

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 $(M, + : M^2 \rightarrow M, 0 \in M)$ 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 $(M, + : M^2 \rightarrow M, \cdot : M^2 \rightarrow M, 0 \in M, 1 \in M)$:

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

*Этот текст содержит критические недочёты. Вы можете помочь исправить их, написав мне по почте (minaevgleb@yandex.ru) или в ВКонтакте (@lounres).

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. Коммутативное кольцо без делителей нуля называется *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 согласуются 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 $a \sim b$. □

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 плоскости) 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 $m \in \mathbb{N} \cup \{0\}$.

Определение 12. Пусть P — кольцо. $I \subseteq P$ называется *правым идеалом*, если

1. $0 \in I$;
2. $a, b \in I \Rightarrow a + b \in I$;
3. $a \in I \Rightarrow -a \in I$;
4. $a \in I, r \in R \Rightarrow ar \in I$.

I называется *левым идеалом*, если аксиому 4 заменить на “ $a \in I, r \in R \Rightarrow ra \in I$ ”. Также I называется *двухсторонним идеалом*, если является левым и правым идеалом, и обозначается как $I \triangleleft P$.

Замечание 3. В коммутативном кольце (и в частности в области целостности) все идеалы двухсторонние.

Пример 7. Пусть дано кольцо P и фиксированы $a_1, \dots, a_n \in P$. Тогда $a_1P + \dots + a_nP = \{a_1x_1 + \dots + a_nx_n \mid x_1, \dots, x_n \in P\}$ есть правый (конечнопорождённый) идеал, порождённый элементами a_1, \dots, a_n . Аналогично $Pa_1 + \dots + Pa_n = \{x_1a_1 + \dots + x_na_n \mid x_1, \dots, x_n \in P\}$ — левый (конечнопорождённый) идеал, порождённый элементами a_1, \dots, a_n .

Определение 13. Область главных идеалов — область целостности, где все идеалы главные.

Определение 14. Область целостности R называется *Евклидовой*, если существует функция (“Евклидова норма”) $N : R \setminus \{0\} \rightarrow \mathbb{N}$, что

$$\forall a, b \neq 0 \exists q, r : a = bq + r \wedge (r = 0 \vee N(r) < N(b))$$

Теорема 1. Евклидово кольцо — область главных идеалов.

Доказательство. Пусть наше кольцо — R . Если $I = \{0\}$, то $I = 0R$. Иначе возьмём $d \in I \setminus \{0\}$ с минимальной Евклидовой нормой. Тогда $\forall a \in I$ либо $d \mid a$, либо $\exists q, r : a = dq - r$. Во втором случае $dq \in I$, $r = a - dq \in I$, но $N(r) < N(d)$ — противоречие. Значит $I = dR$. \square

Определение 15. Общим делителем a и b называется c , что $c \mid a$ и $c \mid b$. Наибольшим общим делителем (НОД) a и b называется общий делитель a и b , делящийся на все другие общие делители a и b .

Теорема 2 (алгоритм Евклида). В Евклидовом кольце у любых двух чисел есть НОД.

Доказательство. Заметим, что $(a, b) = (a + bk, b)$.

Пусть даны a и b . Предположим, что $\phi(a) \geq \phi(b)$, иначе поменяем их местами. Тем самым по аксиоме Евклида найдутся q и r , что $a = bq + r$, а $\phi(r) < \phi(b) \leq \phi(a)$, значит $\phi(a) + \phi(b) > \phi(r) + \phi(b)$. При этом $(a, b) = (r, b)$. Значит бесконечно $\phi(a) + \phi(b)$ не может бесконечно уменьшаться, так как натурально, значит за конечное кол-во переходов мы получим, что одно из чисел делит другое, а значит НОД стал определён. \square

Теорема 3 (линейное представление НОД). $\forall a, b \in R \exists p, q \in R : ap + bq = (a, b)$.

Доказательство. Докажем по индукции по $N(a) + N(b)$.

База. $N(a) + N(b) = 0$. Значит $N(a) = N(b) = 0$, а тогда a и b не могут не делиться друг на друга, значит НОД — любой из них. А в этом случае разложение очевидно.

