КОНСПЕКТЫ ЛЕКЦИЙ ПО АЛГЕБРЕ

Автор: *Каляев Тимур*

Давайте для начала немного обсудим, что такое эти самые поля и группы, так как они являются большой частью предмета нашего изучения.

Примерами полей являются привычные нам рациональные числа (которые обозначаются буквой $\mathbb{Q}$) и действительные числа (обозначение: $\mathbb{R}$).

Что можно делать с этими числами? Складывать, вычитать, умножать, делить (только не на ноль!).

Давайте формализуем это понятие.

Полем называется множество F, на котором введены две операции $+$ (сложение) и $\times$ (умножение) так, что:

1. $\forall a, b, c \in F\ (a+b)+c = a+(b+c)$ (*ассоциативность по сложению*);
2. $\forall a, b \in F\ a+b = b+a$ (*коммутативность по сложению*);
3. существует такой элемент $0 \in F$ (называемый *нулём*), что $\forall a \in F\ a+0 = a$;
4. $\forall a \in F\ \exists\ b \in F:\ a+b=0$, элемент b называется *противоположным* к a и обозначается через $-a$;
5. $\forall a, b, c \in F\ (a \times b) \times c = a \times (b \times c)$ (*ассоциативность по умножению*);
6. $\forall a, b \in F\ a \times b = b \times a$ (*коммутативность по умножению*);
7. существует такой элемент $1 \neq 0 \in F$ (называемый *единицей*), что $\forall a \in F\ a \times 1 = a$;
8. $\forall a \in F\ \exists\ b \in F:\ a \times b = 1$, элемент b называется *обратным* к a и обозначается через a^{-1};
9. $\forall a, b, c \in F\ a \times (b+c) = a \times b + a \times c$ (*дистрибутивность*).

Заметим, что рациональные и действительные числа являются полями, но вообще полей (и даже очень полезных!) очень много. В этом семестре мы будем подробно проходить поле комплексных чисел $\mathbb{C}$, которое содержит все корни всех алгебраических уравнений с действительными коэффициентами, а также приведём примеры ещё некоторых полезных полей. В третьем семестре у нас будет отдельная большая тема “поля”, в том числе, мы полностью поймём, какими бывают поля с конечным числом элементов.

Теперь давайте выясним, что такое группа.

Все поля по сложению и поля по умножению без нуля являются группами. Также группой являются целые числа.

Формально, группа $\mathbf{G}$ это множество с операцией $\times$ или $\cdot$ (*умножение*), для которой выполняются следующие аксиомы:

1. $\forall a, b, c \in \mathbf{G}$ $(a \times b) \times c = a \times (b \times c)$ (*ассоциативность по умножению*);

2. существует такой элемент $e \in \mathbf{G}$ (называемый *единицей*), что $\forall a \in \mathbf{G}$ $a \times e = e \times a = a$;

3. $\forall a \in \mathbf{G}\ \exists\, b \in \mathbf{G}: \ a \times b = e$, элемент b называется *обратным* к a и обозначается через a^{-1}.

Оказывается, поля и группы тесно связаны с теорией Галуа, благодаря которой мы сможем доказать теорему о неразрешимости алгебраических уравнений степени $\geqslant 5$, а также доказать, что неразрешимы следующие две древние задачи:

1. Циркулем и линейкой разделить угол на три равные части;

2. Циркулем и линейкой построить куб, объём которого в 2 раза больше данного куба.

2. Задача о состояниях многоатомной молекулы

Пусть у нас имеется какая-то фигура на плоскости или в пространстве. Рассмотрим все ее движения (то есть отображения точек этой фигуры в себя, сохраняющие расстояния). На множестве таких движений можно ввести операцию композции (ещё её называют суперпозицией) $\circ$. Множество всех движений будет удовлетворять аксиоме ассоциативности (композиция всегда ассоциативна).

Кроме того, всегда существует тождественное движение (ни одна точка фигуры не двигается), композиция которого с любым другим движением не меняет это движение.

Наконец, к любому движению можно подобрать обратное: возьмем наше движение и отобразим все точки в обратную сторону.

