ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Лекция 8

ГРУППА ПОДСТАНОВОК. ПОДГРУППЫ И ТЕОРЕМА ЛАГРАНЖА

Цель лекции	Объяснить устройство группы подстановок и обосновать связь между порядком элемента, порядком подгруппы и порядком конечной группы.
Результат обучения	Студент вычисляет композиции, определяет чётность и порядок подстановки, строит циклическую подгруппу и применяет теорему Лагранжа.
Предварительная подготовка	Отображения и биекции; делимость, НОД и НОК; арифметика вычетов; теоремы Ферма и Эйлера.

Аудиторная нагрузка: 1 академический час. Развёрнутые доказательства и упражнения предназначены также для самостоятельной подготовки.

План лекции

1. Группы и их основные свойства.
2. Подстановки, композиция и циклы.
3. Чётность подстановки и знакопеременная группа.
4. Подгруппы, порядок элемента и циклические группы.
5. Смежные классы и теорема Лагранжа.
6. Связь с теорией чисел и криптографией.

1 Группа как система обратимых действий

При работе с вычетами мы уже выделяли обратимые элементы: только для них умножение можно отменить умножением на обратный элемент. Понятие группы выражает эту идею независимо от природы объектов. Элементами могут быть числа, подстановки или симметрии фигуры; существенны правила выполнения и обращения действий.

Определение. Группой называется непустое множество G с бинарной операцией, обозначаемой умножением, если выполнены следующие условия:

1. Для любых $a, b \in G$ произведение ab принадлежит G.
2. Операция ассоциативна: $(ab)c = a(bc)$.
3. Существует нейтральный элемент e: $ea = ae = a$ для каждого $a \in G$.
4. Для каждого $a \in G$ существует обратный элемент a^{-1}: $aa^{-1} = a^{-1}a = e$.

Первое условие выражает замкнутость операции. Если дополнительно $ab = ba$ для любых элементов, группу называют **коммутативной, или абелевой**. Ассоциативность позволяет опускать скобки; переставлять множители она не разрешает.

Нейтральный элемент единственен: если e и e' нейтральны, то $e = ee' = e'$. Обратный элемент также единственен. Если b и c обратны к a, то $b = b(ac) = (ba)c = c$. Из этих свойств следует правило обращения произведения:

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Действительно, $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = e$; произведение в обратном порядке тоже равно e. При обращении последовательности действий порядок действий меняется на противоположный.

Примеры. Целые числа образуют группу по сложению: нейтральный элемент — 0, обратный к a — число $-a$. Множество $U(m)$ обратимых вычетов образует группу по умножению по модулю m. Все вычеты по составному модулю в общем случае такой группы по умножению не образуют: среди них есть необратимые элементы, в частности ноль.

2 Подстановки и симметрическая группа

2.1 Запись подстановки и порядок композиции

Подстановка степени n — биекция множества $\{1,2,\dots,n\}$ на себя. Совокупность всех таких биекций обозначается S_n. Подстановку можно записать таблицей образов:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

Краткая запись той же таблицы — $[3,4,5,2,1]$. Каждое число от 1 до n встречается в списке ровно один раз. Число подстановок равно $n!$: образ первого элемента выбирается n способами, второго — $n-1$ способами и так далее.

Соглашение курса: в произведении $\sigma\tau$ сначала выполняется правая подстановка τ:

$$(\sigma\tau)(i) = \sigma(\tau(i)).$$

Это соглашение совпадает с практической работой №7. В учебнике Л. М. Мартынова для композиции преобразований используется противоположный порядок записи; при сравнении примеров необходимо учитывать это различие.

Пусть $\tau = [2,3,1,4,5]$. Вычисление произведений удобно организовать по каждому исходному элементу.

i	**1**	**2**	**3**	**4**	**5**
$\tau(i)$	2	3	1	4	5
$\sigma(\tau(i))$	4	5	3	2	1
$\sigma(i)$	3	4	5	2	1
$\tau(\sigma(i))$	1	4	5	3	2

Получаем $\sigma\tau = [4,5,3,2,1]$ и $\tau\sigma = [1,4,5,3,2]$. Результаты различаются, поэтому S_5 некоммутативна. Вообще S_n некоммутативна при $n \geq 3$; достаточно рассмотреть произведения $(1\ 2)(2\ 3)$ и $(2\ 3)(1\ 2)$.

