15.5.21 / 18.10.25

Независимый Московский Университет, Алгебра-1, осень 2015

АЛГЕБРА, ПЕРВЫЙ СЕМЕСТР

Лекция 3 (4 октября 2018): Класиификационные задачи алгебры

3.0. Категорный язык.

3.0.0. Вводные соображения. *Теория категорий* – раздел математики, за которым также укрепилось неакадемичное название *абстрактная чепуха* – это (по крайней мере для математиков, использующих, а не разрабатывающих её) прежде всего *язык,* позволяющий преодолеть ограничения, накладываемые теоретико-множественным взглядом на объекты математики.

Согласно Ю.И. Манину, теория категорий воплощает *социологический подход к математике: объекты рассматриваются не сами по себе, а как члены сообщества себе подобных* (см. недавнее переиздание **[Манин2012]** курса лекций 1970 г.)

На языке теории *множеств,* введённом Георгом Кантором в последней четверти девятнадцатого века, можно было изложить всю существовавшую тогда математику. Единственное, чего было нельзя – это рассматривать *все* множества разом. *Множества* всех множеств не существует: если бы оно существовало, то по теореме Кантора-Бернштейна было бы строго мощнее самого себя.

3.0.1. Категория множеств. Зато существует *категория множеств* $\mathcal{SET}$. Она и является прототипом общего понятия категории.

Главная теоретико-множественная конструкция, аксиоматизируемая в произвольных категориях – сопоставление любой паре множеств множества *отображений* из одного в другое; эти множества отображений на языке теории категорий называются множествами *морфизмов.* Попадающий в центр внимания конгломерат множеств морфизмов снабжён *композициями,* удовлетворяющими закону "ассоциативности"; кроме того, в каждом множестве *эндоморфизмов,* то есть отображений в себя, выделяется *тождественный* эндоморфизм, обладающий очевидными свойствами.

Согласно теоретико-категорной терминологии, множества суть *объекты* категории $\mathcal{SET}$.

Понятия "быть объектом категории" и "быть элементом множества" аналогичны, но не совпадают; мы введём для первого из них (нестандартное!) обозначение $\in\in$. Теперь фразу X–*множество* можно записать в виде

$$X \in\in \mathcal{SET}.$$

В дальнейшем мы также будем (нестандартно) дублировать теоретико-множественные значки для введения соответствующих им категорно-теоретических и логических.

3.0.2. Определение категории. Категория $\mathcal{C}$ считается заданной, если введён *класс* её объектов и для любых двух объектов

$$\forall\forall X, Y \in\in \mathcal{C}$$

определено множество

$$\mathrm{Mor}_{\mathcal{C}}(X, Y)$$

морфизмов из X в Y.

Включение

$$\varphi \in \mathrm{Mor}_{\mathcal{C}}(X, Y)$$

будет констатироваться также абсолютно синонимичными, но более выразительными записями

$$\varphi : X \longrightarrow Y,$$

или

$$X \xrightarrow{\varphi} Y,$$

в которых категория $\mathcal{C}$ должна восстанавливаться из контекста; следует при этом иметь в виду, что далеко не для всех категорий морфизмы являются отображениями – см. далее. В последней записи φ следует воспринимать как *имя* стрелки.

Важное лингвистическое замечание. Запись $X \xrightarrow{\varphi} Y$ – предвестник развития *нелинейных* элементов категорного языка: тексты перестают быть *последовательностями* значков. В частности, будет развиваться язык *диаграмм морфизмов*, не менее важный для понимания, чем язык чертежей для понимания планиметрии.

Для любых трёх объектов

$$\forall\forall X, Y, Z \in\in \mathcal{C}$$

предполагается определённой *композиция*

$$\mathrm{Mor}_{\mathcal{C}}(X, Y) \times \mathrm{Mor}_{\mathcal{C}}(Y, Z) \longrightarrow \mathrm{Mor}_{\mathcal{C}}(X, Z) : (\varphi, \psi) \mapsto \psi \circ \varphi,$$

"ассоциативная" в том смысле, что равенство

$$\psi \circ (\varphi \circ \chi) = (\psi \circ \varphi) \circ \chi$$

должно выполняться всякий раз, когда обе его части имеют смысл, то есть для любых четырёх объектов

$$T, X, Y, Z \in\in \mathcal{C}$$

и для любых трёх морфизмов

$$\chi : T \longrightarrow X,$$

$$\varphi : X \longrightarrow Y,$$

$$\psi : Y \longrightarrow Z.$$

Определение композиции морфизмов проясняется нелинейной записью (и без неё, вероятно, с трудом воспринимается начинающими)

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[rr, bend right, "\psi \circ \varphi"'] & Y \arrow[r, "\psi"] & Z \end{tikzcd}$$

Эта же запись позволяет примириться с "противоестественным"порядком: в случае категории множеств ещё одна "ассоциативность" , являющаяся *определением композиции*

$$(\psi \circ \varphi)(x) := \psi(\varphi(x))$$

$x \in X$, в правой части "читается"слева направо.

