

Алгебра.

Лектор — В. А. Петров

Создатель конспекта — Глеб Минаев *

TODOs

Содержание

1 Основные понятия.	1
2 Теория делимости	3
3 Идеалы и морфизмы	6
4 Многочлены	10
5 Теория категорий	15
5.1 Мономорфизмы и эпиморфизмы	22

Литература:

- Ван дер Варден, “Алгебра”.
- Лэнг, “Алгебра”.
- Винберг, “Курс Алгебры”.
- Маклейн, “Категории для работающего математика”.

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 $(M, + : M^2 \rightarrow M)$ с аксиомами:

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

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

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

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

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

Определение 3. Опишем следующие аксиомы на наборе $(M, + : M^2 \rightarrow M, \cdot : M^2 \rightarrow M)$ в добавок к A_1, \dots, 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 “ \mid ” 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 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 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 R — кольцо. $I \subseteq R$ 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 (ОГИ)* — 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 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 $\varphi(a) \geq \varphi(b)$, иначе поменяем их местами. Тем самым по аксиоме Евклида найдутся q и r , что $a = bq + r$, а $\varphi(r) < \varphi(b) \leq \varphi(a)$, значит $\varphi(a) + \varphi(b) > \varphi(r) + \varphi(b)$. При этом $(a, b) = (r, b)$. Значит бесконечно $\varphi(a) + \varphi(b)$ не может 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 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 $N(a) \geq N(b)$. 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 $N(a) + N(b) \geq N(b) + N(b) > N(b) + N(r)$. 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 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 неделимых единицы a и b . Тогда $\text{WLOG } p \mid a$. 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 (АПСС), если не существует последовательности $d_0R \subsetneq d_1R \subsetneq \dots$. 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. $a_{n+1} \mid a_n \wedge a_n \not\sim a_{n+1}$). 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

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 $a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \dots$ — противоречие. \square

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 $a_0R \subsetneq a_1R \subsetneq a_2R \subsetneq \dots$ — противоречие. \square

Это доказывает существование разложения.

Лемма 15.3. Если $p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$ для простых $p_1, \dots, p_n, q_1, \dots, q_m$, 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. \square

Это доказывает единственность разложения. \square

3 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 $a \sim b$;
- $a \sim b$, $b \sim c$, 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:

- A₁) $\forall a, b, c \in R : ([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$
- A₂) $\forall a \in R : [a] + [0] = [a + 0] = a = [0 + a] = [0] + [a]$
- A₃) $\forall a, b \in R : [a] + [b] = [a + b] = [b + a] = [b] + [a]$
- A₄) $\forall a \in R : [a] + -[a] = [a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a] = -[a] + [a]$
- D) $\forall a, b, k \in R : [k]([a] + [b]) = [k][a + b] = [k(a + b)] = [ka + kb] = [ka] + [kb] = [k][a] + [k][b]$,
 $([a] + [b])[k] = [a + b][k] = [(a + b)k] = [ak + bk] = [ak] + [bk] = [a][k] + [b][k]$
- M₁) $\forall a, b, c \in R : ([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot [b \cdot c] = [a] \cdot ([b] \cdot [c])$
- M₂) $\forall a \in R : [a] \cdot [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \cdot [a]$
- M₃) $\forall a, b \in R : [a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$
- M₄) $\forall a \in R \setminus \{0\} : [a] \cdot [a]^{-1} = [a] \cdot [a^{-1}] = [a \cdot a^{-1}] = [1] = [a^{-1} \cdot a] = [a^{-1}] \cdot [a] = [a]^{-1} \cdot [a]$

□

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

Определение 20. Гомоморфизм — такое отображение $\varphi : R \rightarrow S$ — 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 $f : X \rightarrow Y$. Несложно видеть, что f раскладывается в композицию сюръекции $f : X \rightarrow f(X)$ и инъекции $id : f(X) \rightarrow Y$. Тогда $\text{Im}(f) = \{f(x) \mid x \in X\}$ — 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 .

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \searrow f & \nearrow id \\ & f(X) = \text{Im}(f) & \end{array}$$

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

Утверждение 18. Ядро гомоморфизма — двусторонний идеал.

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

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ r \mapsto [r] \downarrow & & \uparrow id \\ R / \text{Ker}(\varphi) & \xrightarrow[\substack{\sim \\ [r] \mapsto \varphi(r)}]{} & \text{Im}(\varphi) \end{array}$$

Доказательство.

