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.

Утверждение 1. $0 \cdot a = 0$

Определение 4. Коммутативное 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 2. *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 3. *Отношение "$\mid$" рефлексивно и транзитивно.*

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

Утверждение 4. *"$\sim$" — отношение эквивалентности.*

Утверждение 5. $a \sim b \Leftrightarrow \exists$ *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 6. $a \mid b \Leftrightarrow b \in aR \Leftrightarrow bR \subseteq aR$.

Утверждение 7. $a \sim b \Leftrightarrow aR = bR$.

Утверждение 8. $\forall a \in R$

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*, ессли 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 $a_1, \ldots, a_n \in P$. Тогда $a_1P + \cdots + a_nP = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in P\}$ есть правый (конечнопорождённый) идеал, попрождённый элементами $a_1, \ldots, a_n$. Аналогично $Pa_1 + \cdots + Pa_n = \{x_1a_1 + \cdots + x_na_n \mid x_1, \ldots, x_n \in P\}$ — левый (конечнопорождённый) идеал, попрождённый элементами $a_1, \ldots, a_n$.

Определение 13. *Область главных идеалов (ОГИ)* — область целостности, где все идеалы главные.

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

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

Теорема 9. *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 10 (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 $\phi(a) \geqslant \phi(b)$, иначе поменяем их местами. Тем самым по аксиоме Евклида найдутся q и r, что $a = bq + r$, а $\phi(r) < \phi(b) \leqslant \phi(a)$, значит $\phi(a) + \phi(b) > \phi(r) + \phi(b)$. При этом $(a, b) = (r, b)$. Значит бесконечно $\phi(a) + \phi(b)$ не может бесконечнго 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 11 (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. WLOG $N(a) \geqslant N(b)$. 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 $N(a) + N(b) \geqslant N(b) + N(b) > N(b) + N(r)$. 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 назвыается *неприводимым*, если $\forall d \mid p$ либо $d \sim 1$, либо $d \sim p$.

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

Утверждение 12. *Любое простое неприводимо.*

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

Утверждение 13. *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. Область целостности R *удовлетворяет условию обрыва возрастающих цепей главных идеалов (APCC)*, если не существует последовательности $d_0R \subsetneq d_1R \subsetneq \ldots$. Такое кольцо область целостности называют нётеровой.

Теорема 14. *ОГИ нётерова.*

Доказательство. Пусть наша область — R. Предположим противное, т.е. существует последовательность $\{a_n\}_{n=0}^{\infty}$, что a_{n+1} — собственный делитель a_n (т.е. $a_{n+1} \mid a_n \wedge a_n \nsim a_{n+1}$). Тогда $a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \ldots$. 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. $\square$

Определение 19. Область целостности называется *факториальной областью*, если в нём все неприводимые просты и оно нётерово.

Пример 8. ОГИ факториальна.

Теорема 15 (основная теорема арифметики)**.** *Пусть R факториально. Тогда любое число представимо единственным образом в виде произведения простых с точностью до перестановки множителей и ассоциированности.*

Доказательство.

Лемма 15.1. *У каждого числа есть неприводимый делитель.*

Доказательство. Пусть это не так. Тогда 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. □

Лемма 15.2. *Каждое число представимо в виде произведения простых.*

Доказательство. Пусть это не так. Тогда есть подъём идеалов: $a_0 = p_1 a_1$, где p_1 прост, $a_1 = p_2 a_2$, где p_2 прост, и т.д., значит $a_0 R \subsetneq a_1 R \subsetneq a_2 R \subsetneq \dots$ — противоречие. □

Это доказывает существование разложения.

Лемма 15.3. *Если $p_1 \cdot \ldots p_n = q_1 \cdot \dots \cdot q_m$ для простых $p_1, \ldots, p_n, q_1, \ldots, q_m$, то эти два набора совпадают с точностью до перестановки и ассоциированности.*

Доказательство. Докажем индукцией по n.

База: Для $n = 0$ утверждение очевидно, так как тогда $1 = q_1 \cdot \dots \cdot q_m$, значит $m = 0$.

Шаг: Несложно видеть, что $p_n \mid q_1 \cdot \dots \cdot q_m$, значит $p_n \mid q_i$ для некоторого i, значит $p_n \sim q_i$. Переставим q_k, что $q'_m = q_i$. Значит $p_1 \cdot \dots \cdot p_{n-1} = q'_1 \cdot \dots \cdot q'_{m-1}$. По предположению индукции эти два набора совпадают с точностью до перестановки и ассоциированности, значит таковы и начальные наборы. □

Это доказывает единственность разложения. □

2 Идеалы и морфизмы

Теорема 16. *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 $a \sim a$;
- $a \sim b$, $b \sim c$, 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) $\forall a, b, c \in R : ([a]+[b])+[c] = [a+b]+[c] = [(a+b)+c] = [a+(b+c)] = [a]+[b+c] = [a]+([b]+[c])$

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

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

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

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

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

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

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

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

□

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

Определение 20. *Гомоморфизм* — такое отображение $\phi : R \to S$ — это отображение, сохраняющее операции:

- $\phi(a + b) = \phi(a) + \phi(b)$;
- $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$;
- $\phi(0) = 0$;
- $\phi(-a) = -\phi(a)$.