Требуется ещё, чтобы в множестве эндоморфизмов любого объекта существовал выделенный элемент, обычно называемый *единицей* (или *тождественным преобразованием,* хотя, напомним, морфизмы далеко не всегда являются отображениями...), нейтральный слева и справа относительно всех композиций

$$\forall\forall X \in\in \mathcal{C}\ \exists! \mathbf{1}_X \in \mathrm{Mor}_{\mathcal{C}}(X, X);$$

$$[\forall\forall Y \in\in \mathcal{C},\ \forall \varphi : X \longrightarrow Y; \psi \circ \varphi \circ \mathbf{1}_X = \psi \circ \varphi] \wedge$$

$$\wedge [\forall\forall Y \in\in \mathcal{C},\ \forall \psi \circ \varphi : Y \longrightarrow X; \mathbf{1}_X \circ \psi \circ \varphi = \psi \circ \varphi].$$

Как мы видим, две аксиомы теории категорий связаны с ассоциативностью и единицами – как в теории моноидов (в моноиде, правда, единственная единица). В этом смысле теорию категорий можно рассматривать как теорию обобщённых моноидов; в случае, когда объединение множеств морфизмов образует множество (о таких категориях мы вскоре поговорим, они называются *малыми*) можно считать, что композиция – это *частично определённая* ассоциативная операция. Об объектах можно забыть; такая позиция обсуждается в книге одного из основателей теории категорий **[Маклейн2004]**.

3.1. Основные конкретные категории

Неформально категория называется *конкретной*, если её объекты – множества с одной или несколькими дополнительными *структурами,* а морфизмы – отображения множеств, *согласованные* с этими структурами; обычно говорится, что отображения *уважают* эти структуры. Формально конкретность определяется в терминах *забывающего функтора* из рассматриваемой категории в категорию множеств, но мы всё это откладываем на последующие лекции. Общие понятия *структур* и *уважения* к ним определяться не будут, а будут задаваться списком.

3.2.0. Снова категория множеств $\mathcal{SET}$. Как было сказано выше, её объекты – просто множества *без* дополнительных структур[1], множества морфизмов суть множества *всех* отображений, то есть для $X, Y \in\in \mathcal{SET}$

$$\mathrm{Mor}_{\mathcal{SET}}(X,Y) \equiv Y^X := \{\text{отображения } X \longrightarrow Y\},$$

а композиция для $X, Y, Z \in\in \mathcal{SET}$ уже была определена как

$$\mathrm{Mor}_{\mathcal{SET}}(X,Y) \times \mathrm{Mor}_{\mathcal{SET}}(Y,Z) \longrightarrow \mathrm{Mor}_{\mathcal{SET}}(X,Z) : (\alpha,\beta) \mapsto \beta \circ \alpha,$$

где для $x \in X$

$$(\beta \circ \alpha(x)) := \beta(\alpha(x)).$$

В дальнейшем будут рассматриваться множества вместе с *дополнительными структурами* – например, с *(бинарными) операциями*

$$*_X : X \times X \longrightarrow X : (x_1, x_2) \mapsto x_1 *_X x_2$$

с морфизмами $\alpha \in Y^X$, удовлетворяющими для любых $x_1, x_2 \in X$ равеству

$$\alpha(x_1 *_X x_2) = \alpha(x_1) *_Y \alpha(x_2).$$

Отметим, что в дальнейшем множества со структурами будут – как объекты соответствующих категорий – обозначаться так же, как и сами множества. Например, когда *счётность* множества X определяется через наличие биекции $X \simeq \mathbb{N}$, то $\mathbb{N}$ – просто множество натуральных чисел; вскоре будет определена категория *моноидов*, объектом которой будет тройка $(\mathbb{N}; +; 0)$ натуральных чисел вместе с операцией их сложения и нейтральным элементом; в категории *ординалов*, которой мы в обозримом будущем заниматься не будем, имеется важный объект $(\mathbb{N}; \leq)$ и т.д. Разумеется, множества *морфизмов*, связывающих $\mathbb{N}$ с другими объектами, зависит от категории.