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

Замечание 5. Классы эквивалентности по $\text{Ker}(\varphi)$ 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 $\text{Im}(\varphi)$ 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 $\varphi : \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, [a]_{mn} \mapsto ([a]_m; [a]_n)$. Несложно заметить, что ядро φ тривиально, поэтому $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z} / \text{Ker}(\varphi) \cong \text{Im}(\varphi)$. Но в последнем элементов не менее mn , так как $\text{Im}(\varphi) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, но и не более, так как $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn$, поэтому $\text{Im}(\varphi) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, поэтому $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. □

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

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ & \searrow \pi & \nearrow \varphi' \\ & R/I & \end{array}$$

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:

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

□

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 $\text{Frac}(R) = Q / \sim$, 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 $\text{Frac}(R)$:

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

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

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & F \\ & \searrow \pi \quad \nearrow \varphi' & \\ & \text{Frac}(R) & \end{array}$$

Замечание 7. Если $\varphi : E \rightarrow F$ — гомоморфизм полей, сохраняющий 1, то он инъективен. Действительно, $\text{Ker}(\varphi)$ — идеал, значит 0 или E , так как E поле, но случай E не подходит, так как не сохраняется 0, значит $\text{Ker}(\varphi) = 0$, 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 $\varphi'(a)^{-1} = \varphi'(a^{-1})$. \square

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

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

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:

$$\begin{aligned} \frac{a}{b} = \frac{c}{d} & \Rightarrow ad = bc & \Rightarrow \varphi(ad) = \varphi(bc) & \Rightarrow \\ \varphi(a)\varphi(d) = \varphi(b)\varphi(c) & \Rightarrow \frac{\varphi(a)}{\varphi(b)} = \frac{\varphi(c)}{\varphi(d)} & \Rightarrow \varphi'\left(\frac{a}{b}\right) = \varphi'\left(\frac{c}{d}\right) \end{aligned}$$

Теперь проверим согласованность с операциями:

•

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

•

$$\begin{aligned} \varphi'\left(\frac{a}{b} + \frac{c}{d}\right) &= \varphi'\left(\frac{ad + bc}{bd}\right) = \frac{\varphi(ad + bc)}{\varphi(bd)} = \\ &= \frac{\varphi(a)\varphi(d) + \varphi(b)\varphi(c)}{\varphi(b)\varphi(d)} = \frac{\varphi(a)}{\varphi(b)} + \frac{\varphi(c)}{\varphi(d)} = \varphi'\left(\frac{a}{b}\right) + \varphi'\left(\frac{c}{d}\right) \end{aligned}$$

\square

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 :

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

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:

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

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

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

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

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

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

A₄) $\forall (a_n)_{n=0}^\infty \in R :$

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

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:

M₁) $\forall (a_n)_{n=0}^\infty, (b_n)_{n=0}^\infty, (c_n)_{n=0}^\infty \in R :$

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

M₂) Обозначим за 1 в S последовательность $(t_n)_{n=0}^\infty$, где $t_0 = 1$, а все остальные члены равны 0. Тогда $\forall (a_n)_{n=0}^\infty \in R :$

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

M₃) $\forall (a_n)_{n=0}^\infty, (b_n)_{n=0}^\infty \in R :$

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

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

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

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

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

□

5 Теория категорий

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

1. У всякого морфизма f есть прообраз (также “начало”, “source”, “domain”; обозначение: $s(f)$ или $\text{dom}(f)$) и образ (также “конец”, “target”, “codomain”; обозначение: $t(f)$ или $\text{cod}(f)$), являющиеся объектами из рассмотренного семейства. Семейства всех морфизмов из X в Y (т.е. с прообразом X и образом Y) обозначается $\text{Hom}(X, Y)$ или $\text{Mor}(X, Y)$.
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 $X, Y, Z \in \text{Ob}(C)$ и $f \in \text{Hom}(X, Y)$, $g \in \text{Mor}(Y, Z)$ значение $g \circ f$ определено и лежит в $\text{Hom}(X, Z)$. Данный оператор называется *композицией*, а $g \circ f$ — композицией g и f .
3. Операция композиции морфизмов ассоциативна: для всяких $X, Y, Z, T \in \text{Ob}(C)$ и $f \in \text{Hom}(X, Y)$, $g \in \text{Hom}(Y, Z)$, $h \in \text{Hom}(Z, T)$

