Семинар №1 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Определение 1 Полугруппа . . . 1
Определение 2 Моноид . . . 2
Определение 3 Группа . . . 3
Определение 4 Абелева группа . . . 3
Определение 5 Группа (мультипликативная запись) . . . 3
Определение 6 Порядок группы . . . 4
Задача 1 Корни из единицы . . . 4
Задача 2 Единственность единицы . . . 5
Лемма 1 Обратное к произведению . . . 5
Лемма 2 Решение уравнений . . . 5
Задача 3 Нейтральные квадраты . . . 5

Предисловие

В ходе вашего знакомства с математикой вы изучали различные множества и операции с ними. Вам приходилось складывать и умножать числа, вектора и матрицы, работать с остатками от деления или производить композиции отображений. Нетрудно заметить, что у многих подобных операций есть схожие свойства. Именно изучением подобных свойств мы и займемся в курсе. В алгебре рассматриваются абстрактные множества и операции над ними с заданными свойствами, без уточнения конкретной природы этих множеств и операций, изучаются их свойства. Зачастую, полученные результаты оказываются обобщением более частных знакомых вам результатов.
Давайте посмотрим на базовые *алгебраические структуры*, которые встретятся нам в курсе, и задумаемся, почему рассматриваются именно они.

Замечание 1
В зависимости от литературы, приведенные определения могут отличаться, как оставаясь эквивалентными, так и изменяя определяемое понятие.

Начнем с серии структур, которые содержат всего одну бинарную операцию. Для начала посмотрим на случай, когда накладывается всего одно требование, которое используется для подавляющего большинства операций в алгебре — *ассоциативность*.

Определение 1 (Полугруппа)
Полугруппой называется множество M с заданной на нем операцией $+ : M \times M \to M$, которая удоволетворяет следующим свойствам:

$$\forall\ a, b, c \in M :\ (a + b) + c = a + (b + c) \tag{1}$$

В получившейся структуре мы уже вполне резонно можем записать уравнение $a + x = b$, где под знаком равенства понимается, что слева и справа стоит один и тот же элемент множества M. Для некоторых таких уравнений может существовать решение, для других же — нет. Рассмотрим это на таком примере:

Пример 1
Рассмотрим следующий пример полугруппы. В качество множества M возьмем все конечные последовательности из букв a и b. В качестве операции у нас будет $\bullet$ — результатом $\alpha \bullet \beta$ будет слово β, приписанное справа к α, например $bab \bullet aab = babaab$.
Тогда решением уравнения $bab \bullet x = babbb$ будет слово bb, в то время как у уравнения $bab \bullet x = aa$, очевидно, решений нет.

Логично добавить еще одно требование, а именно пожелать, что бы у нашей операции был некий аналог нуля для сложения или единицы для умножения. Обычно элемент, который обладает такими свойствами называют *нейтральным* или *единичным* элементом.

Определение 2 (Моноид)
Моноидом называется множество M с заданной на нем операцией $+ : M \times M \to M$, которая удоволетворяет следующим свойствам:

$$\forall\ a, b, c \in M :\ (a + b) + c = a + (b + c) \tag{1}$$
$$\exists!\ e \in M\ \forall\ a \in M :\ a + e = e + a = a \tag{2}$$

Пример 2
Что бы получить из предыдущего примера моноид, надо добавить в наше множество последовательность из нуля букв, или, как говорят пустое слово *— при его приписывании ничего не происходит.*

Пример 3
Без доказательств приведем примеры моноидов:

$$(\mathbb{N}_0, +); (\mathbb{N}, *); (\Sigma^*, \cdot); (\mathbb{N}, HOK); (\mathbb{R} \cup \{+\infty\}, \min); (2^M, \cup); (\{0, 1\}, \wedge)$$

Пример 4
У уравнения $0 \wedge x = 0$ в моноиде $(\{0, 1\}, \wedge)$ два решения.

Однако просто записывать уравнения — недостаточно, хотелось бы что бы у уравнения $a + x = b$ всегда было одно решение: $x = -a + b$. Для этого определим, что вообще значит $-a$: это такое число, которое вместе с a дает нейтральный элемент. $-a$ называют *обратным* к a элементом.

Определение 3 (Группа)
Группой называется множество M с заданной на нем операцией $+ : M \times M \to M$, которая удоволетворяет следующим свойствам:

$$\forall\ a, b, c \in M :\ (a + b) + c = a + (b + c) \tag{1}$$
$$\exists!\ e \in M\ \forall\ a \in M :\ a + e = e + a = a \tag{2}$$
$$\forall\ a \in M\ \exists!\ -a \in M :\ -a + a = a + -a = e \tag{3}$$

Именно группы и будут в основном изучаться в первой части курса.