3.1.1. Категория моноидов. Как мы знаем, *моноидом* называется множество с одной ассоциативной операцией, обладающей двусторонним нейтральным элементом. На наш формальный язык

[1] это словосочетание имеет смысл независимо от смысла слова *структура*

с дублированием теоретико-множественных значков определение соответствующей категории переводится так:

$$\mathcal{MON} :=:= \{\{(M; \cdot_M; 1_M) \mid\mid$$
$$[\forall m_1, m_2, m_3 \in M; (m_1 \cdot_M m_2) \cdot_M m_3 = m_1 \cdot_M (m_2 \cdot_M m_3)] \wedge$$
$$\wedge [\forall m \in M; 1_M \cdot_M m = m \cdot_M 1_m = m]\}\}.$$

Сократив запись $(M; \cdot_M; 1_M) \in\in \mathcal{MON}$ до $M \in\in \mathcal{MON}$, определяем для двух объектов $M, N \in\in \mathcal{MON}$

$$\mathrm{Mor}_{\mathcal{MON}}(M, N) :=$$
$$:= \{\alpha \in N^M \mid [\alpha(1_M) = 1_N] \wedge [\forall m, m' \in M; \alpha(m \cdot_M m) = \alpha(m) \cdot_N \alpha(m')]\}.$$

В формулах, адресованных понимающему контекст человеку, индексы, указывающие на моноид, а также знак операции (в мультипликативной версии её записи) часто опускаются; так, формула, определяющая *уважение* морфизмом нейтрального элемента, может быть записана как $\alpha(1) = 1$, а определяющая уважение к операции – как $\alpha(m \cdot m') = \alpha(m) \cdot \alpha(m')$ или даже как $\alpha(mm') = \alpha(m)\alpha(m')$.

Наш запас аксиом моноида минимален. Множества с произвольной ассоциативной операции, необязательно с нейтральным элементом, называются *полугруппами*, и мы не будем их рассматривать; примером (неинтересной...) полугруппы без нейтрального элемента является $(\mathbb{N}_{\geq 2}; +)$. Как показывает пример (ассоциативной!) операции $x * y := y$ на любом множестве, левосторонний нейтральный элемент не обязан быть односторонним, и к тому же их может быть много. Наконец, в категории моноидов уважение морфизма к операции не влечёт уважения к нейтральному элементу: например, *левый сдвиг* $\mathsf{L}_e : x \mapsto e * x$ на коммутативном моноиде, уважает операцию, если e является *идемпотентом*, то есть $e * e = e$, но не уважает нейтрального элемента, если e *нетривиален*, то есть отличен от нейтрального элемента. Пример моноида с нетривиальными идемпотентами – $(\mathrm{Sub}(U); \bigcup; \varnothing)$, где $\mathrm{Sub}(U)$ – множество подмножеств любого фиксированного множества U.

На каждом из классических числовых множеств

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

есть две структуры моноида, аддитивная с нейтральным элементом 0 и мультипликативная с нейтральным элементом 1; в связи с этим выражения вроде *рассмотрим моноид* $\mathbb{Q}$ или $\mathbb{Q} \in\in \mathcal{MON}$ недопустимы, следует писать $(\mathbb{Q}; +; 0) \in\in \mathcal{MON}$ или $(\mathbb{Q}; \cdot; 1) \in\in \mathcal{MON}$. Кроме того, имеются классические моноиды с учётом порядка, например,

$$(\mathbb{Q}_{\leq 0}; +; 0) \text{ и } (\mathbb{R}_{>0}; \cdot; 1).$$

Любое из вложений классических числовых множеств, например, $\mathbb{Z} \hookrightarrow \mathbb{C}$, определяет два морфизма моноидов.

Менее тривиальными являются пары взаимно обратных морфизмов, то есть *изо*морфизмов в категории $\mathcal{MON}$: для $a \in \mathbb{R}_{>0} \setminus \{1\}$ определены

$$\log_a : (\mathbb{R}_{>0}; \cdot; 1) \xrightarrow{\simeq} (\mathbb{R}; +; 0)$$

и

$$(\mathbb{R}; +; 0) \xrightarrow{\simeq} (\mathbb{R}_{>0}; \cdot; 1) : x \mapsto a^x$$

(для второго из этих изоморфизмов при $a \neq \mathrm{e} = 2.718281828...$ общепринятого обозначения не существует).

Для любого множества $\forall\forall U \in\in \mathcal{SET}$ отображение (у которого есть несколько обозначений) взятия *дополнения*

$$\mathrm{Sub}(U) \longrightarrow \mathrm{Sub}(U) : X \mapsto U \setminus X$$

определяет в силу *формул де Моргана* <u>два</u> изоморфизма моноидов:

$$(\mathrm{Sub}(U); \bigcup; \varnothing) \xrightarrow{\simeq} (\mathrm{Sub}(U); \bigcap; U)$$

и

$$(\mathrm{Sub}(U); \bigcap; U) \xrightarrow{\simeq} (\mathrm{Sub}(U); \bigcup; \varnothing).$$

Рассмотренные примеры показывают, что в некоторых случаях использование сокращённых записей, то есть записей без указания операций, нежелательно.