$$(f \circ g) \circ h = f \circ (g \circ h).$$

4. Для всякого $X \in \text{Ob}(C)$ есть выделенный морфизм $\text{id}_X \in \text{Hom}(X, X)$ (также 1_X). Он называется тождественным морфизмом X .
5. Для всяких $X, Y \in \text{Ob}(C)$ для всякого $f \in \text{Hom}(X, Y)$ верно, что

$$f \circ \text{id}_X = f = \text{id}_Y \circ f.$$

Пример 9.

1. $\text{Sets} (\text{Ens})$:

- $\text{Ob}(\text{Sets})$ — все множества,
- $\text{Hom}(X, Y)$ — все отображения из X в Y ,
- \circ — обычная композиция отображений,
- id_X — тождественное отображение $X \rightarrow X$.

2. Sets_* :

- $\text{Ob}(\text{Sets}_*)$ — пары (A, a) , где A — любое множество, а $a \in A$,
- $\text{Hom}((A, a), (B, b))$ — все отображения из A в B , переводящие a в b ,
- \circ — обычная композиция отображений,
- id_A — тождественное отображение $A \rightarrow A$.

3. Groups :

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

4. 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 , $R - \text{Mod}$ R -модулей, и т.д. для всякой алгебраической структуры.

5. Top:

- $\text{Ob}(\text{Top})$ — все топологические пространства,
- $\text{Hom}(X, Y)$ — все непрерывные отображения $X \rightarrow Y$,
- \circ — обычная композиция отображений,
- id_X — тождественное отображение $X \rightarrow X$.

6. Top*:

- $\text{Ob}(\text{Top}^*)$ — пары вида (X, x) , где X — топологическое пространство, а $x \in X$,
- $\text{Hom}((X, x), (Y, y))$ — все непрерывные отображения $X \rightarrow Y$, переводящие x в y ,
- \circ — обычная композиция отображений,
- $\text{id}_{(X, x)}$ — тождественное отображение $X \rightarrow X$.

7. HTop:

- $\text{Ob}(\text{HTop})$ — все “хорошие” (компактно порождённые) топологические пространства,
- $\text{Hom}(X, Y)$ — все непрерывные отображения по модулю гомотопии,
- \circ — обычная композиция отображений,
- id_X — тождественное отображение $X \rightarrow X$.

8. $\text{Ob}(C) = \{X\}$. 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).

9. Частичный предпорядок задаёт категорию:

- $\text{Ob}(C) = M$,
- $\text{Hom}(x, y) = \begin{cases} \{\star_{x \rightarrow y}\} & \text{если } x \leq y, \\ \emptyset & \text{иначе,} \end{cases}$
- $\star_{y \rightarrow z} \circ \star_{x \rightarrow y} := \star_{x \rightarrow z}$,
- $\text{id}_x := \star_{x \rightarrow x}$.

10. Rels — категория отношений:

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

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

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

11. Пустая категория: нет объектов, нет морфизмов.

12. Категория с единственным объектом и единственным тождественным морфизмом на нём.
13. Дискретная категория: нет нетождественных морфизмов.
14. *Произведение* категорий C и D — категория H , где $\text{Ob}(H) = \text{Ob}(C) \times \text{Ob}(D)$, а для всяких $X = (X_C, X_D), Y = (Y_C, Y_D) \in H$ $\text{Hom}(X, Y) = \text{Hom}(X_C, Y_C) \times \text{Hom}(X_D, Y_D)$. При этом $(f_C, f_D) \circ (g_C, g_D) := (f_C \circ g_C, f_D \circ g_D)$, а $\text{id}_{(X_C, X_D)} := (\text{id}_{X_C}, \text{id}_{X_D})$.

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

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

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

Определение 30. Объект A категории C называется

- *инициальным*, если для всякого $X \in \text{Ob}(C)$ существует единственный морфизм $A \rightarrow X$,
- *терминальным*, если для всякого $X \in \text{Ob}(C)$ существует единственный морфизм $X \rightarrow A$.