Пример 5
Без доказательств приведем примеры групп:

$$(\mathbb{Z}, +); (Q^*, *); (\mathbb{Z}/n\mathbb{Z}, +); (\mathbb{R}^n, +); (\textit{матрицы одинакового размера}, +)$$

$$(\{0, 1\}, \oplus); (\textit{невырожденные квадратные матрицы одинакового размера}, *); \textit{etc...}$$

Более подробно с примерами групп мы ознакомимся далее по семинару и в течение курса. Заметим, что нигде ранее мы не требовали *коммутативности* нашей операции, хотя это свойство выполняется во многих частных случаях.

Определение 4 (Абелева группа)
Абелевой или коммутативной группой называется группа $G = (M, +)$, такая что

$$\forall\ a, b \in M :\ a + b = b + a$$

Группы

До этого мы использовали для записи нотацию, в которой все напоминало сложение: для операции мы использовали плюсик, обратный элемент обозначали минусом, а единичный элемент тогда логично было бы обозначать ноликом. Но это — суть есть просто обозначения. Зачастую, оказывается удобным другая запись — ассоциированая с умножением. Обратный элемент в ней обозначается -1 степенью, а нейтральный — единицей. Эти записи называются аддитивная и мультипликативная.

Определение 5 (Группа (мультипликативная запись))
Группой называется множество M с заданной на нем операцией $* : M \times M \to M$, которая удоволетворяет следующим свойствам:

$$\forall\ a, b, c \in M :\ (a * b) * c = a * (b * c) \tag{1}$$
$$\exists!\ e \in M\ \forall\ a \in M :\ a * e = e * a = a \tag{2}$$
$$\forall\ a \in M\ \exists!\ a^{-1} \in M :\ a^{-1} * a = a * a^{-1} = e \tag{3}$$

Замечание 2
Свойство ассоциативности позволяет нам отбросить все скобки в некотором сложном выражении (формальное доказательство по индукции есть в учебнике).
В дальнейшем мы часто и будем это делать, в частности, будем использовать такие сокращения:

$$\underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ раз}} = a^n \quad \underbrace{a + a + \dots + a}_{n \text{ раз}} = na$$

Сформулируем это все еще раз в виде таблички.

Название	Мультипликативная	Аддитивная
Знак операции	$*$	$+$
Распространенное обозначение единицы	$e = 1$	$e = 0$
Обозначение обратного элемента	$-a$	a^{-1}
Повторное применение операции	na	a^n

Заметим, что мы не уточняли, сколько элементов должно быть в группе. Это количество может быть как конечным, так и бесконечным.

Определение 6 (Порядок группы)
Порядок группы — мощность носителя группы, то есть, для конечных групп — количество элементов группы. Обозначается |G| или Ord(G).

Зачастую, с ходу бывает не понятно, является ли данное множество с данной операцией группой. Продемонстрируем, как следует поступать в данном случае.

Задача 1 (Корни из единицы)
Образуют ли группу комплексные корни из единицы n-ой степени (решения уравнения $z^n = 1$) с операцией умножения?

Решение Проверим все свойства по очереди:

1. Замкнутость: $\forall z_1, z_2 \in \mathbb{C}\ z_1^n = z_2^n = 1 \to (z_1 z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1$
2. Ассоциативность определяется свойствами комплексных чисел.
3. Наличие нейтрального элемента. Свойствам нейтрального элемента по умножению удовлетворяет единица. Кроме того, $1^n = 1$, т. е. она входит в множество решений.
4. Наличие обратного элемента. Для каждого не нулевого комплексного числа $z \in \mathbb{C}$ есть обратное $z^{-1} : z \cdot z^{-1} = 1$. Кроме того, $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$, т. е. оно входит в множество решений.

А значит все выполнено, образуют.

Определив, что такое группа мы можем доказывать некоторые утверждения опираясь только на определение группы. Они будут верны вне зависимости от природы группы. Сформулируем несколько утверждений, истинных для всех групп.

Единственность единицы не обязательно требовать в её определении. Докажем её единственность из остального определения.

Задача 2 (Единственность единицы)
Пусть существование единицы задано так:

$$\exists e \in M \ \forall a \in M : \ a * e = e * a = a$$

Доказать, что такой элемент e единственный.

Решение Пусть условие выполняется для некоторых элементов e и e'. Тогда

$$e' = e \cdot e' = e$$

Левое равенство выполняется, так как e является единицей, правое — так как e' единица.

