Алгебра.

Лектор — В. А. Петров
Создатель конспекта — Глеб Минаев *

TODOs

Содержание

Литература:

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

Немного истории

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

1 Основные понятия.

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

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

A$_1$) $\forall a, b, c \in M : (a + b) + c = a + (b + c)$ — ассоциативность сложения

A$_2$) $\exists 0 \in M : \forall a \in M : a + 0 = a = 0 + a$ — нейтральный по сложению элемент

*Оригинал конспекта расположен на GitHub. Также на GitHub доступен репозиторий с другими конспектами.

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 $(M, + : M^2 \to M, \cdot : M^2 \to M)$ в добавок к $A_1, \ldots, A_4$:

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) $\exists 1 \in M : \forall a \in M : a \cdot 1 = a = 1 \cdot a$ — 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, M_4.

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 1. $0 \cdot a = 0$

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 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.

2 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 "$|$" рефлексивно и транзитивно.*

Определение 10. a и b *ассоциированы*, 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 $a \sim b$. □

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*, 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 $I \lhd P$.

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, порождённый 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, порождённый 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 $I = dR$. □

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

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 $d = bk + (a - bq)l = al + b(k - ql)$. □

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 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. ☐

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. ☐

Определение 18. Область целостности R *удовлетворяет условию обрыва возрастающих цепей главных идеалов (ACCP)*, 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. ☐

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: $a_0 = a_1b_1$, $a_1 = a_2b_2$ и т.д., значит $a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \ldots$ — противоречие. ☐

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

Доказательство. Пусть это не так. Тогда есть подъём идеалов: $a_0 = p_1a_1$, где p_1 прост, $a_1 = p_2a_2$, где p_2 прост, и т.д., значит $a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \ldots$ — противоречие. ☐

Это доказывает существование разложения.

Лемма 15.3. *Если $p_1 \cdot \ldots p_n = q_1 \cdot \cdots \cdot q_m$ 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 $1 = q_1 \cdot \cdots \cdot q_m$, значит $m = 0$.

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

Это доказывает единственность разложения. ☐

3 Идеалы и морфизмы

Теорема 16. *Пусть даны $I \lhd R$ 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 соответствующей аксиоме и определениях ранее.

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

- $\varphi(a + b) = \varphi(a) + \varphi(b)$;

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

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

Утверждение 17. *Композиция гомоморфизмов — гомоморфизм.*

Определение 21. Пусть $f : X \to Y$. Несложно видеть, что f раскладывается 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.

$$\begin{tikzcd}
X \arrow[rr, "f"] \arrow[dr, "f"'] & & Y \\
& f(X) = \mathrm{Im}(f) \arrow[ur, hook, "id"'] &
\end{tikzcd}$$

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

Утверждение 18. *Ядро гомоморфизма — двусторонний идеал.*

Определение 23. $\varphi : S \to R$ — *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 — область 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 (о гомоморфизме)**.** *Пусть $\varphi : R \to S$ — гомоморфизм. (Вспомним, что* $\mathrm{Ker}(\varphi) \triangleleft R$, *а* $\mathrm{Im}(\varphi) = \varphi(R)$.*) Тогда* $R/\mathrm{Ker}(\varphi) \cong \mathrm{Im}(\varphi)$, *где изоморфизм переводит* $[a] \mapsto \varphi(a)$.

$$\begin{tikzcd}
R \arrow[r, "\varphi"] \arrow[d, "r \mapsto [r]"'] & S \\
R/\mathrm{Ker}(\varphi) \arrow[r, "\sim", "{[r] \mapsto \varphi(r)}"'] & \mathrm{Im}(\varphi) \arrow[u, hook, "id"']
\end{tikzcd}$$

Доказательство.