Таким образом, множество движений любой фигуры является группой относительно операции композиции. Эта группа также называется группой симметрий данной фигуры.

Теперь рассмотрим некоторую молекулу — это система частиц (атомных ядер, окруженных электронами). Если в начальный момент времени конфигурация системы близка к равновесной, то частицы, входящие в систему, всегда будут оставаться около положения равновесия и не будут приобретать больших скоростей. Движения такого типа называются колебаниями относительно равновесной конфигурации, а система — устойчивой.

Любое малое колебание молекулы вблизи положения устойчивого равновесия является композицией так называемых нормальных колебаний. Часто можно определить все параметры молекулы (потенциальную энергию, нормальные частоты), зная внутренние симметрии молекулы.

Внутренние симметрии — это группа, как мы уже знаем. Изучение данной группы (ее представления, например) очень полезно, так как даёт нам возможность посчитать параметры колебания молекулы.

Таким образом, на сегодняшний день развитие структурной теории молекул невозможно себе представить без теории групп.

Гораздо более ранние (но до сих пор идущие) применения теории групп относятся к кристаллографии.

Еще в 1891 году русский кристаллограф Е.С. Федоров, а затем немецкий ученый А.Шенфлис нашли 230 пространственных кристаллографических групп, описывающих все имеющиеся в природе симметрии кристаллов.

3. Задача о кодировании сообщения

В конструировании автоматических систем связи, наземных или космических, обычно в качестве элементарного сообщения берется упорядоченная последовательность — строка (или слово)

$$a = (a_1, a_2, \ldots, a_n)$$

длины n, где $a_i = 0$ или 1.

Так как операции сложения и умножения по модулю два совершенно естественны для компьютера, то поле из двух элементов $\mathbb{F}_2$ или $\mathbb{Z}_2$ — необходимый атрибут специалиста по обработке информации.

Это поле с такими правилами сложения:

$$0 + 0 = 1 + 1 = 0 \text{ и } 0 + 1 = 1 + 0 = 1$$

умножения —

$$0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 \text{ и } 1 \cdot 1 = 1.$$

Иногда удобно использовать в качестве символов a_i элементы других конечных полей (например, поля $\mathbb{F}_{2^k}$ из 2^k элементов, которое существует для любого натурального k).

С целью исключения помех, способных превратить 0 в 1 или наоборот, приходится брать a досаточно длинным и использовать специальную систему кодирования — выбор такого подмножества (кода) S_0 передаваемых строк из всего множества S, чтобы было возможно восстановить слово a по искаженному передаваемому слову a' при условии, что произошло не слишком много ошибок. Так возникают *коды, исправляющие ошибки*.

Алгебраическая теория кодирования, которая развивается последние несколько десятилетий, очень в большой степени основана на теории полей. Она будет проходится на старших курсах в курсе дискретной математики, когда теория полей уже может немного забыться.

Кроме приведённых примеров использования теории групп и теории полей хочется сказать, что очень важной для практических задач дисциплиной является линейная алгебра — сейчас она нужна как для абсолютно всех других предметов высшей математики (функциональный анализ, теория вероятностей и математическая статистика, дифференциальные уравнения и уравнения в частных производных, вычислительная математика, дифференциальная геометрия и т.д.), так и для совершенно практических задач (например, машинного обучения).

В этом семестре мы в основном будем заниматься изучением самых первых основ линейной алгебры, базовыми понятиями теории групп и теории полей, а также многочленами.

Второй семестр будет полностью посвящен линейной алгебре, третий — теории групп, теории полей и колец, представлениям групп, а также основам теории Галуа.

СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

Линейные уравнения $ax = b$ и системы вида

$$\begin{cases} ax + by = e, \\ cx + dy = f \end{cases}$$

с вещественными коэффициентами решаются в средней школе. Наша цель — научиться оперировать с системой линейных алгебраических уравнений самого общего вида

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{12n}x_n = b_2, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m. \end{cases}$$

Здесь m и n — произвольные натуральные числа.