Лемма 1 (Обратное к произведению)
В любой группе для любых элементов a и b выполняется

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Доказательство

$$(b^{-1}a^{-1}) \cdot (ab) = b^{-1} \cdot (a^{-1}a) \cdot b = b^{-1} \cdot e \cdot b = b^{-1}b = e$$

Лемма 2 (Решение уравнений)
Решения в группе уравнений (относительно x)

$$a \cdot x = b \qquad x \cdot a = b$$

единственны.

Доказательство

$$ax = b \iff a^{-1}ax = a^{-1}b \iff x = a^{-1}b$$

Аналогично для второго уравнения.

Задача 3 (Нейтральные квадраты)
Известно, что в группе $\forall\ a \in M : a^2 = e$. Докажите, что данная группа абелева.

Доказательство $ab = abe = ab(aa) = abaea = aba(bb)a = (ab)(ab)ba = ba$

Таблицы Кэли

Для удобной записи всевозможных результатов групповой операции (в первую очередь, в конечных группах) можно построить «таблицу умножения».
Запишем в заголовках столбцов и строк элементы группы, как-нибудь их назвав (условимся обозначать их первыми буквами латинского алфавита, кроме нейтрального — его обозначаем e); в ячейках таблицы результат $a \cdot b$, где a — элемент по строке, b — по столбцу.
Такие таблицы называются таблицами Кэли.

Пример 6
Таблица Кэли для группы $(\mathbb{Z}/3\mathbb{Z}, +)$

	0	*1*	*2*
0	*0*	*1*	*2*
1	*1*	*2*	*0*
2	*2*	*0*	*1*

Так как, в связи с коммутативностью сложения, группа абелева, таблица симметрична относительно диагонали.

Сформулируем несколько утверждений о виде таблиц Кэли на основе того, что мы знаем о группах.

1. Условимся, что первая строка и первый столбец соответствуют нейтральному элементу группы. Тогда первые строка и столбец любой таблицы Кэли будут выглядеть однозначным образом (в клетке $e \cdot a$, очевидно, стоит a и т.д.).

2. Так как решения уравнений $a \cdot x = b$ и $x \cdot a = b$ единственны, то в каждой строке и в каждом столбце всякий элемент стоит не более одного раза. Так как вся таблица должна быть заполнена, то всякий элемент стоит в строке и столбце *ровно один раз.*

3. Так как обратный элемент единственнен, то $ab = e \Leftrightarrow ba = e$, поэтому единичные элементы должны располагаться симметрично относительно главной диагонали.

Пользуясь этими правилами (в основном, первыми двумя), можно частично или даже полностью заолнять таблицы Кэли, ничего не зная про группу или имея частичную информацию. Приведем пару примеров, решая их как судоку.

Пример 7
Руководствуясь правилами судоку, получаем ***единственный*** *вид таблицы для групп порядка 2 и 3.*

	e	a
e	e	a
a	a	e

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Замечание 3
Мы получили единственный вид таблицы Кэли для групп порядка 2 и 3. Конечно, говорить, что групп таких порядков всего есть по одной неправильно: обозначенные буквами элементы и операция над ними могут иметь различную природу. Но групповые свойства у них будут одинаковыми. Это пример ***изоморфизма*** *групп, речь о котором пойдет на следующих семинарах.*

Стоит отметить, что сформулированные условия являются необходимыми, но недостаточными для того, чтобы полученная конструкция была группой. То есть не всякая таблица, заполненная «по правилам судоку» (даже учитывающая все три пункта) является таблицей Кэли некоторой группы.

Пример 8

Пусть в таблице 5×5 на главной диагонали везде стоят единичные элементы. Положив $a \cdot b = c$ (это непринципиально, c или d), далее всю таблицу можно заполнить как судоку. Получится вот это:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Как было установлено в задаче 4, группа, где квадраты всех элементов единичные, должна быть абелевой, то есть её таблица Кэли — симметричной. Наша таблица таковой не является, значит, это не таблица усноженияни для какой группы.

Замечание 4

Для получения противоречия, достаточно было просто предположить, что $a^2 = e$. Тогда положим $a \cdot b = c$ (например), откуда $b = aab = ac$. По «правилам судоку» для оставшейся клетки остается только вариант $a \cdot d = d$, что невозможно, так как $a \neq e$. Таким образом, единица вообще не может стоять на диагонали (кроме первой ячейки). В дальнейшем мы поймем, что вид группы из пяти элементов вообще может быть только один.