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

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

2. Заметим, что работают следующие операции:

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

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

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

$\square$

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

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

$$\mathbb{Z}/m_1 \ldots m_k \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

Доказательство. По индукции по k с помощью КТО для двух чисел. $\square$

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

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & S \\
& R/I \arrow[ur, "\varphi'"'] &
\end{tikzcd}$$

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

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

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

$\square$

Определение 25. Пусть R — область целостности. Тогда рассмотрим $Q = R \times (R \setminus \{0\})$ и отношение $\sim$ на Q, что $(a; b) \sim (c; d) \Leftrightarrow ad = bc$. Несложно видеть, что $\sim$ — отношение эквивалентности. Тогда *полем частных* области целостности R называется $\operatorname{Frac}(R) = Q/\sim$, где операции:

- $[(a; b)] + [(c; d)] := [(ad + bc; bd)]$;

- $[(a;b)]\cdot[(c;d)] := [(ac;bd)]$;
- $0 := [(0;1)]$;
- $-[(a;b)] := [(-a;b)]$;
- $1 := [(1;1)]$;
- $[(a;b)]^{-1} = [(b;a)]$.

Несложно видеть, что все операции корректны, а поле частных — поле.

Замечание 6. Есть нативный инъективный гомоморфизм из R в $\mathrm{Frac}(R)$:

$$\varphi : R \to \mathrm{Frac}(R), r \mapsto [(r;1)]$$

Теорема 25 (Уникальное свойтсво поля частных)**.** *Пусть R — область целостности, F — поле, $\varphi : R \to F$ — инъективный гомоморфизм, сохраняющий 1, $\pi : R \to \mathrm{Frac}(R)$ — нативный гомоморфизм. Тогда существует единственный гомоморфизм $\varphi' : \mathrm{Frac}(R) \to F$, что $\varphi' \circ \pi = \varphi$.*

$$\begin{tikzcd} R \arrow[rr, hook, "\varphi"] \arrow[dr, hook, "\pi"'] & & F \\ & \mathrm{Frac}(R) \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

Замечание 7. Если $\varphi : E \to F$ — гомоморфизм полей, сохраняющий 1, то он инъективен. Действительно, $\mathrm{Ker}(\varphi)$ — идеал, значит 0 или E, так как E поле, но случай E не подходит, так как не сохраняется 0, значит $\mathrm{Ker}(\varphi) = 0$, значит φ инъективно.

Доказательство.

Лемма 25.1. $\varphi'(1/b) = 1/\varphi'(b)$

Доказательство. По замечанию 7 φ' — инъективен, но $\varphi'(0) = 0$, а тогда для всякого $a \neq 0$ верно, что $\varphi'(a) \neq 0$, значит $\varphi'(a)\cdot\varphi'(a^{-1}) = \varphi'(1) = 1$, значит $\varphi'(a)^{-1} = \varphi'(a^{-1})$. □

Лемма 25.2. $\varphi'(a/b) = \varphi'(a)/\varphi'(b)$.

Доказательство. $\varphi'(a/b) = \varphi'(a)\cdot\varphi'(b^{-1}) = \varphi'(a)\cdot\varphi'(b)^{-1} = \varphi'(a)/\varphi'(b)$. □

Заметим, что $\varphi'(a) = \varphi'(\pi(a)) = \varphi(a)$, поэтому $\varphi'(a/b) = \varphi(a)/\varphi(b)$ — это означает единственность φ'.

Теперь рассмотрим соответствующую $\varphi' : a/b \mapsto \varphi(a)/\varphi(b)$. Проверим корректность:

$$\frac{a}{b} = \frac{c}{d} \quad\Rightarrow\quad ad = bc \quad\Rightarrow\quad \varphi(ad) = \varphi(bc) \quad\Rightarrow$$
$$\varphi(a)\varphi(d) = \varphi(b)\varphi(c) \quad\Rightarrow\quad \frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(c)}{\varphi(d)} \quad\Rightarrow\quad \varphi'\left(\frac{a}{b}\right) = \varphi'\left(\frac{c}{d}\right)$$

Теперь проверим согласованность с операциями:

