Семинар №3 по курсу «Основы высшей алгебры и теории кодирования»

Репеев Роман, Шиманогов Игорь

Лемма 1 Обратимость вычета по умножению . . . 2
Определение 1 Функция Эйлера . . . 2
Утверждение 1 Вычисление функции Эйлера . . . 2
Определение 2 Мультипликативная группа вычетов . . . 2
Теорема 1 Теорема Эйлера . . . 2
Теорема 2 Малая теорема Ферма . . . 2
Задача 1 Вычисление вычетов . . . 2
Определение 3 Изоморфизм групп . . . 3
Лемма 2 Изоморфизм циклических групп . . . 3
Утверждение 2 Свойства изоморфизма . . . 3
Задача 2 Неизоморфные группы . . . 3
Определение 4 Автоморфизм . . . 4
Утверждение 3 Группа автоморфизмов . . . 4
Утверждение 4 Автоморфизмы циклических групп . . . 4
Определение 5 Перестановка . . . 4
Определение 6 Группа перестановок . . . 5
Определение 7 Циклы . . . 5
Определение 8 Транспозиция . . . 5
Теорема 3 Теорема о транспозициях . . . 5
Определение 9 Четность перестановки . . . 6
Утверждение 5 Порядок перестановки . . . 6
Определение 10 Знакопеременная группа . . . 6
Теорема 4 Кэли . . . 6
Определение 11 Прямое произведение групп . . . 7
Лемма 4 Порядок элемента в произведении . . . 7
Теорема 5 Китайская теорема об остатках . . . 7

Малая теорема Ферма, теорема Эйлера

Лемма 1 (Обратимость вычета по умножению)
$\text{НОД}(k, n) = 1 \iff \exists\, t : t \cdot k = 1 \mod n$

Доказательство Задача из домашки.

Определение 1 (Функция Эйлера)
Пусть $n \in \mathbb{N}, n > 1$. Тогда $\varphi(n)$ — количество натуральных чисел меньших n взаимно простых с n.

Утверждение 1 (Вычисление функции Эйлера)
Пусть p — простое число. Тогда:

- $\varphi(p) = p - 1$
- $\forall n \in \mathbb{N} \quad \varphi(p^n) = p^n - p^{n-1}$
- $\forall n > 1 \quad \varphi(n) = n \prod\limits_q \left(1 - \frac{1}{q}\right)$, где q пробегает значения всех простых делителей n.

Определение 2 (Мультипликативная группа вычетов)
Мультипликативной группой вычетов по модулю n называется множество обратимых элементов аддитивной группы вычетов по модулю n с операцией умножения по модулю n.

Замечание 1
Данная конструкция является группой по своему определению. Ее порядок равен $\varphi(n)$.

Теорема 1 (Теорема Эйлера)
Пусть $a, n \in \mathbb{N},$ НОД $(a, n) = 1, n > 1$ Тогда $a^{\varphi(n)} \equiv 1 \bmod n$.

Доказательство Пусть r — остаток от деления a на n. Тогда $\text{НОД}(r, n) = 1$, поэтому r — элемент мультипликативной группы вычетов. Тогда обозначим порядок r за k. В силу теоремы Лагранжа $\varphi(n) = kq$, тогда по по модулю n: $a^{\varphi(n)} = r^{kq} = 1^q = 1$.

Теорема 2 (Малая теорема Ферма)
Пусть $a, p \in \mathbb{N}, p -$ простое. Тогда $a^{p-1} \equiv 1 \bmod p$

Доказательство Следует из теоремы Эйлера.

Задача 1 (Вычисление вычетов)
Вычислить $10^{111} \bmod 121$.

Решение 10 и $121 = 11^2$ взаимно просты, поэтому по модулю 121 : $1 \equiv 10^{\varphi(121)} \equiv 10^{\varphi\left(11^2\right)} \equiv 10^{11^2 - 11} \equiv 10^{110}$. Витоге , $10^{111} = 10 \cdot 10^{110} \equiv 10 \bmod 121$

Изоморфизм групп

Как мы уже заметили, многие группы ведут себя одинаково, несотря на то, что множество и операция в них могут иметь различную природу. Формализуем этот факт.

