \in \mathbb{Z}$

$x \equiv r_1 \mod m_1$ .... $x \equiv r_k \mod m_k$

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

Доказательство. ? $x \equiv r_1 \mod m_1$. ... $x \equiv r_k \mod m_k$.

$(m_i, m_j) = 1$.

$n = m_1 \dots m_k$.

$n_i = n/m_i$.

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

$n_i y_i \equiv 0 \mod m_j\ j \neq i\ n_i y_i \equiv 1 \mod m_j\ j = i$

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

$\forall i\colon 1 \leqslant i \leqslant k\colon$

$l \equiv r_i n_i y_i \equiv r_i mod m_i$. □