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) $a + b = b + a$ — коммутативность сложения

A_2) $(a + b) + c = a + (b + c)$ — ассоциативность сложения

A_3) $a + 0 = a = 0 + a$ — нейтральный элемент

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

Определение 3. *Кольцо* — набор $(M, +, \cdot, 0)$, что верны A_1, A_2, A_3, A_4 и D.
Ассоциативное кольцо — кольцо с M_2.
Кольцо с единицей — кольцо с M_3.
Тело — кольцо с M_2, M_3.
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 $\exists c \in R : b = ac$.