Имеется огромный класс моноидов, доставляемых <u>любым</u> объектом <u>любой</u> категории. Если $\mathcal{C}$ – категория, то для любого её объекта $X \in\in \mathcal{C}$ множеством *эндоморфизмов* этого объекта называется

$$\mathrm{End}_{\mathcal{C}}(X) := \mathrm{Mor}_{\mathcal{C}}(X, X).$$

Очевидно, композиция морфизмов определяет на этом множестве структуру моноида:

$$\forall\forall(\mathrm{End}_{\mathcal{C}}(X); \circ; \mathbf{1}_X) \in\in \mathcal{MON}.$$

3.1.2. Категория групп. Как известно, *группой* называется моноид, в котором каждый элемент двусторонне обратим. Формально:

$$\mathcal{GRP} :=:= \{\{(G; \cdot_G; 1_G) \in\in \mathcal{MON} \mid\mid$$

$$[\forall g \in G\ \exists h \in G;\ g \cdot_G h = h \cdot_G g = 1_G].$$

Категория групп является *полной подкатегорией* категории моноидов – определение будет обсуждаться позже; это означает, что

$$\forall\forall G, H \in\in \mathcal{GRP}[\mathrm{Mor}_{\mathcal{GRP}}(G, H) := \mathrm{Mor}_{\mathcal{MON}}(G, H)]\}\}.$$

Приведённое определение удобно с категорной точки зрения. но неудобно при практическом использовании: оно требует нового обозначения для каждого обратного элемента. Однако двусторонний обратный в группе единственен – действительно, из системы равенств $gh = hg = gh' = h'g = 1$ путем умножения, например, равенства $gh = 1$ слева на h' вытекает $h = h'$ – поэтому удобно использовать традиционное обозначение $h = g^{-1}$.

Это, однако, требует определения группы не как тройки $(G, \cdot, 1)$, а как *четвёрки* $(G, \cdot, 1, ^{-1})$, в которой подробная запись с пометками $_G$ неудобна по типографским причинам. Эквивалентности двух определений с логической точки зрения – довольно тонкий вопрос; см. **[BarrettHalvorson2016]**.

Введённая система аксиом группы минимальна. Потребовать одностороннюю обратимость недостаточно: для любого множества $X \in\in \mathcal{SET}$ моноид $(X^X, \circ, \mathrm{id}_X)$ содержит подмоноиды *инъективных* и *сюръективных* отображений. Элементы первого из них обратимы слева, а второго – справа; однако в случае *бесконечного* X эти подмоноиды различны (таково <u>определение</u> бесконечности).

На каждом из классических числовых множеств, кроме множества натуральных чисел

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

есть структура *аддитивной* группы, и вложения определяют соответствующие морфизмы в категории $\mathcal{GRP}$. Группой является также *мультипликативный* моноид положительных вещественных чисел $(\mathbb{R}_{>0}; \cdot; 1)$, и описанные выше изоморфизмы, задаваемые логарифмами и показательными функциями, являются изоморфизмами групп.

Изоморфизмы же, переводящие друг в друга операции объединения и пересечения, остаются в категории моноидов, то есть не являются морфизмами групп. Действительно, операции $\bigcup$ и $\bigcap$ обладают крайней степенью необратимости: обратимы лишь нейтральные элементы.

Обратимость в $\mathrm{Sub}(U)$ можно восстановить, заменив объединение на *симметрическую разность*:

$$X\Delta Y := (X\bigcup Y)\setminus(X\bigcap Y) = (X\setminus Y)\bigcup(X\setminus Y),$$

но при этом симметрия объединения и пересечения пропадает.

Огромный класс групп доставляется <u>любым</u> объектом <u>любой</u> категории. Если $\mathcal{C}$ – категория, то для любого её объекта $X \in\in \mathcal{C}$ множеством *автоморфизмов* этого объекта называется множество *обратимых* эндоморфизмов

$$\mathrm{Aud}_{\mathcal{C}}(X) := \{\alpha \in \mathrm{End}_{\mathcal{C}}(X) \mid \exists\beta \in \mathrm{End}_{\mathcal{C}}(X)[\alpha\circ\beta = \beta\circ\alpha = \mathbf{1}_X]\}.$$

Очевидно, композиция морфизмов определяет на этом множестве структуру группы:

$$\forall\forall(\mathrm{Aut}_{\mathcal{C}}(X);\circ;\mathbf{1}_X) \in\in \mathcal{GRP}.$$

Не будет преувеличением сказать, что бóльшая часть известных человечеству групп возникла с помощью этой конструкции.