Лемма 27. *Инициальный и терминальный объекты не более чем единственны с точностью до изоморфизма (даже, точнее говоря, с точностью до единственного изоморфизма).*

Доказательство. Пусть A и B являются инициальными объектами. Тогда id_A — единственный морфизм $A \rightarrow A$ (по инициальности A), а id_B — единственный морфизм $B \rightarrow B$. Также по инициальности A и B есть морфизмы $f \in \text{Hom}(A, B)$ и $g \in \text{Hom}(B, A)$. При этом $g \circ f$ — морфизм A , т.е. $g \circ f = \text{id}_A$, и по аналогии $f \circ g = \text{id}_B$. Следовательно A и B изоморфны по определению. Значит все инициальные объекты изоморфны.

$$\text{id}_A \curvearrowright A \xrightleftharpoons[g]{f} B \curvearrowleft \text{id}_B$$

Причём изоморфизм единственен. Так как если есть два изоморфизма: один образован f_1 и g_1 , а второй — f_2 и g_2 , то $f_2 \circ g_1$ — морфизм $A \rightarrow A$, а значит равен id_A . Следовательно

$$f_2 = f_2 \circ \text{id}_B = f_2 \circ (g_1 \circ f_1) = (f_2 \circ g_1) \circ f_1 = \text{id}_A \circ f_1 = f_1;$$

аналогично $g_1 = g_2$.

Утверждение для терминальных объектов доказывается аналогично. □

Определение 31. *Противоположная (двойственная) категория* категории C — категория C^{op} , где

- $\text{Ob}(C^{\text{op}}) := \text{Ob}(C)$,
- $\text{Hom}_{C^{\text{op}}}(X, Y) := \text{Hom}_C(X, Y)$,
- $\text{dom}_{C^{\text{op}}}(f) := \text{cod}_C(f)$, $\text{cod}_{C^{\text{op}}}(f) := \text{dom}_C(f)$,
- $f \circ_{C^{\text{op}}} g := g \circ f$.

Замечание. Инициальные объекты суть двойственны терминальным объектам в двойственном пространстве.

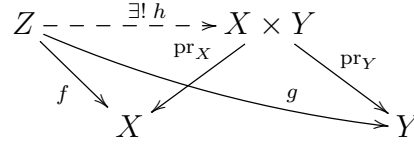
Существование двойственных категорий значит, что всякая теорема без условий, зависящих от инициальности (терминальности) объектов, и верная для инициальных объектов, верна и для терминальных объектов (и наоборот).

Пример 10.

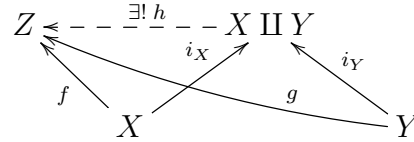
1. В \mathbf{Sets} инициальным является только пустое множество, а терминальным — любое одноэлементное множество.
2. В \mathbf{Vect}_F единственным инициальным и единственным терминальным является 0-мерное пространство.
3. В \mathbf{Top} — тоже самое, что и для \mathbf{Sets} .
4. В \mathbf{Top}_* инициальные и терминальные объекты — одноточечные пространства.
5. В категории порождённой частичным предпорядком инициальный и терминальный объекты — наименьший и наибольший элементы соответственно (если существуют).

Определение 32. Пусть фиксированы объекты X и Y категории C .

- *Произведением* (также “product”) объектов X и Y называется объект $X \times Y \in \mathbf{Ob}(C)$ и морфизмы $\text{pr}_X \in \mathbf{Hom}(X \times Y, X)$ и $\text{pr}_Y \in \mathbf{Hom}(X \times Y, Y)$, что для всякого объекта $Z \in \mathbf{Ob}(C)$, у которого есть морфизмы $f \in \mathbf{Hom}(Z, X)$ и $g \in \mathbf{Hom}(Z, Y)$, существует единственный морфизм $h \in \mathbf{Hom}(Z, X \times Y)$, что $f = \text{pr}_X \circ h$ и $g = \text{pr}_Y \circ h$.



- *Копроизведением* (также “coproduct” или “categorical sum”) объектов X и Y называется объект $X \amalg Y \in \mathbf{Ob}(C)$ (или также обозначается $X \oplus Y$) и морфизмы $i_X \in \mathbf{Hom}(X, X \amalg Y)$ и $i_Y \in \mathbf{Hom}(Y, X \amalg Y)$, что для всякого объекта $Z \in \mathbf{Ob}(C)$, у которого есть морфизмы $f \in \mathbf{Hom}(X, Z)$ и $g \in \mathbf{Hom}(Y, Z)$, существует единственный морфизм $h \in \mathbf{Hom}(X \amalg Y, Z)$, что $f = h \circ i_X$ и $g = h \circ i_Y$.