Определение 3 (Изоморфизм групп)
Изоморфизмом групп называется $(G, *)$ и $(G', \cdot)$ назвается отображение $\varphi : G \to G'$, такое что:

1. оно биективное

2. $\forall\ a, b :\ \varphi(a * b) = \varphi(a) \cdot \varphi(b)$ (оно уважает/сохраняет операцию)

Группы, между которыми существует изморфизм называются изоморфными, обозначаются $G \cong G'$.

Если группы изоморфны, то с алгебраической точки зрения между ними нет различий: любое свойство группы, которое можно выразить, используя групповую операцию, выполняется или не выполняется в обеих группах одновременно.

Пример 1
Расмотрим две группы, с которыми мы работали больше всего — это аддитивная группа остатков по модулю n и группа корней из единицы n степени. Между ними существует изоморфизм $\varphi :\ \exp \frac{2\pi i k}{n} \to [k]$.

Лемма 2 (Изоморфизм циклических групп)
Все циклические группы одного порядка изморфны друг другу.

Пример 2
Между $(\mathbb{R}, +)$ *и* $(\mathbb{R}_+, \cdot)$ *есть изоморфизм* $x \to e^x$.

Утверждение 2 (Свойства изоморфизма)
Для произвольного изоморфизма верно следующее:

1. он уважает единицу

2. он уважает обратный элемент

3. обратное отображение является изоморфизмом

4. композиция изоморфизмов является изоморфизмом

Когда группы изоморфны, доказать это обычно можно явно предявив изоморфизм между ними. Однако, если не удаётся построить изоморфизм, нужно искать какое-то алгебраическое свойство, различающее эти группы.

Задача 2 (Неизоморфные группы)
$(\mathbb{Q}, +)$ и $(\mathbb{Q}_+, \cdot)$ не изоморфны.

Решение Пусть существует изоморфизм φ. Обозначим $b = \frac{\varphi^{-1}(2)}{2}$. Заметим, что $\varphi(b)^2 = \varphi(b)\varphi(b) = \varphi(b+b) = \varphi(\varphi^{-1}(2)) = 2$, но уравнение $x^2 = 2$ не имеет рационального положительного решения.

Определение 4 (Автоморфизм)
Изоморфизм группы с самой собой называется автоморфизмом.

Очевидно, что хотя бы один автоморфизм всегда существует — это тождественное отображение, однако этим все не исчерпывается. Например, в циклических группах довольно легко придумать нетривиальные изоморфизмы.

Утверждение 3 (Группа автоморфизмов)
Автоморфизмы любой группы G образуют относительно композиции группу, которая называется группой автоморфизмов группы G.

Утверждение 4 (Автоморфизмы циклических групп)
$\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$

Доказательство Идея доказательства состоит в следующем.
Автоморфизм циклической группы задается образом порождающего элемента: $\varphi(1) = k$. Тогда $\varphi(m) = \varphi(\underbrace{1 + \dots + 1}_{m \text{ раз}}) = [mk]$. Для того, чтобы для всех m были различные значения $[mk]$ нужно, чтобы k было взаимно просто с n. А множество таких k и образует $\mathbb{Z}_n^*$.

Группы перестановок

Рассмотрим конечное множество X, состоящее из n элементов. Занумеруем элементы множества X натуральными числами и будем считать, что множество X состоит из этих номеров:

$$X = \{1, 2 \dots n\}$$

Определение 5 (Перестановка)
Перестановкой степени n будем называть биективное отображение (биекцию) n-элементного множества X на себя:

$$\varphi : X \to X; \quad i \to \varphi(i); \quad i = 1, 2, \dots n.$$

Множество всех перестановок степени n будем обозначать символом S_n и для произвольной перестановки $\varphi \in S_n$ будем применять следующую запись:

$$\varphi = \begin{pmatrix} 1 & 2 & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix}$$