3.1.3. Категория коммутативных групп $\mathcal{AB}$. Группа называется *коммутативной*, или *абелевой*, если операция в ней коммутативна. Формально:

$$\mathcal{AB} :=:= \{\{(A;\cdot_A;1_A) \in\in \mathcal{GRP} \mid\mid$$

$$[\forall a, b \in A\ [a\cdot_A b = b\cdot_A a]]\}\}.$$

Категория абелевых групп является *полной подкатегорией* категории групп – (определение будет позже); это означает, что

$$\forall\forall A, B \in\in \mathcal{AB}[\mathrm{Mor}_{\mathcal{AB}}(A,B) := \mathrm{Mor}_{\mathcal{GRP}}(A,B)].$$

Три рассмотренные категории (в интуитивно ясном смысле) вложены друг в друга:

$$\mathcal{MON} \subset\subset \mathcal{GRP} \subset\subset \mathcal{AB}.$$

Сводка рассмотренных примеров и классов примеров содержится в следующей схеме:

$(\mathbb{N};+;0)$ $(\mathbb{N};\cdot;1)$ $(\mathbb{Z};\cdot;1)$ $(\mathbb{Q};\cdot;1)(\mathbb{R};\cdot;1)(\mathbb{C};\cdot;1)$
$(\mathrm{Sub}(U);\bigcup;\varnothing)$ $(\mathrm{Sub}(U);\bigcap;U)$ $(\mathrm{End}_{\mathcal{C}}(X);\circ;\mathbf{1}_X)$

$(\mathrm{Aut}_{\mathcal{C}}(X);\circ;\mathbf{1}_X)$

$(\mathbb{Z};+;0)$ $(\mathbb{Q};+;0)(\mathbb{R};+;0)(\mathbb{C};+;0)$
$(\mathbb{Q}^{\times};\cdot;1)(\mathbb{R}^{\times};\cdot;1)(\mathbb{C}^{\times};\cdot;1)$
$(\mathrm{Sub}(U);\Delta;\varnothing)$
$\mathcal{AB}$

$\mathcal{GRP}$

$\mathcal{MON}$

3.1.4. Категория колец $\mathcal{RING}$. Как мы знаем, *кольцом* называется множество с двумя операциями, называемыми *сложением* и *умножением*. Относительно сложения кольцо должно образовывать абелеву группу, а относительно умножения – моноид; требуется двусторонняя *дистрибутивность* сложения относительно умножения. Формально:

$$\mathcal{RING} :=:= \{\{(R;+,\cdot;0,1) \mid\mid$$

$$[(R;+;0) \in\in \mathcal{AB}] \wedge [(R;\cdot;1) \in\in \mathcal{MON}] \wedge$$

$$\wedge[\forall r,s,t \in R[[r\cdot(s+t) = r\cdot s + r\cdot t] \wedge [(r+s)\cdot t = r\cdot s + r\cdot t]]]$$

Введённая система аксиом кольца минимальна. Потребовать одностороннюю дистрибутивность недостаточно[2]: "кольцо многочленов" $(\mathbb{Q}[x];+,\circ;0,x)$ с композицией вместо умножения доставляет пример пары операций, обладающей левой, но не правой дистрибутивностью.

Умножение в "числовых" кольцах коммутативно – см. следующий подраздел. Типичные *некоммутативные кольца*, которые встретятся в нашем курсе – это *внешние алгебры* (умножение в которых, впрочем, *суперкоммутативно*), *групповые кольца* и *кватернионы*, введённые в начале этой лекции. Сейчас упомянем один широкий класс некоммутативных колец – кольца *эндоморфизмов абелевых групп*: произвольная абелева группа $A \in\in \mathcal{AB}$ определяет *кольцо эндоморфизмов*

$$(\mathrm{End}(A);+,\circ;0,\mathbf{id}_A),$$

[2]получающийся набор аксиом характеризовал бы класс *почти-колец (near-rings)*, см. **[Pilz1981]**

в котором под *сложением* эндоморфизмов понимается поэлементное сложение, то есть

$$(\alpha +_{\mathrm{End}(A)} \beta)(a) := \alpha(a) +_A \beta(a)$$

для $\alpha, \beta \in \mathrm{End}(A)$ и $a \in A$.