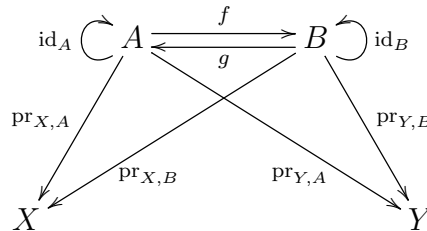


Лемма 28. Для всяких $X, Y \in \mathbf{Ob}(C)$ их произведение и копроизведение не более чем единственны с точностью до изоморфизма.

Доказательство. Пусть A и B суть произведения X и Y . Так как A — произведение X и Y , то значит есть единственный морфизм $h \in \mathbf{Hom}(A, A)$, что $\text{pr}_{X,A} = h \circ \text{pr}_{X,A}$ и $\text{pr}_{Y,A} = h \circ \text{pr}_{Y,A}$; и этот морфизм — id_A . При этом $f \circ \text{pr}_{X,B} = \text{pr}_{X,A}$, а $g \circ \text{pr}_{Y,A} = \text{pr}_{X,B}$, следовательно

$$\text{pr}_{X,A} = f \circ \text{pr}_{X,B} = (f \circ g) \circ \text{pr}_{X,A}; \quad \text{аналогично} \quad \text{pr}_{Y,A} = (f \circ g) \circ \text{pr}_{Y,A}.$$

Следовательно $f \circ g = \text{id}_A$. Аналогично $g \circ f = \text{id}_B$.



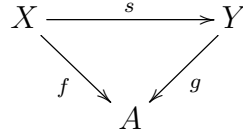
Утверждение для копроизведений доказывается аналогично. □

Пример 11.

1. В **Sets** $X \times Y$ — декартово произведение (где pr_X и pr_Y — извлечения первого и второго элемента пары соответственно), а $X \amalg Y$ — дизъюнктное объединение (где i_X и i_Y — нативные вложения).
2. В **Groups** $G \times H$ — декартово произведение групп, а $G \amalg H$ — свободное произведение.
3. В **Top** так же, как в **Sets**.
4. В **Top*** $(X, x) \times (Y, y) = (X \times Y, (x, y))$, а $(X, x) \amalg (Y, y)$ — упражнение.
5. В категории, порождённой частичным предпорядком, $x \times y = \min(x, y)$, а $x \amalg y = \max(x, y)$.

Определение 33 (категория стрелки). Пусть даны категория C и объект $A \in \text{Ob}(C)$. Тогда C/A обозначается категория, где

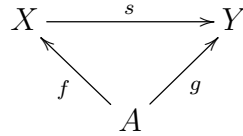
- $\text{Ob}(C/A)$ — пары вида (X, f) , где $X \in \text{Ob}(C)$, а $f \in \text{Hom}(X, A)$,
- $\text{Hom}((X, f), (Y, g))$ — морфизмы $s \in \text{Hom}(X, Y)$, что $f = s \circ g$ (осторожно: одно и то же s может быть (и будет) использовано как сразу несколько разных морфизмов в C/A , так как всё зависит от начала и конца морфизма),



- $s \circ_{C/A} t := s \circ_C t$,
- id_X — id_X из C .

С другой стороны $C \backslash A$ обозначается категория, где

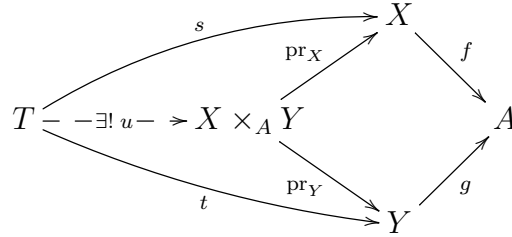
- $\text{Ob}(C \backslash A)$ — пары вида (X, f) , где $X \in \text{Ob}(C)$, а $f \in \text{Hom}(A, X)$,
- $\text{Hom}((X, f), (Y, g))$ — морфизмы $s \in \text{Hom}(X, Y)$, что $g = f \circ s$ (осторожно: одно и то же s может быть (и будет) использовано как сразу несколько разных морфизмов в C/A , так как всё зависит от начала и конца морфизма),



- $s \circ_{C \backslash A} t := s \circ_C t$,
- id_X — id_X из C .

