# 1. Лекция 1. Алгебраические структуры.

1.1. **Алгебраические структуры.** Алгебра изучает алгебраические структуры.

**Определение 1.1.** Алгебраическая структура – это множество с набором операций.

Под $n$-арной операцией мы подразумеваем произвольное

$$* : M \times \ldots \times M \to M.$$

Обычно мы будем рассматривать бинарные операции $* : M \times M \to M$.

**Примеры.**

(1) Натуральные числа $\mathbb{N} = \{1, 2, 3, \ldots, \}$, целые числа $\mathbb{Z}$, рациональные числа $\mathbb{Q}$, действительные числа $\mathbb{R}$ является алгебраическими структурами относительно сложения $+$ и умножения $\cdot$.

Мы не даем определение действительных чисел и не определяем операции, это обычно делается на курсе математического анализа. Рациональные числа мы определим позже.

(2) Вектора на плоскости и в пространстве образуют алгебраическую структуру относительно сложения.

(3) Множества отображений

$$Map(M, M) = \{f : M \to M\}$$

и биективных отображений

$$S(M) := \{f \in Map(M, M) \mid f - \text{биекция}\}$$

образуют алгебраическую структуру относительно композиции.

(4) Множество отображений

$$Map(M, \mathbb{R}) = \{f : M \to \mathbb{R}\}$$

образуют алгебраическую структуру относительно операций поточечного сложения и умножения.

Более точно, алгебра изучает алгебраические структуры с точностью до изоморфизма.

**Определение 1.2.** Алгебраические структуры $(M, *)$ и $(N, \cdot)$ изоморфны $(M, *) \simeq (N, \cdot)$, если существует биективное отображение

$$f : M \to N$$

такое, что $f(x * y) = f(x) \cdot f(y)$ для любых $x, y \in M$.

**Примеры.**

(1) $(\mathbb{R}, +) \simeq (\mathbb{R}_{>0}, \cdot)$ посредством отображения $f : \mathbb{R} \to \mathbb{R}_{>0}, x \mapsto 2^x$.

(2) Множество векторов на плоскости (в пространстве) с операцией сложения изоморфно множестве параллельных переносов относительно композиции: вектору сопоставляем параллельный перенос вдоль этого вектора.

1.2. **Группы, кольца, поля.** Изучать произвольные алгебраические структуры без каких-либо ограничений дело достаточно безнадёжное и бессмысленное. Числовые алгебраические структуры обладают набором свойств, аксиоматизируя которые мы приходим к понятиям *группы, кольца* и *поля*.

(1) $\forall\ a, b, c \in X\ a + (b + c) = (a + b) + c$ (ассоциативность);
(2) $\exists\ 0\ \forall\ a \in X\ a + 0 = 0 + a = a$ (нейтральный элемент);
(3) $\forall\ a \in X\ \exists\ b \in X$ так что $a + b = b + a = 0$, (обратный элемент);
(4) $\forall\ a, b \in X\ a + b = b + a$ (коммутативность);
(5) $\forall\ a, b, c \in X\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(6) $\exists\ e\ \forall\ a \in X\ a \cdot e = e \cdot a = a$;
(7) $\forall\ a \in X \setminus \{0\}\ \exists\ b \in X$ так что $a \cdot b = b \cdot a = e$;
(8) $\forall\ a, b \in X\ a \cdot b = b \cdot a$;

(9) $\forall\ a, b, c \in X\ a(b+c) = a \cdot b + a \cdot c$ (левая дистрибутивность);
(10) $\forall\ a, b, c \in X\ (a+b) \cdot c = a \cdot c + b \cdot c$ (правая дистрибутивность).

**Определение 1.3.** Множество $(X, +)$ с бинарной операцией $+$ удовлетовряющей аксиомам 1)-3) называется группой.

Это так называемая аддитивная нотация. Обычно группу определяют с помощью мультипликативной нотации:

(1) $\forall\ a, b, c \in X\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
(2) $\exists\ e\ \forall\ a \in X\ a \cdot e = e \cdot a = a$;
(3) $\forall\ a \in X\ \exists\ b \in X$ так что $a \cdot b = b \cdot a = e$;

**Определение 1.4.** Множество $(X, +)$ с бинарной операцией $+$ удовлетворяющими аксиомам 1)-4) называется абелевой группой.

**Определение 1.5.** Множество $(X, +, \cdot)$ с бинарными операциями $+, \cdot$ удовлетворяющими аксиомам 1)-4), 9)-10) называется кольцом.

**Определение 1.6.** Множество $(X, +, \cdot)$ с бинарными операциями $+, \cdot$ удовлетворяющими аксиомам 1)-4), 9)-10) называется кольцом.

**Определение 1.7.** Множество $(X, +, \cdot)$ с бинарными операциями $+, \cdot$ удовлетворяющими аксиомам 1)-5), 9)-10) называется ассоциативным кольцом.

По умолчанию все кольца в этих лекциях будут считаться ассоциативными.