3.1.5. Категория коммутативных колец $\mathcal{ANN}$. Кольцо называется *коммутативным*, если умножение в нём коммутативно. Формально:

$$\mathcal{ANN} :=:= \{\{(R; +, \cdot; 0, 1) \in\in \mathcal{RING} \mid\mid$$
$$[\forall r, s \in R;\ [r \cdot s = s \cdot r]]\}\}.$$

Категория коммутативных колец является *полной подкатегорией* категории колец – (определение будет ...); это означает, что

$$\forall\forall R, S \in\in \mathcal{ANN}[\mathrm{Mor}_{\mathcal{ANN}}(R, S) := \mathrm{Mor}_{\mathcal{RING}}(R, S)].$$

На каждом из классических числовых множествах, кроме множества натуральных чисел,

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

есть структура коммутативного кольца, и вложения определяют соответствующие морфизмы в категории $\mathcal{ANN}$.

Особняком стоит класс *булевых* колец, определяемых для любого множества U:

$$(\mathrm{Sub(U)}; \Delta, \bigcap; \varnothing, \mathrm{U}).$$

Сводка упомянутых колец содержится в следующей схеме:

[для $A \in\in \mathcal{AB}$] $(\mathrm{End}(A); +, \circ; 0, \mathbf{id}_A)$

$(\mathbb{Z}; +, \cdot; 0, 1)$ $(\mathbb{Q}; +, \cdot; 0, 1))$

$(\mathbb{R}; +, \cdot; 0, 1)$ $(\mathbb{C}; +, \cdot; 0, 1)$

$(\mathrm{Sub}(U); \Delta, \bigcup; \varnothing, U)$

$\mathcal{ANN}$

$\mathcal{RING}$

3.2 Изоморфизмы

3.2.0. Что вместо равенства объектов? Понятие *равенства объектов категории* НЕ вводится и объявляется лишённым смысла. Любой акт *отождествления* объектов заслуживает осмысления и обозначения. Объекты сравниваются на основе наличия морфизмов со специальными свойствами.

3.3.1. Односторонняя обратимость морфизмов. Пусть дана категория $\mathcal{C}$ и два её объекта

$$X, Y \in\in \mathcal{C}.$$

Морфизм $\mu : X \to Y$ называется *обратимым слева*, если найдётся такой морфизм $\varphi : Y \to X$, что

$$\varphi \circ \mu = \mathbf{1}_X.$$

Обратимые слева морфизмы являются *мономорфизмами* (обсудим это понятие в следующем семестре), отсюда выбор буквы.

В категории множеств морфизм обратим слева тогда и только тогда, когда *инъективен*. Действительно, если отображение $\mu : X \to Y$ инъективно, то на множестве $\mu(X) \subseteq Y$ корректно определено отображение $y \mapsto f^{-1\circ}(y)$; для получения левого обратного достаточно доопределить это отображение на $Y \setminus \mu(X)$ произвольно. Наоборот, если φ – левое обратное к μ, то достаточно применить его к равенству $\mu(x_1) = \mu(x_2)$ для $x_1, x_2 \in X$, чтобы получить $x_1 = x_2$.

Для других конкретных категорий инъективность морфизма не обязательно влечёт обратимость слева. Например, в категории колец (неважно, $\mathcal{ANN}$ или $\mathcal{RING}$) вложение $\mathbb{Z} \hookrightarrow \mathbb{Q}$ не может иметь (ни левого, ни правого) обратного, поскольку, очевидно, $\mathrm{Mor}_{\mathcal{ANN}}(\mathbb{Q}, \mathbb{Z}) = \varnothing$.

Морфизм $\varepsilon : X \to Y$ называется *обратимым справа*, если найдётся такой морфизм $\varphi : Y \to X$, что

$$\varepsilon \circ \varphi = \mathbf{1}_Y.$$

Обратимые справа морфизмы являются *эпиморфизмами* (обсудим это понятие в следующем семестре), отсюда выбор буквы.

В категории множеств морфизм обратим справа тогда и только тогда, когда *сюръективен*. Действительно, если отображение

$\mu : X \to Y$ сюръективно, то выбор для $y \in Y$ *произвольного* элемента из непустого множества $\varepsilon^{-1\circ}(y)$ определяет[3] требуемое отображение $\varphi : Y \to X$. для Наоборот, если φ – правое обратное к ε, то для любого $y \in Y$ отображение ε переводит $\varphi(y)$ в y.

Для других конкретных категорий сюръективность морфизма не обязательно влечёт обратимость справа. Например, в категории групп (неважно, $\mathcal{AB}$ или $\mathcal{GRP}$) сюръективное отображение $\mathbb{Z} \to \{\pm 1\} : n \mapsto (-1)^n$ не может иметь (ни левого, ни правого) обратного, поскольку, очевидно, $\mathrm{Mor}_{\mathcal{AB}}(\{\pm 1\}, \mathbb{Z}) = \varnothing$.

