Конспект лекций по алгебре. ЛЭТИ, ФКТИ, весна 2016/17 уч. г.

А.В.Степанов

Предисловие

Этот конспект по разным причинам не будет полностью совпадать с тем, что я говорил на лекциях. Однако я надеюсь, что слушателям будет нетрудно понять, что лекции и конспект эквивалентны, просто некоторые утверждения написаны другими словами, а некоторые вынесены под отдельный заголовок. Приведем некоторые обозначения.

Обозначения и терминология

$\coprod_{k \in K} X_k$ – это объединение непересекающихся множеств X_k (это называют дизъюнктным объединением).

Собственное подмножество – это подмножество, не совпадающее со всем множеством.

$x \mod n$ означает остаток от деления целого числа x на n (обозначение из Паскаля).

$[n] = \{1, \ldots, n\}$

Глава 1

Функции и операции, основные алгебраические структуры

1. Функции

Я далек от мысли, записать весь курс исходя только из аксиом теории множеств. Однако, на примере понятия функции мне хотелось бы показать, что можно определить любое математическое понятие не оперируя неопределенными ранее словами, что сплошь и рядом встречается в учебной литературе. Если определение начинается со слов "функция – это отображение...", то первый же вопрос, который возникает у внимательного читателя: "А что такое отображение?".

Определение 1.1. Кортеж длины n (другие названия: последовательность длины n или, короче, n-ка) определяется рекурсивно: кортеж длины 1 – это одноэлементное множество, кортеж длины n – это множество, состоящее из кортежа длины $n-1$ и еще одного элемента. Кортеж длины n обозначается $(a_1, \dots, a_n)$. В отличие от множества, в кортеже важен порядок элементов.

Упорядоченная пара $(x, y) = \big\{\{x\}, y\big\}$ – это кортеж длины 2.

Декартово произведение множеств X и Y – это множество

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

Определение 1.2. Функция – это тройка (X, Y, Γ), где X и Y – множества, а Γ – подмножество в $X \times Y$ такое, что для любого $x \in X$ существует единственный $y \in Y$, удовлетворяющий условию $(x, y) \in \Gamma$. При этом X называется областью определения, Y – множеством значений, а Γ – графиком функции.

Пусть $f = (X, Y, \Gamma)$ – функция. Обычно говорят, что f – это функция из X в Y и пишут $f : X \to Y$. Вместо $(x, y) \in \Gamma$ принято писать $f(x) = y$ и говорить, что y – это образ элемента x под действием функции f.

Определение 1.3. Образ функции $f : X \to Y$ – это множество $\operatorname{Im} f = \{f(x) \mid x \in X\}$. Если $X' \subseteq X$, то $f(X') = \{f(x) \mid x \in X'\}$ называется образом X' под действием функции f.

Если $x \in X$, а $y = f(x)$, то x называется прообразом элемента y. Полный прообраз y – это множество всех его прообразов. Он обозначается через $f^{-1}(y)$. Полный прообраз подмножества $Y' \subseteq Y$ – это множество $f^{-1}(Y') = \{x \in X \mid f(x) \in Y'\}$. Ясно, что $f^{-1}(Y') = \coprod\limits_{y \in Y'} f^{-1}(y)$.

Пусть $X' \subseteq X$ сужением функции $f : X \to Y$ называется функция $f|_{X'} : X' \to Y$, заданная формулой $f|_{X'}(x) = f(x)$. В обозначениях определения 1.2 $f|_{X'} = (X', Y, (X' \times Y) \cap \Gamma)$, где Γ – график функции f.

Лемма 1.4. *Если $f : X \to Y$ – функция, то $X = \coprod\limits_{y \in Y} f^{-1}(y)$.*

Определение 1.5. Функция $f : X \to Y$ называется

- инъективной, если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$;
- сюръективной, если $\operatorname{Im} f = Y$;
- биективной, если она и инъективна, и сюръективна.

Определение 1.6. Пусть $f : X \to Y$ и $g : Y \to Z$ – функции. Композицией $g \circ f$ называется функция из X в Z, заданная формулой $g \circ f(x) = g\big(f(x)\big)$ для любого $x \in X$. Композиция $g \circ f$ определена, только если множество значений функции f совпадает с областью определения функции g.