- $$\varphi'\left(\frac{a}{b}\cdot\frac{c}{d}\right) = \frac{\varphi(ac)}{\varphi(bd)} = \frac{\varphi(a)}{\varphi(b)}\cdot\frac{\varphi(c)}{\varphi(d)} = \varphi'\left(\frac{a}{b}\right)\cdot\varphi'\left(\frac{c}{d}\right);$$
- $$\varphi'\left(\frac{a}{b}+\frac{c}{d}\right) = \varphi'\left(\frac{ad+bc}{bd}\right) = \frac{\varphi(ad+bc)}{\varphi(bd)} =$$
$$\frac{\varphi(a)\varphi(d)+\varphi(b)\varphi(c)}{\varphi(b)\varphi(d)} = \frac{\varphi(a)}{\varphi(b)} + \frac{\varphi(c)}{\varphi(d)} = \varphi'\left(\frac{a}{b}\right) + \varphi'\left(\frac{c}{d}\right)$$

□

4 Многочлены

Теорема 26. *Пусть дано кольцо R. Рассмотрим множество S финитных бесконечных последовательностей элементов из R; т.е. все такие последовательности $(a_n)_{n=0}^{\infty}$, что всякое $a_n \in R$ и есть такое N, что для всякого $n > N$ верно, что $a_n = 0_R$. Также рассмотрим операции сложения и умножения на S:*

$$+ : S^2 \to S, ((a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty}) \mapsto (a_n + b_n)_{n=0}^{\infty} \quad \cdot : S^2 \to S, ((a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty}) \mapsto \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right)_{n=0}^{\infty}$$

Тогда

1. *S является кольцом, где $+$ — операция сложения, $\cdot$ — операция умножения, $(0_R)_{n=0}^{\infty}$ — нейтральный по сложению элемент.*

2. *S наследует от R аксиомы M_1, M_2 и M_3.*

3. *R изоморфно подкольцу S, состоящему из элементов вида $(a, 0, 0, \dots)$, где $a \in R$.*

Определение 26. Множество S из прошлой теоремы называется *кольцом многочленов над R* и обозначается $R[x]$. При этом всякий его элемент $(a_n)_{n=0}^{\infty}$ обозначается как $a_0 + \dots + a_n x^n + \dots = \sum_{n=0}^{\infty} a_n x^n$.

Доказательство.

1. Важно сказать, что из A_1 следует корректность определения умножения. Проверим аксиомы:

   A_1) $\forall (a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty}, (c_n)_{n=0}^{\infty} \in S$:

$$\begin{aligned}((a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty}) + (c_n)_{n=0}^{\infty} &= (a_n + b_n)_{n=0}^{\infty} + (c_n)_{n=0}^{\infty} \\ &= ((a_n + b_n) + c_n)_{n=0}^{\infty} \\ &= (a_n + (b_n + c_n))_{n=0}^{\infty} \\ &= (a_n)_{n=0}^{\infty} + (b_n + c_n)_{n=0}^{\infty} \\ &= (a_n)_{n=0}^{\infty} + ((b_n)_{n=0}^{\infty} + (c_n)_{n=0}^{\infty})\end{aligned}$$

   A_2) $\forall (a_n)_{n=0}^{\infty} \in R$:

$$\begin{aligned}(a_n)_{n=0}^{\infty} + (0)_{n=0}^{\infty} &= (a_n + 0)_{n=0}^{\infty} \\ &= (a_n)_{n=0}^{\infty} \\ &= (0 + a_n)_{n=0}^{\infty} \\ &= (0)_{n=0}^{\infty} + (a_n)_{n=0}^{\infty}\end{aligned}$$

   A_3) $\forall (a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty} \in R$:

$$\begin{aligned}(a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty} &= (a_n + b_n)_{n=0}^{\infty} \\ &= (b_n + a_n)_{n=0}^{\infty} \\ &= (b_n)_{n=0}^{\infty} + (a_n)_{n=0}^{\infty}\end{aligned}$$