3.2.2. Двусторонняя обратимость морфизмов. Пусть по-прежнему дана категория $\mathcal{C}$ и два её объекта

$$X, Y \in\in \mathcal{C},$$

а морфизм $\iota : X \to Y$ обратим и слева, и справа. Это значит, что существуют такие $\lambda, \rho : Y \to X$, что

$$\lambda \circ \iota = \mathbf{1}_X \tag{3.2.2a}$$

и

$$\iota \circ \rho = \mathbf{1}_Y. \tag{3.2.2b}$$

Предложение. *Если морфизм обратим и слева, и справа, то его обратные слева и справа единственны и совпадают. Иначе говоря, во введённых обозначениях $\lambda = \rho$.*

Доказательство. Рассмотрим подходящую комбинацию имеющихся стрелок: с одной стороны,

$$(\lambda \circ \iota) \circ \rho =_{(\mathbf{3.2.2a})} \rho, \tag{3.2.2c}$$

а с другой –

$$\lambda \circ \iota (\circ \rho) =_{(\mathbf{3.2.2b})} \lambda. \tag{3.2.2d}$$

Из "ассоциативности" композиции в силу **(3.2.2c)** и **(3.2.2d)** следует $\lambda = \rho$.■

Определение. Морфизм $\iota : X \to Y$ называется *изоморфизмом*, если существует такой морфизм $\iota' : Y \to X$, что

$$\iota' \circ \iota = \mathbf{1}_X \tag{3.2.2e}$$

---

[3] согласие с тем, что таким произвольным образом действительно можно определять отображения, равносильно *аксиоме свободного выбора*; не все математики принимают её

и
$$\iota \circ \iota' = \mathbf{1}_Y. \tag{3.2.2f}$$
Из предложения **3.2.2** вытекает, что двусторонне обратный к изоморфизму единственен; мы будем применять нестандартное обозначение $\iota' = \iota^{-1\circ}$.

3.2.3. Изоморфность, в том числе каноническая. Объекты $X, Y \in\in \mathcal{C}$ называются *изоморфными*, если существует изоморфизм $X \to Y$; обозначение изоморфизма часто опускается. Факт изоморфности объектов обозначается одним из двух способов: различаются *канонические*
$$X \cong Y$$
и *неканонические* (*произвольные, случайные* – общепринятого термина не существует)
$$X \simeq Y$$
изоморфизмы.

Точные определения приведём позже, а пока ограничимся примерами.

Декартово произведение в категорных терминах будет определено позже, а пока определим его для множеств по Декарту:
$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}.$$
Имеются очевидные, не зависящие ни от чего изоморфизмы
$$X \times Y \longrightarrow Y \times X : (x, y) \mapsto (y, x)$$
и
$$X \times (Y \times Z) \longrightarrow (X \times Y) \times Z : (x, (y, z)) \mapsto ((x, y), z).$$
В силу их уникальности и *естественности* эти изоморфизмы считают *каноническими* и записывают в виде
$$X \times Y \cong Y \times X$$
и
$$X \times (Y \times Z) \cong (X \times Y) \times Z.$$
С другой стороны, рассмотренные выше "экспоненциально-логарифмические" изоморфизмы в категории $\mathcal{GRP}$
$$\mathbb{R} \longrightarrow \mathbb{R}_{>0} : x \mapsto a^x$$
и
$$\mathbb{R}_{>0} \longrightarrow \mathbb{R} : y \mapsto \log_a y$$

определены при любом $a \in \mathbb{R}_{>0} \setminus \{1\}$, и нет причин для выбора какого-нибудь из них[4]. Поэтому указанные изоморфизмы не считаются каноническими, и обычно используется запись

$$(\mathbb{R}; +; 0) \simeq (\mathbb{R}_{>0}; \cdot; 1).$$

Рассмотрим пример из конечной математики. Пусть даны два трёхэлементных множества, между которыми не видно бросающейся в глаза биекции[5], например, поэтов

$$\text{П} := \{\text{Пушкин, Лермонтов, Некрасов}\}$$

и цветов

$$\text{Ц} := \{\text{синий, зелёный, красный}\}.$$

В категории $\mathcal{SET}$ констатируем неканоническую изоморфность $\text{П} \simeq \text{Ц}$, но она не имеет отношения к алгебре. Выбрав же произвольную биекцию $\iota : \text{П} \to \text{Ц}$, мы получим изоморфизм 6-элементных групп

$$\mathrm{Aut}_{\mathcal{SET}}(\text{П}) \longrightarrow \mathrm{Aut}_{\mathcal{SET}}(\text{Ц}) : \alpha \mapsto \iota \circ \alpha \circ \iota^{-1\circ}.$$

Поскольку этот изоморфизм зависит от случайно выбранного ι (проверьте!), мы получили неканонический изоморфизм

$$\mathrm{Aut}_{\mathcal{SET}}(\text{П}) \simeq \mathrm{Aut}_{\mathcal{SET}}(\text{Ц}).$$

3.3. Классификация в алгебре

Введённые категорные понятия могут быть применены к одной из основных проблем современной алгебры.