Тождественной функцией $id_X : X \to X$ называется функция, заданная формулой $id_X(x) = x$. Часто индекс X в обозначении тождественной функции опускают.

Функция $f^{-1} : Y \to X$ называется обратной к функции $f : X \to Y$, если $f^{-1} \circ f = id_X$, а $f \circ f^{-1} = id_Y$.

Лемма 1.7. *Пусть $f : X \to Y$ и $g : Y \to Z$ – функции.*

(1) *Если $g \circ f$ инъективна, то f инъективна.*
(2) *Если $g \circ f$ сюръективна, то g сюръективна.*
(3) *Для функции f существует обратная тогда и только тогда, когда она биективна.*

Обратите внимание, что полный прообраз точки обозначается так же, как и значение обратной функции в этой точке. Это обычно не ведет к недоразумению, потому что если неизвестно, что f биективна, то про обратную функцию говорить нельзя, и $f^{-1}(y)$ означает полный прообраз точки y; если же f оказалась биекцией, то прообраз точки состоит из 1 элемента, и мы просто отождествляем одноэлементное множество с его элементом.

Полный прообраз точки называется еще слоем функции. Ясно, что область определения разбивается в дизъюнктное объединение слоев: для $f : X \to Y$

$$X = \coprod_{y \in Y} f^{-1}(y).$$

Обратно, если $X = \coprod_{i \in I} X_i$, то функция $\pi : X \to I$, заданная равенством $\pi(x) = i \iff x \in X_i$, имеет множества X_i своими слоями. Более того, π удовлетворяет следующему универсальному свойству: для любой функции $f : X \to Y$, постоянной на каждом X_i, существует единственная функция $g : I \to Y$ такая, что $g \circ \pi = f$.

2. Отношения эквивалентности

Определение 2.1. Отношением на множестве X называется подмножество в $X \times X$.

Если R – отношение на X, то вместо $(x, y) \in R$ обычно пишут xRy. Это связано с тем, что конкретные отношения обычно обозначаются значками типа $\sim$ или $\geqslant$, а не буквами.

Определение 2.2. Отношение $\sim$ на множестве X называется отношением эквивалентности, если для любых $x, y, z \in X$ выполнены следующие условия:

(1) $x \sim x$ (рефлексивность);
(2) $x \sim y \iff y \sim x$ (симметричность);
(3) $x \sim y \,\&\, y \sim z \implies x \sim z$ (транзитивность).

Определение 2.3. Пусть $\sim$ – отношение эквивалентности на X, а $x \in X$. Классом эквивалентности, содержащим x, называется множество всех элементов, эквивалентных x.

Лемма 2.4. *Два класса эквивалентности либо не пересекаются, либо совпадают. Множество X распадается в дизъюнктное объединение классов эквивалентности.*

Таким образом, отношение эквивалентности задает разбиение множества в дизъюнктное объединение классов эквивалентности. Как мы видели в предыдущем параграфе, мы можем построить сюръективную функцию, слоями которой будут классы эквивалентности.

Определение 2.5. Фактормножеством X по эквивалентности $\sim$ называется множество классов эквивалентности. Оно обозначается через $X/\sim$.

Функция $\pi : X \to X/\sim$, отображающая элемент x в класс эквивалентности, который его содержит, называется канонической проекцией или факторотображением.

Каноническая проекция удовлетворяет следующему универсальному свойству.

Лемма 2.6. *Пусть $\sim$ – отношение эквивалентности на X, а $\pi : X \to X/\sim$ – каноническая проекция. Для любой функции $f : X \to Y$ такой, что $f(x_1) = f(x_2)$ для любых $x_1 \sim x_2$, существует единственное отображение $g : X/\sim \to Y$ такое, что $g \circ \pi = f$.*

3. Алгебраические структуры

Определение 3.1. Операцией называется функция $X_1 \times \cdots \times X_n \to X$. Чаще всего рассматривается ситуация, когда $X_1 = \cdots = X_n = X$. В этом случае операция называется n-арной операцией на множестве X. Декартово произведение пустого набора множеств по определению равно одноточечному множеству. Поэтому 0-арная операция на X – это выбор фиксированной точки множества X. 1-арная операция называется унарной, а 2-арная – бинарной. Бинарные операции обычно обозначаются не буквами, а значками, например $\star$, и вместо $\star(x, y)$ пишут $x \star y$.