Шаг. $N(a) + N(b) \geq 1$. Если $b \mid a$, то b — НОД, а тогда разложение очевидно. Иначе по аксиоме Евклида $\exists q, r : a = bq + r$. Заметим, что $(a, b) = (b, r) = d$, но $N(a) + N(b) \geq N(b) + N(r) > N(b) + N(r)$. Таким образом по предположению индукции для b и r получаем, что $d = bk + rl$ для некоторых k и l , значит $d = bk + (a - bq)l = al + b(k - ql)$. \square

Определение 16. Элемент p области целостности R называется *неприводимым*, если $\forall d \mid p$ либо $d \sim 1$, либо $d \sim p$.

Определение 17. Элемент p области целостности R называется *простым*, если из условия $p \mid ab$ следует, что $p \mid a$ или $p \mid b$.

Утверждение 8. Любое простое неприводимо.

Доказательство. Предположим противное, т.е. некоторое простое p представляется в виде произведения неделителей единицы a и b . Тогда $\text{WLOG } p \mid a$. Значит $p \sim a$, а $b \sim 1$ — противоречие. \square

Утверждение 9. В области главных идеалов неприводимые просты.

Доказательство. Пусть неприводимое p делит ab . Пусть тогда $pR + aR = dR$. В таком случае $d \sim p$, значит либо $d \sim p$, либо $d \sim 1$. Если $d \sim p$, то $p \mid a$. Иначе $px + ay = 1$, значит $pxb + aby = b$. Но $p \mid pxb$ и $p \mid aby$, значит $p \mid b$. Поскольку рассуждение не зависит от a и b , то p просто. \square

Определение 18. Назовём разложением числа a на неприводимые множители представление его в виде произведения $\alpha \prod_{i=1}^n p_i$ с точностью до перестановки членов произведения и домножения их на делители 1 (т.е. их ассоциативности), где все p_i просты.

Область целостности называется *факториальным кольцом*, если в нём все ненулевые элементы разложимы на неприводимые множители единственным образом (также говорят, что в области целостности верна *основная теорема арифметики*).

Утверждение 10. В факториальном кольце неприводимые просты.

Теорема 4. Область главных идеалов удовлетворяет условию обрыва цепи главных идеалов.

Доказательство. Пусть наша область — R . Сначала докажем существование разложения.

Предположим противное, т.е. существует последовательность $\{a_n\}_{n=0}^{\infty}$, что a_{n+1} — собственный делитель a_n (т.е. $a_{n+1} \mid a_n \wedge a_n \not\sim a_{n+1}$). Тогда $a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \dots$. Тогда $\exists x : xR = \bigcup_{n=0}^{\infty} a_nR$, так как это объединение — идеал. Но тогда $x \in a_jR$ для некоторого j , а значит $xR \subseteq a_jR$, а тогда $a_{j+1}R \subseteq a_jR$ — противоречие. \square

Теорема 5. Пусть R — область целостности. Тогда следующие утверждения равносильны.

1. R факториально.
2. R удовлетворяет условию обрыва возрастающей цепи главных идеалов.

Доказательство. Сначала докажем в одну сторону. Пусть R факториально.

Лемма 6. Любой неприводимый в R прост.

Доказательство. Пусть $p \mid ab$ для любого неприводимого p и каких-то a и b . Тогда имеем $px = ab$ для некоторых x , а значит по факториальности, что $a = p_1 \dots p_k$, $b = q_1 \dots q_l$, $x = r_1 \dots r_m$. Тогда имеем два разложения $px = ab$ на простые: $p \cdot r_1 \cdot \dots \cdot r_m$ и $p_1 \cdot \dots \cdot p_k \cdot q_1 \cdot \dots \cdot q_l$. Значит по факториальности оба разложения совпадают, а значит p равно какому-то неприводимому из разложений a и b . А значит $p \mid a$ или $p \mid b$, что и означает простоту p . \square

Лемма 7. Если $a \mid b$, то разложение на неприводимые в a есть подмножество разложения на неприводимые в b .