**Определение 1.8.** Множество $(X, +, \cdot)$ с бинарными операциями $+, \cdot$ удовлетворяющими аксиомам 1)-6), 9)-10) называется (ассоциативным) кольцом с единицей.

**Определение 1.9.** Множество $(X, +, \cdot)$ с бинарными операциями $+, \cdot$ удовлетворяющими аксиомам 1)-7), 9)-10) называется (ассоциативным) коммутативным кольцом с единицей.

**Определение 1.10.** Множество $(X, +, \cdot)$ с бинарными операциями $+, \cdot$ удовлетворяющими аксиомам 1)-10) называется полем.

Иными словам, поле - это множество с двумя бинарными операциями $(X, +, \cdot)$ такое, что $(X, +), (X \setminus \{0\}, \cdot)$ – абелевы группы + дистрибутивность.

(1) Примеры групп: $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{Q}\setminus\{0\}, \cdot), (\mathbb{R}, +), (\mathbb{R}\setminus\{0\}, \cdot)$, (Вектора, $+$), $(S(M), \circ)$, $(Map(M, \mathbb{R}), +)$, $(R^\times, \cdot)$, где $R$ – произвольное кольцо с единицей, $R^\times$ – обратимые элементы этого кольца.
(2) Примеры абелевых групп: все выше, кроме $(S(M), \circ)$.
(3) Примеры колец: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(Map(M, \mathbb{R}), +, \cdot)$. Все кольца ассоциативные, коммутативные и с единицей.
(4) Примеры полей: $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$.

Цель первых лекций – обобщить понятие числа (кольца), а именно, построить некоторые алгебраические структуры, обладающие свойствами чисел: коммутативные кольца с единицей и поля.

1.3. **Целые числа.** Какие вопросы можно задавать о кольцах? Один из возможных вопросов звучит так: как устроенны его элементы? Напомним, что натуральное число называется *простым*, если оно
1) Не равно единице;
2) Делится только на себя и на единицу.
Чуть менее известно определение простого целого числа. Напомним, что $\mathbb{Z}^\times = \{1, -1\}$.

**Определение 1.11.** Элемент $n \in \mathbb{Z}$ называется простым, если:

(1) $n$ необратим;
(2) Если $n = ab$, то либо $a \in \mathbb{Z}^\times$, либо $b \in \mathbb{Z}^\times$.

**Теорема 1.12** (Основная теорема арифметики)**.** Любое целое необратимое число единственным образом представляется в виде произведения простых чисел. Точнее, если $n \in \mathbb{Z}$ и $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_s$, где все $p_i, q_i$ – простые, то

(1) $k = s$;
(2) С точностью до перестановки $p_i = \pm q_i$.

*Доказательство.* Существование разложения очевидно: если число $n > 1$ не простое, то поделим его на какой-то его делитель $1 < a < n$: $n = ab$ и продолжим эту процедуру с числами $a$ и $b$. Так как каждый раз числа уменьшаются, то процесс не может быть бесконечным. Единственность следует из следующего утверждения:

**Лемма 1.13** (Лемма Евклида)**.** Пусть $p$ – простое, $a, b$ – целые и $p$ делит $ab$. Тогда $p$ делит $a$ или $p$ делит $b$.

Действительно, если $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_s$, то из леммы Евклида следует, что $p_1$ делит некоторый $q_i$, а значит, $p_1 = \pm q_i$. Поделив на $p_1$ оба выражения, получим два различных разложения на простые множители двух меньших чисел и по предположению индукции получаем доказательство теоремы. □

Лемму Евклида мы докажем в следующем разделе.

1.4. **Деление с остатком.** Для доказательства леммы Евклида нам понадобится деление с остатком.

**Предложение 1.14** (Деление с остатком)**.** Для любых $a, b \in \mathbb{Z}$ существует единственные $q, r \in \mathbb{Z}$ такие, что $a = bq + r$, $0 \leq r < |b|$.

**Определение 1.15.** *Наибольшим общим делителем* чисел $a, b \in \mathbb{Z}$ называется $d \in \mathbb{Z}$ такой, что:

(1) $d$ общий делитель $a, b$;
(2) $d$ – наибольший среди всех общих делителей.

Для нахождения НОД двух чисел существует алгоритм Евклида, который базируется на следующем наблюдении.

**Лемма 1.16.** $\text{НОД}(a, b) = \text{НОД}(a - b, b)$.

Алгоритм следующий:

$$a = bq_1 + r_1;$$
$$b = r_1 q_2 + r_2;$$
$$r_1 = q_3 r_2 + r_3$$
$$\ldots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n$$

Последний ненулевой остаток $r_n = \text{НОД}(a, b)$. Набор равенств выше позволяет выразить $\text{НОД}(a, b)$ через $a, b$.

**Предложение 1.17** (Линейное представление НОД)**.** Для любых $a, b \in \mathbb{Z}$ существует $x, y \in \mathbb{Z}$ такие, что

$$ax + by = \text{НОД}(a, b)$$

*Доказательство леммы Евклида:* Пусть $p$ не делит $a$. Тогда $\text{НОД}(a, p) = 1$. Значит, существуют $x, y \in \mathbb{Z}$ такие, что $ax + py = 1$. Домножая на $b$ получаем

$$abx + pby = b,$$

откуда следует, что $b$ делится на $p$. □

1.5. **Факториальные кольца.** Попробуем обобщить основную теорему арифметики на произвольное коммутативное кольцо с единицей $R$. Обозначим через $R^\times$ обратимые элементы кольца $R$.