Пример умножения (последовательного выполнения, композиции) перестановок

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}; \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ \varphi & \downarrow & \downarrow & \downarrow & \downarrow \\ & 4 & 1 & 3 & 2 \\ \psi & \downarrow & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 & 4 \end{array} \qquad \begin{array}{ccccc} & 1 & 2 & 3 & 4 \\ \psi & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 4 & 1 & 2 \\ \varphi & \downarrow & \downarrow & \downarrow & \downarrow \\ & 3 & 2 & 4 & 1 \end{array}$$

$$\psi\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}; \quad \varphi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Тождественной (единичной) перестановкой называют

$$e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} \in S_n$$

Всякая перестановка $\varphi \in S_n$ имеет обратную $\varphi^{-1} \in S_n$:

$$\varphi\varphi^{-1} = \varphi^{-1}\varphi = e$$

Например:

$$\varphi^{-1} = \begin{pmatrix} 4 & 1 & 3 & 2 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

Определение 6 (Группа перестановок)
Группой перестановок S_n называется множество всех перестановок из n элементов с операцией композиции.

Для алгебры важен ещё один способ записи перестановок: цикловое разложение. В качестве полезного промежуточного шага построим граф перестановки. Это ориентированный граф на множестве вершин $1, 2, ..., n$, в котором из вершины i исходит ровно одно ребро в вершину $\pi(i)$. В силу биективности в каждую вершину этого графа также входит ровно одно ребро. В любом случае ориентированный граф, входящие и исходящие степени вершин которого равны 1, разбивается на непересекающиеся циклы (петли считаем циклами длины 1). Записывая вершины в порядке обхода этих циклов и разделяя циклы скобками, получаем цикловое разложение перестановки. Порядок циклов в записи циклового разложения несущественен. Внутри каждого цикла важен лишь циклический порядок: неважно, какой именно элемент цикла стоит на первом месте.

Определение 7 (Циклы)
Циклом длины n называется перестановка

$$(i_1\ i_2\ \dots\ i_n) = \begin{pmatrix} i_1 & i_2 & \dots & i_{n-1} & i_n \\ i_2 & i_3 & \dots & i_n & i_1 \end{pmatrix}$$

Определение 8 (Транспозиция)
Транспозицией называется цикл длины 2.

Теорема 3 (Теорема о транспозициях)
Любая перестановка представляется как композиция транспозиций.

Доказательство Каждый цикл в разложении можно представить в виде произведения

$$(i_1\ i_2\ \dots\ i_n) = (i_1\ i_2)(i_1\ i_3)\dots(i_1\ i_n)$$

Определение 9 (Четность перестановки)
Четностью перестановки называется четность количества транспозиций в соответствующем разложении.

Конечно, разложения могут быть разными, но четность будет всегда одинаковая (оставим это здесь без доказательства).

Любая перестановка раскладывается в произведение *непересекающихся* циклов, то есть циклов, в которых нет одинаковых номеров. Достаточно очевидно следующее утверждение:

Лемма 3
Непересекающиеся циклы коммутируют.

Ясно также, что порядок цикла равен его длине. Тогда иожем сформулировать полезное

Утверждение 5 (Порядок перестановки)
Порядок перестановки равен НОК длин циклов в ее разложении на непересекающиеся циклы.

Задача 3
Найти всевозможные порядки элементов S_7

Решение Каждая перестановка $\varphi \in S_n$ представима в виде произведения независимых циклов суммарной длины не более n. Порядок произвольной перестановки равен наименьшему общему кратному длин этих циклов.

$$7 = 6+1 = 5+1+1 = 5+2 = 4+3 = 4+2+1 = 4+1+1+1 = 3+3+1 =$$

$$= 3+2+2 = 3+2+1+1 = 3+1+1+1+1 = 2+2+2+1 = 2+2+1+1+1 = 2+1+1+1+1+1$$

Тогда возможные порядки: 7, 6, 5, 10, 12, 4, 3, 2, 1.

Определение 10 (Знакопеременная группа)
Знакопеременной группой A_n называют подгруппу S_n, состоящую из всех чётных перестановок.