Гомоморфизм кольца с 1 — гомоморфизм, что $\phi(1) = 1$.

Утверждение 17. *Композиция гомоморфизмов — гомоморфизм.*

Определение 21. Пусть $f : X \to Y$. Несложно видеть, что f расклаадывается в композицию сюръекции $f : X \to f(X)$ и инъекции $id : f(X) \to Y$. Тогда $\mathrm{Im}(f) = \{f(x) \mid x \in X\}$ — *множество значений* f, а классы значений X, переходящих в один $y \in Y$ суть *слои* — $f^{-1}(y) = \{x \mid f(x) = y\}$ для некоторого y.

Определение 22. Пусть $\phi : R \to S$ — гомоморфизм. Тогда *ядром* ϕ называется $\mathrm{Ker}(\phi) := \{r \in R \mid \phi(r) = 0\}$.

Утверждение 18. *Ядро гомоморфизма — двусторонний идеал.*

Определение 23. $\phi : S \to R$ — *изоморфизм*, если это биективный гомоморфизм.

Определение 24. Два кольца называются изоморфными, если между ними есть изоморфизм. Обозначение: $R \cong S$.

Утверждение 19. *Пусть $R \cong S$. Тогда*

- *Если R коммутативно, то и S коммутативно.*
- *Если R — областсть целостности, то и S — область целостности.*
- *Если R — ОГИ, то и S — ОГИ.*

Утверждение 20.

1. $R \cong R$.
2. $R \cong S \Leftrightarrow S \cong R$.
3. $R \cong S \cong T \Rightarrow R \cong T$.

Теорема 21 (теорема о гомоморфизме). *Пусть $\phi : R \to S$ — гомоморфизм. (Вспомним, что $\operatorname{Ker}(\phi) \triangleleft R$, а $\operatorname{Im}(\phi) = \phi(R)$.) Тогда $R/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$, где изоморфизм переводит $[a] \mapsto \phi(a)$.*

Доказательство.

1. Корректность. $[a] = [a'] \Leftrightarrow a - a' \in \operatorname{Ker}(\phi) \Leftrightarrow \phi(a - a') = 0 \Leftrightarrow \phi(a) = \phi(a')$.

   Замечание 5. Классы эквивалентности по $\operatorname{Ker}(\phi)$ как раз слои ϕ.

2. Заметим, что работают следующие операции:

   - $[a] + [b] = [a + b] \mapsto \phi(a) + \phi(b) = \phi(a + b)$;
   - $[a] \cdot [b] = [a \cdot b] \mapsto \phi(a) \cdot \phi(b) = \phi(a \cdot b)$.

3. Сюръективность следует из того, что $\phi(a) = \phi(b) \Leftrightarrow [a] = [b]$.

4. Инъективность следует из того, что каждый элемент в $\operatorname{Im}(\phi)$ имеет прообраз.

□

Теорема 22 (китайская теорема об остатках (КТО) для двух чисел). *Пусть m и n взаимно просты. Тогда $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Доказательство. Рассмотрим $\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, a \mapsto ([a]_m; [a]_n)$. Несложно заметить, что ядро ϕ тривиально, поэтому $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}/\operatorname{Ker}(\phi) \cong \operatorname{Im}(\phi)$. Но в последнем элементов не менее mn, так как $\operatorname{Im}(\phi) \cong \mathbb{Z}/mn\mathbb{Z}$, но и не более, так как $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn$, поэтому $\operatorname{Im}(\phi) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, поэтому $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

Теорема 23 (КТО). *Пусть $m_1, \dots, m_k$ — попарно взаимно простые числа. Тогда*

$$\mathbb{Z}/m_1 \dots m_k \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_k\mathbb{Z}$$

Доказательство. По индукции по k с помощью КТО для двух чисел. □

Теорема 24. *Пусть есть $I \triangleleft R$ и гомоморфизмы $\pi : R \to R/I$ — нативный гомоморфизм, и $\pi : R \to S$, что $\pi(I) = \{0\}$. Тогда существует и единственен гомоморфизм $\phi' : R/I \to S$, что $\phi' \circ \pi = \phi$.*

Доказательство. $\phi'([a]) = (\phi' \circ \pi)(a) = \phi(a)$ — это означает единственность; так функцию и определим. Осталось показать корректность.

Несложно заметить, что если $[a] = [b]$, то $a - b \in I$, значит $\phi(a - b) = 0$, значит $\phi(a) = \phi(b)$. Теперь проверим операции:

- $\phi'([a] + [b]) = \phi'([a + b]) = \phi(a + b) = \phi(a) + \phi(b) = \phi'([a]) + \phi'([b])$.
- $\phi'([a] \cdot [b]) = \phi'([a \cdot b]) = \phi(a \cdot b) = \phi(a) \cdot \phi(b) = \phi'([a]) \cdot \phi'([b])$

□