Алгебра.

В. А. Петров
lektorium.tv

Зарождение — Аль Хорезин, “Китхаб Альджебр валь мукабалт”. “Альджебр” значит “перенос из одной части уравнения в другую”, а “мукабалт” — “приведение подобных”.

Литература:

- Ван дер Варден “Алгебра”
- Лэнг “Алгебра”
- Винберг “Курс Алгебры”

Определение 1. Алгебраическая структура — это множество M + заданные на нём операции + аксиомы на операциях.

Определение 2. Абелева группа — набор $(M, + : M^2 \to M, 0 \in M)$ с аксиомами:

A_1) $\forall a, b, c \in M : (a + b) + c = a + (b + c)$ — ассоциативность сложения

A_2) $\forall a \in M : a + 0 = a = 0 + a$ — нейтральный по сложению элемент

A_3) $\forall a, b \in M : a + b = b + a$ — коммутативность сложения

A_4) $\forall a \in M : \exists -a : a + (-a) = 0 = (-a) + a$ — существование противоположного

Определение 3. Опишем следующие аксиомы на наборе $(M, + : M^2 \to M, \cdot : M^2 \to M, 0 \in M, 1 \in M)$:

D) $\forall a, b, k \in M : k(a + b) = ka + kb$, $(a + b)k = ak + bk$ — дистрибутивность

M_1) $\forall a, b, c \in M : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ — ассоциативность умножения

M_2) $\forall a \in M : a \cdot 1 = a = 1 \cdot a$ — нейтральный по умножению элемент

M_3) $\forall a, b \in M : a \cdot b = b \cdot a$ — коммутативность умножения

M_4) $\forall a \in M \setminus \{0\} : \exists\, a^{-1} : a \cdot a^{-1} = 1 = a^{-1} \cdot a$ — существование обратного

По этим аксиомам определим следующие понятия:

- *Кольцо* — набор $(M, +, \cdot, 0)$, что верны A_1, A_2, A_3, A_4 и D.
- *Ассоциативное кольцо* — кольцо с M_1.
- *Кольцо с единицей* — кольцо с M_2.
- *Тело* — кольцо с M_1, M_2.
- *Поле* — кольцо с M_1, M_2, M_3, M_4.

- *Полукольцо* — кольцо без A_4.

Пример 1. Если взять $\mathbb{R}^3$, то векторное произведение в нём неассоциативно и антикоммутативно. Но есть

Лемма (Тождество Якоби). $u \times (v \times w) + v \times (w \times u) + w \times (u \times v) = 0$

Пример 2. Если взять $R^4 = R \times R^3$ и рассмотреть $\cdot : ((a; u); (b; v)) \mapsto (ab - u \cdot v; av + bu + u \times v)$ и $+ : ((a; u); (b; v)) \mapsto (a + b, u + v)$, тогда получим $\mathbb{H}$ — ассоциативное некоммутативное тело кватернионов. Ассоциативность доказал Гамильтон.

Лемма. $0 \cdot a = 0$

Определение 4. Кольцо без делителей нуля называетсся *областью (целостности).*

Определение 5. Пусть $m \in \mathbb{N}$. Тогда *множество остатков при делении на m* или $\mathbb{Z}/m\mathbb{Z}$ — это фактор-множество по отношению эквивалентности $a \sim b \Leftrightarrow (a - b) \mid m$.

Определение 6. *Подкольцо* — это подмножество кольца, согласованное с его операциями.

Как следствие ноль и обратимость соглассуются автоматически.

Утверждение 1. *Если R — подкольцо области целостности S, то R — область целостности.*

Определение 7. *Целые Гауссовы числа* или $\mathbb{Z}[i]$ — это $\{a + bi \mid a, b \in \mathbb{Z}\}$.

Определение 8. Некоторое подмножество R кольца S *замкнуто относительно сложения (умножения)*, если $\forall a, b \in R : a + b \in R$ ($ab \in R$ соответственно).

Замечание 1. Замкнутое относительно сложения **И** умножения подмножество — подкольцо.

Пример 3. Пусть d — целое, не квадрат. Тогда $\mathbb{Z}[\sqrt{d}]$ — область целостности.

1 Теория делимости

Пусть R — область целостности.

Определение 9. "*a делит b*" или же $a \mid b$ значит, что $\exists c \in R : b = ac$.

Утверждение 2. *Отношение "$\mid$" рефлексивно и транзитивно.*

Определение 10. a и b *ассоциативны*, если $a \mid b$ и $b \mid a$. Обозначение: $a \sim b$.

Утверждение 3. *"$\sim$" — отношение эквивалентности.*

Утверждение 4. *$a \sim b \Leftrightarrow \exists$ обратимый $\varepsilon : a = \varepsilon b$.*

Доказательство. Пусть $a \sim b$. Тогда $\exists c, d : ac = b, bd = a$. Тогда $a(1 - cd) = a - acd = a - bd = a - a = 0$, значит либо $a = 0$, либо $cd = 1$. В первом случае $b = ac = 0c = 0$, значит можно просто взять $\varepsilon = 1$. Во втором случае, $cd = 1$, значит c и d обратимы, тогда можно взять $\varepsilon = d$. следствие в одну сторону доказано.

Пусть $a = \varepsilon b$, где ε обратим. Значит:

1. $b \mid a$;
2. $\exists \delta : \delta\varepsilon = 1$, значит $\delta a = \delta\varepsilon b = b$, значит $a \mid b$.

Таким образом $a \sim b$. $\square$

Пример 4. В $\mathbb{Z}[i]$ есть только следующие обратимые элементы: 1, -1, i и $-i$. Поэтому все ассоциативные элементы получаются друг из друга домножением на один из 1, -1, i, $-i$ и вместе образуют квадрат (на комплексной плоскоти) с центром в нуле.

Определение 11. *Главным идеалом* элемента a называется множество $M := \{ak \mid k \in R\} = \{b \mid a \text{ делит } b\}$. Обозначение: (a) или aR.

Утверждение 5. *$a \mid b \Leftrightarrow b \in aR \Leftrightarrow bR \subseteq aR$.*

Утверждение 6. *$a \sim b \Leftrightarrow aR = bR$.*

Утверждение 7. *$\forall a \in R$*

1. $0 \in aR$
2. $x \in aR \Rightarrow -x \in aR$
3. $x, y \in aR \Rightarrow x + y \in aR$
4. $x \in aR, r \in R \Rightarrow xr \in aR$

Замечание 2. То же верно и в некоммутативном R.

Пример 5. В поле есть только $0R$ и $1R$.

Пример 6. В $\mathbb{Z}$ есть только $m\mathbb{Z}$ для каждого $m \in \mathbb{N} \cup \{0\}$.