Пусть X – множество, а $\star$ – бинарная операция на X. Рассмотрим следующие свойства.

(1) $\forall x, y, z \in X : \ (x \star y) \star z = x \star (y \star z)$ (ассоциативность).
(2) $\exists e \in X \ \forall x \in X : \ e \star x = x \star e = x$ (e называется нейтральным элементом).
(3) $\forall x \in X \exists x' \in X : \ xx' = x'x = e$ (x' называется элементом обратным к x).
(4) $\forall x, y \in X : \ x \star y = y \star x$ (коммутативность).

Определение 3.2. Множество X с операцией $\star$ называется

– полугруппой, если операция ассоциативна;
– моноидом, если операция ассоциативна и существует нейтральный элемент;
– группой, если выполнены свойства (1)–(3).

Полугруппа, моноид или группа называется коммутативной, если выполнено свойство (4). Коммутативную группу называют абелевой группой.

Элемент моноида называется обратимым, если для него существует обратный.

Нейтральный элемент относительно операции умножения обычно обозначается символом 1, а относительно сложения – 0. Если из контекста неясно, нейтральным элементом какого множества является данный элемент, то пишут e_X, 1_X и 0_X для нейтрального элемента множества X относительно различных операций.

Обратный к x элемент относительно сложения обозначается через $-x$, относительно других операций – через x^{-1}.

Лемма 3.3. *Нейтральный элемент единственен (это утверждение не зависит даже от ассоциативности).*

Если операция ассоциативна и обладает нейтральным элементом, то элемент, обратный к данному, единственный.

Лемма 3.4. *Если в моноиде M элементы x и y обратимы, то $x \star y$ обратим, причем $(x \star y)^{-1} = y^{-1} \star x^{-1}$.*

Множество обратимых элементов моноида является группой. Мы будем обозначать это множество через M^*.

Определение 3.5. Пусть теперь на множестве R заданы операции сложения и умножения, причем R является абелевой группой по сложению и полугруппой по умножению. Предположим, что выполнено следующее свойство:

5. $\forall x, y, z \in R : (x + y)z = xz + yz$ и $z(x + y) = zx + zy$ (дистрибутивность).

Тогда R называется (ассоциативным) кольцом.

Если существует нейтральный элемент по умножению, то кольцо называется кольцом с единицей, если умножение коммутативно, то коммутативным кольцом.

Поле – это коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Лемма 3.6. *Для любого элемента r произвольного кольца R: $0 \cdot r = r \cdot 0 = 0$.*

Если R – кольцо с единицей, то $(-1) \cdot r = -r$.

Как следует из леммы 3.4, множество обратимых (по умножению) элементов кольца R является группой. Эта группа называется мультипликативной подгруппой кольца и обозначается через R^*.

Примеры колец и полей.

(1) $\mathbb{Z}$ ($\mathbb{N}$ не является кольцом!).
(2) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля.
(3) $\mathbb{Z}_n = \{0, \dots, n-1\}$, сложение $a +_n b = a + b \mod n$, умножение $a *_n b = ab \mod n$. $\mathbb{Z}_n$ является полем тогда и только тогда, когда n – простое число.
(4) $\mathrm{M}_n(R)$ – множество матриц с элементами из кольца R с обычными операциями сложения и умножения матриц (некоммутативное кольцо).
(5) $R[t]$ – кольцо многочленов с коэффициентами из коммутативного кольца R.

Примеры групп.