Пример 12. В C/A терминальным объектом будет (A, id_A) .

Определение 34. Пусть даны $X, Y, A \in \text{Ob}(C)$ и фиксированы морфизмы $f \in \text{Hom}(X, A)$ и $g \in \text{Hom}(Y, A)$. Тогда если $(X, f) \times (Y, g)$ определено в $\text{Ob}(C)$ и равно (Z, h) , то Z называется *расслоённым произведением* $X \times_A Y$.



Таким образом $X \times_A Y$ — это такой объект в категории C вместе с $\text{pr}_X \in \text{Hom}(X \times_A Y, X)$ и $\text{pr}_Y \in \text{Hom}(X \times_A Y, Y)$, образующие с f и g коммутативный квадрат (так называемый “декартов квадрат”), что для всякого объекта $T \in \text{Ob}(C)$ и морфизмов $s \in \text{Hom}(T, X)$ и $t \in \text{Hom}(T, Y)$, что $s \circ f = t \circ g$, есть единственный морфизм $u \in \text{Hom}(T, X \times_A Y)$, что $s = u \circ \text{pr}_X$ и $t = u \circ \text{pr}_Y$.

Пример 13.

1. В Sets для множеств X, Y, A и отображений $f : X \rightarrow A$ и $g : Y \rightarrow A$ расслоённое произведение

$$X \times_A Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}.$$

2. В Sets^{op}

$$X \amalg_A Y = (X \sqcup Y) / \sim,$$

где \sim — отношение эквивалентности, порождённое соотношениями $f(a) \sim g(a)$.

Фактически это работает как склейка в топологии.

3. В Groups $G \times_K H$ — также как в Sets , а $G \amalg_K H$ — свободное произведение с объединённой подгруппой.

Определение 35. Пусть даны категории C и D . *Функтор* (также “ковариантный функтор”) $F : C \rightarrow D$ — совокупность “функций” $\text{Ob}(C) \rightarrow \text{Ob}(D)$ и “функций” из класса морфизмов C в класс морфизмов D , что

- для всякого морфизма $f \in \text{Hom}(X, Y)$, где $X, Y \in \text{Ob}(C)$, $F(f) \in \text{Hom}(F(X), F(Y))$,
- для всяких морфизмов f и g в C $F(f \circ g) = F(f) \circ F(g)$,
- для всякого объекта $X \in \text{Ob}(C)$ $F(\text{id}_X) = \text{id}_{F(X)}$.

Пример 14.

1. Взятие фундаментальной группы топологического порождает функтор $\pi_1 : \text{Top}^* \rightarrow \text{Groups}$.
2. Пусть M_1 и M_2 — моноиды как категории. Тогда всякий функтор $M_1 \rightarrow M_2$ — гомоморфизм моноидов.
3. Пусть M — моноид как категория. Тогда всякий функтор $M \rightarrow \text{Vect}_K$ выглядит так: единственному элементу категории M сопоставляется некоторое векторное пространство V , а функтор отображает сам моноид M в $\text{End}(V)$ (моноид по умножению) как гомоморфизм моноидов.
4. Всякий функтор между классами, порождёнными частичными предпорядками, — монотонная функция.

5. Пусть имеется категория S , состоящая из одного объекта и одного морфизма, и любая категория C . Тогда всякий функтор $S \rightarrow C$ — выбор объекта в C , а $C \rightarrow S$ — отобразить всё в данный единственный объект.
6. Функтор из категории с двумя объектами и двумя морфизмами в категорию C — выбор двух (не обязательно различных) объектов в C .
7. Функтор из категории с двумя объектами и тремя морфизмами в категорию C — выбор двух (не обязательно различных) объектов в C и морфизма между ними.
8. *Забывающий функтор* $U : \text{Groups} \rightarrow \text{Sets}$ — функтор, переводящий группу G в множество G , а гомоморфизм f в функцию f .
9. *Свободный функтор* $F : \text{Sets} \rightarrow \text{Groups}$ — функтор, где $F(X)$ — свободная группа на образующих X , а $F(f)$ — гомоморфизм, порождённый соответствием образующих f .
10. ...
11. ...
12. В случае AbGroups и Groups , то есть тривиальный *забывающий функтор* $U : \text{AbGroups} \rightarrow \text{Groups}$ и функтор $F : \text{Groups} \rightarrow \text{AbGroups}$, $G \mapsto G/[G, G]$.
13. Есть тривиальный забывающий функтор $U : \text{Sets}_* \rightarrow \text{Sets}$, $(A, a) \mapsto A$, $f \mapsto f$. При этом в обратную сторону есть функтор