A$_4$) $\forall (a_n)_{n=0}^{\infty} \in R$:

$$\begin{aligned}(a_n)_{n=0}^{\infty} + (-a_n)_{n=0}^{\infty} &= (a_n + -a_n)_{n=0}^{\infty}\\ &= (0)_{n=0}^{\infty}\\ &= (-a_n + a_n)_{n=0}^{\infty}\\ &= (-a_n)_{n=0}^{\infty} + (a_n)_{n=0}^{\infty}\end{aligned}$$

D) $\forall (a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty}, (k_n)_{n=0}^{\infty} \in R$:

$$\begin{aligned}(k_n)_{n=0}^{\infty}((a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty}) &= (k_n)_{n=0}^{\infty} \cdot (a_n + b_n)_{n=0}^{\infty}\\ &= \left(\sum_{t=0}^{n} k_t(a_{n-t} + b_{n-t})\right)_{n=0}^{\infty}\\ &= \left(\sum_{t=0}^{n} k_t \cdot a_{n-t} + \sum_{t=0}^{n} k_t \cdot b_{n-t}\right)_{n=0}^{\infty}\\ &= \left(\sum_{t=0}^{n} k_t \cdot a_{n-t}\right)_{n=0}^{\infty} + \left(\sum_{t=0}^{n} k_t \cdot b_{n-t}\right)_{n=0}^{\infty}\\ &= (k_n)_{n=0}^{\infty}(a_n)_{n=0}^{\infty} + (k_n)_{n=0}^{\infty}(b_n)_{n=0}^{\infty}\end{aligned}$$

и

$$\begin{aligned}((a_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty})(k_n)_{n=0}^{\infty} &= (a_n + b_n)_{n=0}^{\infty} \cdot (k_n)_{n=0}^{\infty}\\ &= \left(\sum_{t=0}^{n}(a_{n-t} + b_{n-t})k_t\right)_{n=0}^{\infty}\\ &= \left(\sum_{t=0}^{n} a_{n-t} \cdot k_t + \sum_{t=0}^{n} b_{n-t} \cdot k_t\right)_{n=0}^{\infty}\\ &= \left(\sum_{t=0}^{n} a_{n-t} \cdot k_t\right)_{n=0}^{\infty} + \left(\sum_{t=0}^{n} b_{n-t} \cdot k_t\right)_{n=0}^{\infty}\\ &= (a_n)_{n=0}^{\infty}(k_n)_{n=0}^{\infty} + (b_n)_{n=0}^{\infty}(k_n)_{n=0}^{\infty}\end{aligned}$$

2. Проверим наследственность для каждой аксиомы:

M$_1$) $\forall (a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty}, (c_n)_{n=0}^{\infty} \in R:$

$$\begin{aligned}
((a_n)_{n=0}^{\infty} \cdot (b_n)_{n=0}^{\infty}) \cdot (c_n)_{n=0}^{\infty} &= \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right)_{n=0}^{\infty} \cdot (c_n)_{n=0}^{\infty} \\
&= \left(\sum_{k=0}^{n} \left(\sum_{l=0}^{k} a_l \cdot b_{k-l}\right) \cdot c_{n-k}\right)_{n=0}^{\infty} \\
&= \left(\sum_{\substack{0\leqslant k \\ l\leqslant 0 \\ k+l\leqslant n}} (a_k \cdot b_l) \cdot c_{n-k-l}\right)_{n=0}^{\infty} \\
&= \left(\sum_{\substack{0\leqslant k \\ l\leqslant 0 \\ k+l\leqslant n}} a_k \cdot (b_l \cdot c_{n-k-l})\right)_{n=0}^{\infty} \\
&= \left(\sum_{k=0}^{n} a_{n-k} \cdot \left(\sum_{l=0}^{k} b_l \cdot c_{k-l}\right)\right)_{n=0}^{\infty} \\
&= (a_n)_{n=0}^{\infty} \cdot \left(\sum_{k=0}^{n} b_k \cdot c_{n-k}\right)_{n=0}^{\infty} \\
&= (a_n)_{n=0}^{\infty} \cdot ((b_n)_{n=0}^{\infty} \cdot (c_n)_{n=0}^{\infty})
\end{aligned}$$