3.3.0. Постановка проблемы. Мы рассмотрели несколько видов алгебраических структур – от моноидов до коммутативных колец. Каждому такому виду была сопоставлена категория – от $\mathcal{MON}$ до $\mathcal{ANN}$. Будем называть такого рода конкретные категории *алгебраическими.*

Важный аспект категорных рассмотрений – (психологическое) <u>отождествление</u> изоморфных объектов. Общая проблема заключается в

классификации объектов алгебраических категорий или их подходящих подкатегорий с точностью до изоморфизма.

[4]несмотря на традиционность выбора $a = \mathrm{e} = 2.718281828\ldots$, существующего всё же наряду с $a = 2$ и $a = 10$

[5]$\{a, b, c\}$ и $\{a', b', c'\}$ не годятся...

Уточнение этой формулировки – одна из целей следующей лекции.

3.4.1. Тайна хорошей аксиоматики. Составление списков свойств операций, определяющих рассматриваемые алгебраические категории, может выглядеть достаточно произвольной фиксацией некоторых свойств операций в классических числовых множествах – это и есть *аксиоматизация*. Однако наугад взятые списки аксиом (особо ценны краткие), скорее всего, к интересной математике не приведут. Принципы, по которым всё-таки создаются плодотворные аксиоматики, современной науке вряд ли понятны; например, гениальной была идея не включать *коммутативность* в число "очевидных" свойств операций. См. введение к **[Шафаревич1999]**.

Один из важнейших признаков хорошей алгебраической аксиоматики – содержательные и красивые классификационные результаты. Им будет посвящена существенная часть курса.

3.3.2. Структуры на конечных множествах. В любой алгебраической категории $\mathcal{C}$ есть и весьма важна подкатегория конечных[6] множеств с соответствующими структурами; обозначим эту подкатегорию $\mathcal{C}[\mathbf{fin}]$. *Классифицируемость* объектов подкатегории $\mathcal{C}[\mathbf{fin}]$ – важная характеристика категории $\mathcal{C}$. Приведём некоторые сведения о рассмотренных нами категориях.

Категория $\mathcal{C}$	О классификации $\mathcal{C}[\mathbf{fin}]$
$\mathcal{MON}$	Вряд ли существует
$\mathcal{GRP}$	Одно из важнейших достижений XX века
$\mathcal{AB}$	Имеется полная классификация, будет рассказана
$\mathcal{RING}$	Известна и сложна, см. **[KP1970]**
$\mathcal{ANN}$	Известна, будет намечена

Литература

[BarrettHalvorson2016] Barrett, Thomas William and Halvorson, Hans, *Glymour and Quine on Theoretical Equivalence.* Journal of Philosophical Logic 45 (5), 2016:467-483.

[Frobenius1878] Ferdinand Georg Frobenius, (1878) *Uber lineare Substitutionen und bilineare Formen.* Journal fur die reine und angewandte Mathematik 84, (1878), 1–63.

[6]словосочетание *конечный объект категории* имеет и другой смысл, который будет обсуждаться в последующих лекциях

[Hamilton1844] William Rowan Hamilton, *On a new species of Imaginary Quantities connected with the Theory of QUATERNIONS.* Irish Academy Proceedings, II., 1844, pp. 424-434.
[KP1970] Robert L. Kruse and David T. Price, *Enumerating finite rings.* J. London Mat. Soc. (2), 2 (1970), 149 – 159.
[Pilz1981] G. Pilz, *Near-Rings: What They Are and What They Are Good For.* In Contemp. Math., 9, pp. 97–119. Amer. Math. Soc., Providence, R.I., 1981.
[Кострикин1977] Кострикин А. И., *Введение в алгебру.* М.: Наука, 1977.
[Маклейн2004] Маклейн С., *Категории для работающего математика.* М.: Физматлит, 2004.
[Манин2012] Юрий Манин, *Введение в теорию схем и квантовые группы.* МЦНМО, 2012.
[Шафаревич1999] Шафаревич И.Р., *Основные понятия алгебры.* Ижевск, 1999.