Для удобства всегда будем считать, что элемент a_{ij} находится в i-м уравнении при переменной x_j. Число b_i называется свободным членом i-го уравнения. Система называется однородной, если все $b_i = 0$, $i = 1, 2, ..., m$.

При любых b_i линейную систему

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{12n}x_n = 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{cases}$$

называют *однородной системой, ассоциированной* с исходной.

Коэффициенты при неизвестных составляют прямоугольную таблицу,

$$\begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots\dots & \dots\dots \\ a_{m1} & a_{m2} \dots a_{mn} \end{pmatrix},$$

называемую матрицей размера $m \times n$ и сокращенно обозначаемую символом (a_{ij}) или просто A. Естественно говорить об i-й строке или j-м столбце этой матрицы, а в случае квадратной матрицы $(m = n)$ — ещё и о главной диагонали, состоящей из элементов $a_{11}, a_{22}, ..., a_{nn}$.

Матрица, у которой все элементы вне главной диагонали равны нулю, обозначается иногда через

$$\mathrm{diag}(a_{11}, a_{22}, ..., a_{nn})$$

и называется диагональной матрицей, а при $a_{11} = a_{22} = \dots = a_{nn} = a$ обозначается aE — скалярная матрица.

Наряду с матрицей коэффициентов рассматривают и расширенную матрицу $(a_{ij}|bi)$, получающуюся из исходной добавлением столбца свободных членов.

Если каждое из уравнений нашей линейной системы обращается в ноль после замены неизвестных x_i числами x_i^0, то упорядоченный набор из n чисел $x_1^0, x_2^0, \dots, x_n^0$ называется решением системы.

Система, не имеющая ни одного решения, называется несовместной. Если у системы есть решение, то она называется совместной. Если при этом оно единственно, то система называется определённой. Если у системы больше одного решения, то она называется неопределённой.

ПОРЯДОК ЭЛЕМЕНТА ГРУППЫ

Рассмотрим целые степени элемента a группы G

$$\dots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \dots$$

Возможны два случая

Случай 1 *Все элементы в этом ряду различны (т. е. $a^k \neq a^l$ для всех целых чисел $k \neq l$). В этом случае будем говорить, что порядок элемента бесконечный (обозначение: $O(a) = \infty$).*

Случай 2 *В этом ряду $a^k = a^l$ для некоторых $k \neq l$. Пусть $k > l$. Тогда $a^{k-l} = e$, где $k - l > 0$, т. е. встретилась и натуральная степень элемента a, равная e.*

Рассмотрим множество:

$$T = \{t \in \mathbb{Z} \mid t > 0,\ a^t = e\} \tag{1}$$

Это непустое подмножество натуральных чисел. Следовательно, в T существует наименьший элемент n, который мы назовем порядком элемента a и обозначим через $O(a)$

Таким образом:

1. $a^n = e,\ n > 0$;
2. если a^k, $k > 0$, то $k \geqslant n$.

Ясно, что если группа G конечна, то $O(g) < \infty$ для всех $g \in G$.

Лемма 1 *Если $O(a) = n < \infty$, то*

1. *все элементы $e = a^0, a, a^2, \ldots, a^{n-1}$ различны;*
2. *для любого $k \in \mathbb{Z}$ элемент a^k совпадает с одним из $e, a, a^2, \ldots, a^{n-1}$, а именно, если $k = nq + r$, где $0 \leq r < n$, то $a^k = a^r$.*

Доказательство

1. Следует из определения порядка элемента $O(a)$.
2. Пусть $k \in \mathbb{Z}$. Тогда $k = nq + r$, где $0 \leq r < n$. Следовательно, $a^k = (a^n)^q a^r = ea^r = a^r$. $\square$

Лемма 2 *Пусть $O(a) = n < \infty$. Тогда $a^k = e$ тогда и только тогда, когда $k = nq$.*

Доказательство

1. Если $k = nq$, то $a^k = (a^n)^q = e^q = e$.
2. Допустим противное, т.е. что $k = nq + r$, где $0 \leq r < n$. Тогда, $a^k = (a^n)^q a^r = ea^r = a^r \neq e$ (по лемме 1). Получили противоречие $\square$