Доказательство. Пусть p — неприводимый из разложения a . Тогда $p \mid b$, а значит p делит какой-то неприводимый q из разложения b , значит $p \sim q$, значит $a'p \mid b'$, где $a'p = a$, $b'q = b$. Тогда спуском по кол-ву неприводимых в разложении a получаем требуемое утверждение. \square

Проверить начиная с этого момента до конца раздела формальные моменты и довести доказательства.

Пусть нашлась возрастающая последовательность главных идеалов $\{a_n R\}_{n=0}^\infty$, тогда a_{n+1} — собственный делитель a_n для всех n . Тогда разложение на неприводимые a_0 является собственным подмножеством разложением a_n , а поскольку разложение по определению конечно, то такой последовательности быть не может.

Теперь докажем в обратную сторону. Пусть R удовлетворяет условию обрыва возрастающей цепи главных идеалов.

Лемма 8. $ab \sim cd$, $b \sim d$, значит $a \sim c$.

Доказательство. $b = \varepsilon d$, $ab = \delta cd$, где $\varepsilon \sim \delta \sim 1$. тогда $(a\varepsilon - \delta c)d = a\varepsilon d - \delta cd = ab - \delta cd = 0$, значит $a = \varepsilon^{-1}\delta c$, значит $a \sim c$. \square

Теперь предположим имеется R , удовлетворяющее условию обрыва возрастающей цепи главных идеалов. Тогда у каждого числа есть неприводимый делитель, так как иначе есть подъём идеалов: $a_0 = a_1 b_1$, $a_1 = a_2 b_2$ и т.д., значит $a_0 R \subsetneq a_1 R \subsetneq a_2 R \subsetneq \dots$ — противоречие. Тогда и каждое число \square

2 Идеалы

Теорема 9. Пусть даны $I \triangleleft R$ и $a \sim b \Leftrightarrow a - b \in I$. Тогда \sim — отношение эквивалентности, а $R/I := R/\sim$ — кольцо.

Доказательство. Проверим, что \sim — отношение эквивалентности:

- $a - a = 0 \in I$, значит $a \sim a$;
- $a \sim b$, значит $a - b \in I$, значит $b - a = -(a - b) \in I$, значит $a \sim b$;
- $a \sim b$, $b \sim c$, значит $a - b \in I$, $b - c \in I$, значит $a - c = (a - b) + (b - c) \in I$, значит $a \sim c$.

Определим на R/I операции сложения и умножения, нуля, противоположного, единицы и обратного:

- $[a] + [b] := [a + b]$;
- $[a] \cdot [b] := [a \cdot b]$;
- $0 := [0] = I$;
- $-[a] := [-a]$;
- $1 := [1]$;
- $[a]^{-1} := [a^{-1}]$.

Покажем, что R/I — кольцо:

$$A_1) \quad \forall a, b, c \in R : ([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$$

$$A_2) \quad \forall a \in R : [a] + [0] = [a + 0] = a = [0 + a] = [0] + [a]$$

$$A_3) \quad \forall a, b \in R : [a] + [b] = [a + b] = [b + a] = [b] + [a]$$

$$A_4) \quad \forall a \in R : [a] + -[a] = [a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a] = -[a] + [a]$$

$$D) \quad \forall a, b, k \in R : [k]([a] + [b]) = [k][a + b] = [k(a + b)] = [ka + kb] = [ka] + [kb] = [k][a] + [k][b], \\ ([a] + [b])[k] = [a + b][k] = [(a + b)k] = [ak + bk] = [ak] + [bk] = [a][k] + [b][k]$$

$$M_1) \quad \forall a, b, c \in R : ([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c])$$

$$M_2) \quad \forall a \in R : [a] \cdot [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \cdot [a]$$

$$M_3) \quad \forall a, b \in R : [a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$$

$$M_4) \quad \forall a \in R \setminus \{0\} : [a] \cdot [a]^{-1} = [a \cdot a^{-1}] = [1] = [a^{-1} \cdot a] = [a^{-1}] \cdot [a] = [a]^{-1} \cdot [a]$$

Замечание 4. Доказательство для классов эквивалентности каждой аксиомы основывалось только на соответствующей аксиоме и определениях ранее.

□