$$F : \text{Sets} \rightarrow \text{Sets}_*, A \mapsto (A \sqcup \{\emptyset\}, \emptyset), f \mapsto f_* := \begin{cases} f(x), & \text{если } x \in A, \\ \emptyset, & \text{если } x = \emptyset. \end{cases}$$

14. Пусть имеется категория C и фиксирован объект $A \in \text{Ob}(C)$. Тогда можно определить функтор $F : C \rightarrow \text{Sets}$, $X \mapsto \text{Hom}(A, X)$, $f \mapsto F(f) := f \circ \varphi$.

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ & \swarrow \varphi & \nearrow F(f)(\varphi) \\ & A & \end{array}$$

Функтор F называется *копредставимым*.

Лемма 29. Пусть дан функтор $F : C \rightarrow D$. Тогда если объекты X и Y категории C изоморфны, то $F(X)$ и $F(Y)$ изоморфны.

Определение 36. *Контрвариантный функтор* $F : C \rightarrow D$ — это обычный функтор $C^{op} \rightarrow D$. Т.е. это совокупность “функций” $\text{Ob}(C) \rightarrow \text{Ob}(D)$ и “функций” из класса морфизмов C в класс морфизмов D , что

- для всякого морфизма $f \in \text{Hom}(X, Y)$, где $X, Y \in \text{Ob}(C)$, $F(f) \in \text{Hom}(F(Y), F(X))$,
- для всяких морфизмов f и g в C $F(f \circ g) = F(g) \circ F(f)$,
- для всякого объекта $X \in \text{Ob}(C)$ $F(\text{id}_X) = \text{id}_{F(X)}$.

Пример 15.

1. Есть контрвариантный функтор $F : \text{Top} \rightarrow \mathbb{C}\text{-CommAlg}$, где $F(X) = C(X)$ — множество комплекснозначных непрерывных функций на X , а $F(f)(\varphi) := \varphi \circ f$.
2. *Представимые функторы.* Пусть дана категория C и фиксирован объект $A \in \text{Ob}(C)$. Тогда есть контрвариантный функтор $h_A : C^{op} \rightarrow \text{Sets}$, что $h_A(X) = \text{Hom}(X, A)$, а $h_A(f)(\varphi) = \varphi \circ h$.

5.1 Мономорфизмы и эпиморфизмы

Определение 37. Морфизм f называется

- *мономорфизмом*, если для всяких морфизмов g и h будет верно $f \circ g = f \circ h \Rightarrow g = h$ (на f можно сокращать слева).
- *расщепимым мономорфизмом*, если есть морфизм r , что $r \circ f = \text{id}$ (у f есть обратимый слева). r называется *ретракцией* f .
- *эпиморфизмом*, если для всяких морфизмов g и h будет верно $g \circ f = h \circ f \Rightarrow g = h$ (на f можно сокращать справа).
- *расщепимым эпиморфизмом*, если есть морфизм r , что $f \circ r = \text{id}$ (у f есть обратимый справа).

Пример 16.

1. В Sets (расщепимые) мономорфизмы — инъективные отображения, (расщепимые) эпиморфизмы — сюръективные отображения.
2. В Groups (расщепимые) мономорфизмы — инъективные гомоморфизмы, (расщепимые) эпиморфизмы — сюръективные гомоморфизмы.
3. В Rings так же как в Groups.
4. ...

Замечание. Функторы совершенно не всегда сохраняют мономорфизмы и эпиморфизмы.

Лемма 30. Функторы сохраняют расщепимые мономорфизмы и расщепимые эпиморфизмы.

Лемма 31.

1. Всякий морфизм, являющийся расщепимым мономорфизмом и эпиморфизмом, есть изоморфизм.
2. Всякий морфизм, являющийся расщепимым эпиморфизмом и мономорфизмом, есть изоморфизм.