M$_2$) Обозначим за 1 в S последовательность $(t_n)_{n=0}^{\infty}$, где $t_0 = 1$, а все остальные члены равны 0. Тогда $\forall (a_n)_{n=0}^{\infty} \in R:$

$$\begin{aligned}
(a_n)_{n=0}^{\infty} \cdot 1 &= \left(\sum_{k=0}^{n} a_k \cdot t_{n-k}\right)_{n=0}^{\infty} \\
&= (a_n)_{n=0}^{\infty} \\
&= \left(\sum_{k=0}^{n} t_{n-k} \cdot a_k\right)_{n=0}^{\infty} \\
&= 1 \cdot (a_n)_{n=0}^{\infty}
\end{aligned}$$

M$_3$) $\forall (a_n)_{n=0}^{\infty}, (b_n)_{n=0}^{\infty} \in R:$

$$\begin{aligned}
(a_n)_{n=0}^{\infty} \cdot (b_n)_{n=0}^{\infty} &= \left(\sum_{k=0}^{n} a_k \cdot b_{n-k}\right)_{n=0}^{\infty} \\
&= \left(\sum_{k=0}^{n} b_k \cdot a_{n-k}\right)_{n=0}^{\infty} \\
&= (b_n)_{n=0}^{\infty} \cdot (a_n)_{n=0}^{\infty}
\end{aligned}$$

3. Рассмотрим отображение $\varphi : R \to S, a \mapsto (a, 0, 0, \dots)$. Тогда

- $\varphi(a) + \varphi(b) = (a + b, 0, \dots) = \varphi(a + b)$

- $\varphi(a) \cdot \varphi(b) = (ab, 0, \dots) = \varphi(a \cdot b)$
- $\varphi(0) = (0, 0, \dots) = 0$
- (в случае M_2) $\varphi(1) = (1, 0, \dots) = 1$

Значит $\mathrm{Ker}(\varphi) = \{0\}$, $R \cong \mathrm{Im}(\phi)$. При этом несложно видеть, что $\mathrm{Im}(\phi)$ и есть множество всех последовательностей вида $(a, 0, 0, \dots)$.

$\square$

5 Теория категорий

Определение 27. *Категория* C есть совокупность семейства (не обязательно множества) объектов $\mathrm{Ob}(C)$ и семейства *морфизмов* (также “arrows”), что выполнены следующие условия.

1. У всякого морфизма f есть прообраз (также “начало”, “source”, “domain”; обозначение: $s(f)$ или $\mathrm{dom}(f)$) и образ (также “конец”, “target”, “codomain”; обозначение: $t(f)$ или $\mathrm{cod}(f)$), являющиеся объектами из рассмотренного семейства. Семейства всех морфизмов из X в Y (т.е. с прообразом X и образом Y) обозначается $\mathrm{Hom}(X, Y)$ или $\mathrm{Mor}(X, Y)$.

2. На семействе морфизмов введён не полностью определённый бинарный оператор $\circ$ (можно считать, функциональное отношение из $M \times M$ в M, где M — семейство морфизмов), что для всяких $X, Y, Z \in \mathrm{Ob}(C)$ и $f \in \mathrm{Hom}(X, Y)$, $g \in \mathrm{Mor}(Y, Z)$ значение $g \circ f$ определено и лежит в $\mathrm{Hom}(X, Z)$. Данный оператор называется *композицией*, а $g \circ f$ — композицией g и f.

3. Операция композиции морфизмов ассоциативна: для всяких $X, Y, Z, T \in \mathrm{Ob}(C)$ и $f \in \mathrm{Hom}(X, Y)$, $g \in \mathrm{Hom}(Y, Z)$, $h \in \mathrm{Hom}(Z, T)$
$$(f \circ g) \circ h = f \circ (g \circ h).$$

4. Для всякого $X \in \mathrm{Ob}(C)$ есть выделенный морфизм $\mathrm{id}_X \in \mathrm{Hom}(X, X)$ (также 1_X). Он называется тождественным морфизмом X.