Также сформулируем теорему, помогающую получить преставление о том, как выглядит любая конечная группа.

Теорема 4 (Кэли)
Любая конечная группа порядка n является подгруппой симметрической группы S_n.

Доказательство Мы задаем изоморфизм группы G с группой перестановок множества самой группы G.

$$\varphi : G \to S_G \qquad \varphi(a) = \pi_a : \quad \pi_a(x) = a \cdot x$$

Прямые произведения групп. КТО

Определение 11 (Прямое произведение групп)
Прямое произведение групп G и H это группа $G \times H$ с носителем $M_G \times M_H$ и операцией $(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h2)$.

Замечание 2
Нетрудно заметить, что данная конструкция дествительно является группой и верно $G \times H \cong H \times G$. Также выполнено $(G \times H) \times K \cong G \times (H \times K)$, а значит можно говорить о прямом произведении нескольких групп.

Лемма 4 (Порядок элемента в произведении)
Порядок элемента $(g_1, g_2, \dots, g_n) \in G_1 \times G_2 \times \dots \times G_n$ равен НОК порядков g_i.

Доказательство Равенство $(g_1, g_2, \dots, g_n)^k = e$ равносильно тому, что $g_i^k = e$, а значит что k является кратным порядка элемента g_i. Таким образом, k является общим кратным порядков элементов.

Теорема 5 (Китайская теорема об остатках)
Если p, q — взаимно просты, то $C_{pq} \cong C_p \times C_q$.

Доказательство Достаточно указать в группе $C_p \times C_q$ элемент порядка pq. Это пара (a, b), где a — порождающий в C_p, а b — порождающий C_q. Так как p и q взаимно просты, то по лемме о порядке элемента в произведении порядок пары (a, b) равен pq.

Замечание 3
Несколько раз применяя теорему, можно получить, что для произвольного набора взаимно простых чисел $q_1, \dots, q_n$ утверждение также выполняется: $C_{q_1 \dots q_n} \cong C_{q_1} \times \dots \times C_{q_n}$

Замечание 4
Вы могли видеть формулировку КТО в более человеческом формате, что для системы сравнений по модулю взаимно простых чисел существует решение, при том единственное (в том смысле, что различные решения имеют одинаковые остатки).
В сущности, это та же самая теорема: решение i-го уравнения в системе отдельно — это какой-то элемент $\mathbb{Z}_{q_i}$. Собирая вместе все решения, получаем элемент $\mathbb{Z}_{q_1} \times \dots \times \mathbb{Z}_{q_n}$, а дальше задаваемый в теореме изоморфизм дает нам существование нужного числа в $\mathbb{Z}_{q_1 \dots q_n}$.

Задача 4
Найти наименьшее положительное целое x, такое что

$$\begin{aligned} x &\equiv 4 (\mathrm{mod} 5) \\ x &\equiv 5 (\mathrm{mod} 6) \\ x &\equiv 6 (\mathrm{mod} 7) \end{aligned} \tag{1}$$

Решение Заметим, что -1 является решением всех трех уравнений. То есть, в группе $\mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7$ нас интересует элемент $(-1, -1, -1)$.
Вспомним, как мы строили изоморфизм КТО: порождающим в произведении групп мы брали пару порождающих составляющих групп. В общем порождающему элементу в $\mathbb{Z}_{5\cdot 6\cdot 7}$ (то есть, 1) мы ставим в соответствие $(1, 1, 1)$. Тогда $(-1, -1, -1) = -(1, 1, 1)$, откуда получаем, что искомое решение в группе $\mathbb{Z}_{5\cdot 6\cdot 7}$ равно -1.
Тогда ответом будет $5 \cdot 6 \cdot 7 - 1 = 209$.

Замечание 5
Здесь нам повезло, и для всех уравнений ответ был одинаковый. Может возникнуть вопрос: а есть ли какой-то алгоритм решения таких систем уравнений в общем случае? Есть, но он не то чтобы простой (но если очень хочется, можете почитать, например, на Википедии)