Определение 38. Пусть имеются морфизмы $F, G : C \rightarrow D$. Естественное преобразование $\alpha : F \rightarrow G$ — это совокупность морфизмов $\alpha_X \in \text{Hom}(F(X), G(X))$ для всякого $X \in \text{Ob}(C)$, что для всяких $A, B \in \text{Ob}(C)$ и всякого морфизма $f \in \text{Hom}(A, B)$ верно, что $G(f) \circ \alpha_A = \alpha_B \circ F(f)$.

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha_A} & G(A) \\ \downarrow F(f) & & \downarrow G(f) \\ F(B) & \xrightarrow{\alpha_B} & G(B) \end{array}$$

Композицией (также вертикальной композицией) естественных преобразований $\alpha : F \rightarrow G$ и $\beta : G \rightarrow H$, где $F, G, H : C \rightarrow D$ называется естественное преобразование $\beta \circ \alpha := \alpha : F \rightarrow H$, что $\gamma_X := \beta_X \circ \alpha_X$.

$$\begin{array}{ccccc} & & \gamma_A & & \\ & \xrightarrow{\quad} & & \xrightarrow{\quad} & \\ F(A) & \xrightarrow{\alpha_A} & G(A) & \xrightarrow{\beta_A} & H(A) \\ \downarrow F(f) & & \downarrow G(f) & & \downarrow H(f) \\ F(B) & \xrightarrow{\alpha_B} & G(B) & \xrightarrow{\beta_B} & H(B) \\ & & \gamma_B & & \end{array}$$

Горизонтальной композицией естественных преобразований $\alpha : F \rightarrow G$ и $\beta : H \rightarrow I$, где $F, G : C \rightarrow D$, $H, I : D \rightarrow E$ называется естественное преобразование $\beta \cdot \alpha := \gamma : H \circ F \rightarrow I \circ G$, где $\gamma_X := \beta_{G(X)}H(\alpha_X) = I(\beta_X)\alpha_{H(X)}$. (В равенстве и определённости композиции можно убедиться, если нарисовать диаграмму всех переходов для каких-нибудь объектов A и B и морфизма $f \in \text{Hom}(A, B)$; но она будет большая: 14 узлов, 29 стрелок и абсолютная коммутативность.)

Если α обратим, т.е. α_X обратим и его можно заменить на α_X^{-1} , то α называется *естественным изоморфизмом*, а F и G называются *изоморфными*, и пишут $F \simeq G$.

Категории C и D называются эквивалентными, если есть функторы $F : C \rightarrow D$, $G : D \rightarrow C$ и естественные изоморфизмы $\alpha : \text{id}_D \rightarrow G \circ F$ и $\beta : \text{id}_C \rightarrow F \circ G$.

Замечание 8. Таким образом мы получили категорию $\text{Funct}(C, D)$ функторов $C \rightarrow D$, где морфизмами являются естественные преобразования.

Лемма 32. Зафиксируем категорию I состоящую из объектов 0 и 1 и единственного нетождественного морфизма $0 \rightarrow 1$. Тогда для всяких функторов $F, G : C \rightarrow D$ задать естественное преобразование $F \rightarrow G$ — всё равно, что задать функционал $H : C \times I \rightarrow D$, что $H(\cdot, 0) = F$ и $H(\cdot, 1) = G$.

Лемма 33. Горизонтальная и вертикальная композиции коммутируют.

Пример 17.

1. ...
2. Назовём *топологической группой* группу заданную на топологическом пространстве G , что сама операция группы есть непрерывное отображение $G \times G \rightarrow G$. Например, \mathbb{R}^+ и \mathbb{R}^\times есть топологические группы на \mathbb{R} и $\mathbb{R} \setminus \{0\}$ соответственно. Будем рассматривать категорию локально компактных (у всякой точки есть замкнутая окрестность, являющаяся компактной) топологических абелевых групп. Для всякой группы A определим сопряжённую $A^* := \text{Hom}(A, S^1)$ — группа непрерывных гомоморфизмов $A \rightarrow S^1$ с некоторой топологией. Тогда есть тривиальный функтор F и нетривиальный функтор G из рассматриваемой категории в себя, где $G(A) = A^{**}$. При этом естественное преобразование $F \rightarrow G$ строится также как для векторных пространств.