5. Для всяких $X, Y \in \mathrm{Ob}(C)$ для всякого $f \in \mathrm{Hom}(X, Y)$ верно, что
$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$

Пример 9.

1. Sets (Ens):
   - $\mathrm{Ob}(\mathrm{Sets})$ — все множества,
   - $\mathrm{Hom}(X, Y)$ — все отображения из X в Y,
   - $\circ$ — обычная композиция отображений,
   - id_X — тождественное отображение $X \to X$.

2. Groups:
   - $\mathrm{Ob}(\mathrm{Groups})$ — все группы,
   - $\mathrm{Hom}(G, H)$ — все гомоморфизмы $G \to H$,
   - $\circ$ — обычная композиция гомоморфизмов,
   - id_G — тождественный гомоморфизм $G \to G$.

3. Аналогично описываются категории Rings колец, CommRings коммутативных колец (если в случаях Rings и CommRings рассматриваются кольца с единицей, то надо требовать, чтобы гомоморфизмы переводили единицу в единицу), Vect_F векторных пространств над полем F, $R - \mathrm{Mod}$ R-модулей, и т.д. для всякой алгебраической структуры.

4. Top:
   - $\mathrm{Ob}(\mathrm{Top})$ — все топологические пространства,

- $\mathrm{Hom}(G, H)$ — все непрерывные отображения,
- $\circ$ — обычная композиция отображений,
- id_G — тождественное отображение $G \to G$.

5. HTop:

   - $\mathrm{Ob}(\mathrm{HTop})$ — все “хорошие” (компактно порождённые) топологические пространства,
   - $\mathrm{Hom}(G, H)$ — все непрерывные отображения по модулю гомотопии,
   - $\circ$ — обычная композиция отображений,
   - id_G — тождественное отображение $G \to G$.

6. $\mathrm{Ob}(C) = \{X\}$. В таком случае мы получаем *моноид* некоторых отображений X на себя: у нас есть множество морфизмов X на себя с операцией композиции (произведение в моноиде), которая ассоциативна и имеет нейтральный элемент (но не обязательно обратима).

7. Частичный предпорядок задаёт категорию:

   - $\mathrm{Ob}(C) = M$,
   - $\mathrm{Hom}(x, y) = \begin{cases} \{\star_{x\to y}\} \text{ если } x \leqslant y, \\ \varnothing \text{ иначе}, \end{cases}$
   - $\star_{y\to z} \circ \star_{x\to y} := \star_{x\to z}$,
   - $\mathrm{id}_x := \star_{x\to x}$.

8. Rels — категория отношений:

   - $\mathrm{Ob}(\mathrm{Rels})$ — все множества;
   - $\mathrm{Hom}(X, Y)$ — все подмножества $X \times Y$;
   - для всяких $S \in \mathrm{Hom}(X, Y)$ и $R \in \mathrm{Hom}(Y, Z)$

   $$R \circ S := \{(x, z) \in X \times Z \mid \exists y \in Y : \qquad (x, y) \in S \land (y, z) \in R\};$$

   - $\mathrm{id}_X := \{(x, x)\}_{x\in X}$.

9. Пустая категория: нет объектов, нет морфизмов.

10. Категория с единственным объектом и единственным тождественным морфизмом на нём.

11. Дискретная категория: нет нетождественных морфизмов.

Определение 28. $X, Y \in \mathrm{Ob}(C)$ называются *изоморфными*, если есть $f \in \mathrm{Hom}(X, Y)$ и $g \in \mathrm{Hom}(Y, X)$, что

$$f \circ g = \mathrm{id}_Y \qquad \text{и} \qquad g \circ f = \mathrm{id}_X.$$

Определение 29. *Подкатегория* S категории C — категория, семейства объектов и морфизмов которой суть подсемейства объектов и морфизмов категории C соответственно.