(1) $(R, +)$, где R – кольцо.
(2) Циклические группы $C = \{a^m \mid m \in \mathbb{Z}\}$ с операцией $a^x a^y = a^{x+y}$. При этом может оказаться, что $a^k = a^l$ при $k \neq l$. Тогда $a^{k-l} = e$. Если n – наименьшее натуральное число такое, что $a^n = 0$, то $C = C_n = \{e, a, \dots, a^{n-1}\}$, а $a^x a^y = a^{x+y \mod n}$. Если же такого n не существует, то все элементы a^m различны. Ясно, что в первом случае C_n – это просто $\mathbb{Z}_n$ в мультипликативных обозначениях, а бесконечная циклическая группа – это $\mathbb{Z}$ в мультипликативных обозначениях.
(3) R^* – мультипликативная группа кольца R с 1, т. е. множество обратимых (по умножению) элементов кольца с операцией умножения. В частности, $\mathrm{GL}_n(R)$ – полная линейная группа степени n над кольцом R – мультипликативная группа кольца $\mathrm{M}_n(R)$. Подгруппы в $\mathrm{GL}_n(R)$: $\mathrm{SL}_n(R)$ – множество матриц с определителем 1 (R – коммутативное кольцо); $\mathrm{D}_n(R)$ – множество обратимых диагональных матриц; $\mathrm{B}_n(R)$ – множество обратимых верхнетреугольных матриц; $\mathrm{U}_n(R)$ – множество верхнетреугольных матриц с 1 по диагонали.
(4) Группа самосовмещений геометрической фигуры, т. е. биекций геометрической фигуры на себя, не меняющих расстояний между точками. Операцией является композиция. Например, диэдральная группа D_n – группа самосовмещений правильного n-угольника. Она состоит из n поворотов, включая поворот на 0 градусов, т. е. тождественное отображение, и n осевых симметрий.

4. Симметрическая группа

Одним из важных примеров групп является симметрическая группа. Обозначим $[n] = \{1, \dots, n\}$.

Определение 4.1. Пусть X – множество. Множество биекций $X \to X$ с операцией композиции называется симметрической группой множества X и обозначается через S_X. Если $X = [n]$, то S_X обозначается через S_n и называется симметрической группой порядка n.

Ясно, что множество всех функций $X \to X$ является моноидом (нейтральный элемент – тождественное отображение $id(x) = x \forall x \in X$), а S_X является его группой обратимых элементов. Далее будем изучать группу S_n. Тождественная перестановка обычно обозначается буквой e. Вместо композиции обычно говорят о произведении перестановок, при этом значок композиции опускают.

Перестановку можно записать в табличной форме: в первой строке аргументы (обычно упорядоченные по возрастанию), а во второй – значения. Однако для приложений в теории групп гораздо удобнее использовать циклическую запись. Цикл $\sigma = (i_0\, i_2\, \dots\, i_{n-1})$ – это перестановка, заданная равенствами $\sigma(i_k) = i_{k+1 \mod n}$ и оставляющая на месте все остальные элементы из $[n]$. Циклы $(i_0 \dots i_{n-1})$ и $(j_0 \dots j_{m-1})$ называются независимыми, если $i_k \neq j_l$ ни при каких k, l. Цикл длины 1 – это тождественная перестановка. Ясно, что любую перестановку можно записать в

виде произведения независимых циклов, причем такая запись единственна с точностью до: (1) циклов длины 1, (2) перестановки независимых циклов, (3) циклической перестановки элементов каждого цикла.

Транспозицией называется цикл длины 2.

Определение 4.2. Пусть $\sigma \in S_n$. Инверсией называется пара (i, j), $1 \leqslant i < j \leqslant n$, такая, что $\sigma(i) > \sigma(j)$. Четность количества инверсий называется четностью перестановки σ.