**Определение 1.18.** Элемент $a \in R \setminus \{0\}$ называется делителем нуля, если существует $b \in R \setminus \{0\}$ такой, что $ab = 0$.

**Определение 1.19.** Коммутативное кольцо с единицей называется *областью целостности*, если в нём нет делителей нуля.

Пример: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Не пример: $Map(M, \mathbb{R})$.

В дальнейшем $R$ - область целостности. Следующее определение - аналог простоты целого числа.

**Определение 1.20** (Неприводимый элемент)**.** Элемент $n \in R$ называется неприводимым, если:

(1) $n$ необратим;
(2) Если $n = ab$, то либо $a \in R^\times$, либо $b \in R^\times$.

Почему мы рассматриваем область целостности? Пусть $R = \mathbb{Z}/6\mathbb{Z}$. Тогда это кольцо не содержит неприводимых элементов.

**Определение 1.21.** Элемент $p \in \mathbb{R}$ – простой, если

(1) $p \neq 0$ и $p$ необратим;
(2) Из того, что $p$ делит $ab$ следует, что $p$ делит $a$ или $p$ делит $b$.

Ясно, что любой простой элемент неприводим. Пусть $p$ простой и $p = ab, a, b$ - необратимы. Пусть $p|a$. Тогда $p = qpb$, то есть

$$p(1 - qb) = 0,$$

а значит $b$ обратим. Обратное верно не всегда.

**Упражнение.** В кольце $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$ элемент 2 неприводим, но не прост.

**Определение 1.22.** Элементы $a, b \in R$ называются *ассоциированными*, если существует обратимый $q \in R$ такой, что $a = qb$.

Лемма Евклида означает, что в кольце $\mathbb{Z}$ любой неприводимый элемент прост. Кольцо называется *факториальным*, если в нём верна основная теорема арифметики.

**Определение 1.23.** Пусть $R$ – область целостности. Говорят, что $R$ факториально, любой ненулевой необратимый элемент единственным образом представляется в виде произведения неприводимых. Точнее, если $n \in R$ и $n = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_s$, где все $p_i, q_i$ – неприводимые, то

(1) $k = s$;
(2) С точностью до перестановки $p_i$ ассоциированно с $q_i$.

Дословное повторение доказательства основной теоремы арифметики даёт следующее предложение.

**Предложение 1.24.** Пусть в коммутативном кольце с единицей любой элемент представляется в виде произведения конечного числа неприводимых элементов. Тогда кольцо факториально тогда и только тогда когда любой неприводимый элемент прост.

**Упражнение.** Кольцо $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$ не факториально.

1.6. **Кольца и поля вычетов.** Деление с остатком позволяет получить новые примеры колец и полей. А именно пусть $n \in \mathbb{Z}_{>0}$. Пусть $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$ - множество остатков при делении на $n$. Для любого $a \in \mathbb{Z}$ обозначим через $[a]$ остаток $a$ при делении на $n$. На множестве $\mathbb{Z}/n\mathbb{Z}$ определим операции сложения и умножения:

$$[a] + [b] := [a + b] \quad [a] \cdot [b] := [ab]$$

Тогда $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ – коммутативное кольцо с единицей.

**Предложение 1.25.** Элемент $[a] \in \mathbb{Z}/n\mathbb{Z}$ обратим тогда и только тогда когда НОД$(a, n) = 1$.

*Доказательство.* ($\Leftarrow$) Если НОД$(a, n) = 1$, то существуют $x, y \in \mathbb{Z}$ такие, что $ax + ny = 1$, тогда $[a]^{-1} = [x]$.

($\Rightarrow$) Если НОД$(a, n) = d > 1$, то $n = qd, a = sd$, значит, $aq = sdq = ns = 0$, и $a$ – делитель нуля. А делитель нуля не может быть обратим (почему?). □

**Следствие 1.26.** $\mathbb{Z}/p\mathbb{Z}$ - конечное поле.

Это новое поле обладает интересными свойствами.

**Предложение 1.27.** Пусть $a, b \in \mathbb{Z}/p\mathbb{Z}$. Тогда

(1) $(a + b)^p = a^p + b^p$;
(2) Пусть $a \neq 0$. Тогда $a^{p-1} = [1]$.

*Доказательство.* 1) $(a + b)^p = a^p + \binom{p}{1} a^{p-1}b + \ldots + \binom{p}{p-1} ab^{p-1} + b^p$. Но $\binom{p}{k}$ делится на $p$ для любого $0 < k < p$.
2) $a^p = \underbrace{(1 + \ldots + 1)^p}_{p \text{ раз}} = \underbrace{(1 + \ldots + 1)}_{p \text{ раз}} = a$. □