Лемма 4.3. *Любая перестановка записывается в виде произведения транспозиций соседних индексов.*

Доказательство. Если $\sigma \neq e$, то существует индекс i такой, что $\sigma(i) > \sigma(i+1)$. Тогда в перестановке $\sigma \circ (i\, i+1)$ инверсий на 1 меньше, чем в σ. Далее индукция по числу инверсий. □

Лемма 4.4. *Если перестановка представлена в виде произведения m транспозиций соседних индексов, то ее четность равна четности m.*

Доказательство. Если $\sigma(i) > \sigma(i+1)$, то в перестановке $\sigma \circ (i\, i+1)$ инверсий на 1 меньше, чем в σ, в противном случае – на 1 больше. □

Теорема 4.5. *Отображение $\varepsilon : S_n \to \mathbb{Z}_2$, сопоставляющее перестановке ее четность, удовлетворяет соотношению $\varepsilon(\sigma\tau) = \varepsilon(\sigma) + \varepsilon(\tau) \mod 2$.*

5. Простейшие конструкции

Определение 5.1. Непустое подмножество H группы G называется подгруппой, если $ab, a^{-1} \in H$ для любых $a, b \in H$.

Непустое подмножество R кольца A называется подкольцом, если $a+b, -a, ab \in R$ для любых $a, b \in R$.

Если $a \in H$, то $a^{-1} \in H$, а, следовательно, и их произведение равное нейтральному элементу лежит в подгруппе H. Аналогично любое подкольцо содержит 0. Ясно, что подгруппа (подкольцо) сама являются группой (соотв., кольцом) относительно тех же операций, которые заданы в объемлющей группе (соотв., кольце).

Если H – подгруппа в G, то пишут $H \leqslant G$ (аналогичное обозначение для подкольца не используется).

В любой группе есть две тривиальные подгруппы: сама группа и множество состоящее из одного нейтрального элемента. Конечно, кольцо является подкольцом самого себя. По умолчанию мы всегда будем рассматривать кольца с 1 и считать, что подкольцо содержит единицу самого кольца. При этой договоренности нулевое подмножество $\{0\}$ ненулевого кольца не является подкольцом.[1]

Прямым произведением алгебраических структур одного типа называется декартово произведение множеств с покомпонентными операциями. В случае, если одна из операций называется сложением, обычно говорят о прямой сумме, а не о прямом произведении. Надо отметить, что эта терминология не совпадает с терминологией теории категорий, которая приобретает все большую популярность. Дадим более подробные определения для групп и колец.

Определение 5.2. Пусть G_1 и G_2 – группы с операциями $\star_1$ и $\star_2$ соответственно. Прямое произведение $G = G_1 \times G_2$ – это декартово произведение G_1 и G_2 с операцией $\star$, заданной следующим образом: $(g_1, g_2) \star (h_1, h_2) = (g_1 \star_1 h_1, g_2 \star_2 h_2)$, где $g_1, h_1 \in G_1$, а $g_2, h_2 \in G_2$.

Аналогично определяется прямое произведение любого (даже не обязательно конечного) семейства групп. Если группы коммутативны, операция обозначена знаком $+$, а их количество

[1] При этом нулевое кольцо является кольцом с 1. Действительно, в нем $1 = 0$.

конечно, то вместо термина “прямое произведение” обычно употребляют термин “прямая сумма” и обозначают ее знаком $\bigoplus$, например, $G = \bigoplus\limits_{k=1}^{n} G_n$.

Кольцо R называется прямой суммой колец R_1 и R_2, если $R = R_1 \times R_2$, $(r_1, r_2) + (s_1, s_2) = (r_1 + s_1, r_2 + s_2)$ и $(r_1, r_2) \cdot (s_1, s_2) = (r_1 \cdot s_1, r_2 \cdot s_2)$, где $r_1, s_1 \in G_1$, а $r_2, s_2 \in G_2$. В этом случае пишут $R = R_1 \bigoplus R_2$.

Аналогично определяется прямая сумма любого конечного количества колец. Для бесконечного семейства колец подобная конструкция называется прямым произведением, а термин прямая сумма оставлен для множества последовательностей, у которых только конечное число элементов отлично от нуля (при этом прямая сумма бесконечного семейства ненулевых колец не имеет единицы, даже если все кольца семейства ее имеют!).

Лемма 5.3. *Мультипликативная группа прямой суммы конечного семейства колец равна прямому произведению мультипликативных групп этих колец, т. е.* $\left(\bigoplus\limits_{k=1}^{n} R_n\right)^* = \underset{k=1}{\overset{n}{\times}} R_n^*$.