Композиция биекций является биекцией и ассоциативна. Тождественная подстановка $e(i) = i$ нейтральна, а обратное отображение задаёт обратную подстановку. Следовательно, S_n — группа, называемая **симметрической группой**.

2.2 Независимые циклы

Начиная с элемента 1, последовательно применим σ: получим переходы $1 \to 3 \to 5 \to 1$. Затем рассмотрим ещё не использованный элемент 2: $2 \to 4 \to 2$. Поэтому

$$\sigma = (1\ 3\ 5)(2\ 4).$$

Цикл $(a_1\ a_2\ \dots\ a_l)$ переводит a_1 в a_2, затем a_2 в a_3, а a_l — в a_1. Одноэлементные циклы соответствуют неподвижным точкам; обычно их не записывают. Разложение на непересекающиеся циклы единственно с точностью до перестановки циклов и выбора начальной точки внутри каждого цикла.

$$\sigma = (1\ 3\ 5)(2\ 4)$$



Рисунок 1. Подстановка состоит из двух независимых циклов с периодами 3 и 2.

Непересекающиеся циклы коммутируют, поскольку действуют на разных элементах. Для обращения цикла достаточно изменить направление переходов:

$$\sigma^{-1} = (1\ 5\ 3)(2\ 4) = [5,4,1,2,3].$$

Уравнение в группе. Из $\sigma x = \tau$ следует $x = \sigma^{-1}\tau$: обе части умножаются слева на σ^{-1}. Для выбранных подстановок $x = [4,1,5,2,3]$. Подстановка в исходное равенство даёт $\sigma x = \tau$. Умножение справа привело бы к другой формуле; в некоммутативной группе сторона умножения существенна.

3 Чётные и нечётные подстановки

3.1 Инверсии и знак

Пусть подстановка записана списком $[a_1, \dots, a_n]$. Пара позиций (i, j) называется **инверсией**, если $i < j$, но $a_i > a_j$. Число таких пар обозначим $I(\sigma)$, а знак определим формулой

$$\operatorname{sgn}(\sigma) = (-1)^{I(\sigma)}.$$

При чётном числе инверсий подстановка чётная, при нечётном — нечётная. Для $\sigma = [3,4,5,2,1]$ первые три позиции дают по две инверсии, четвёртая — одну. Поэтому $I(\sigma) = 7$ и знак равен -1.

Транспозиция — цикл длины 2, меняющий местами два элемента. Перестановка двух соседних позиций меняет число инверсий ровно на 1 по модулю 2. Обмен позиций $i < j$ можно выполнить с помощью $2(j - i) - 1$ соседних обменов. Следовательно, любая транспозиция меняет чётность.

Каждый цикл раскладывается в транспозиции. При принятом порядке композиции справедливо

$$(a_1\ a_2\ \dots\ a_l) = (a_1\ a_l) \cdots (a_1\ a_3)(a_1\ a_2).$$

Например, $(1\ 3\ 5) = (1\ 5)(1\ 3)$. Если некоторое разложение подстановки содержит r транспозиций, то её знак равен $(-1)^r$. Поэтому чётность числа транспозиций не зависит от выбранного разложения: она совпадает с чётностью числа инверсий самой подстановки.

3.2 Знак через длины циклов

Цикл длины l состоит из $l-1$ транспозиций и имеет знак $(-1)^{l-1}$. Для непересекающихся циклов длин $l_1, \dots, l_c$, включая неподвижные точки, получаем

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{c} (-1)^{l_i - 1} = (-1)^{n-c}.$$

У нашей подстановки $n = 5$, $c = 2$, поэтому знак равен $(-1)^3 = -1$, как и при подсчёте инверсий. Два способа дают удобную взаимную проверку.

Соединяя разложения двух подстановок в транспозиции, получаем основное свойство знака:

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

Множество чётных подстановок обозначают A_n и называют **знакопеременной группой**. Оно содержит e, замкнуто относительно композиции и обращения: знак произведения двух чётных подстановок равен 1, а знак обратной совпадает со знаком исходной. Значит, A_n является подгруппой S_n.

При $n \geq 2$ умножение на фиксированную транспозицию взаимно однозначно переводит чётные подстановки в нечётные. Таких подстановок поровну, следовательно, $|A_n| = n!/2$. Для $n = 1$ группа $A_1 = S_1$ состоит из одного элемента.

4 Подгруппы и порядки

4.1 Как проверить подгруппу

Подгруппа $H \leq G$ — подмножество, которое само является группой относительно той же операции. Простое наличие нескольких элементов группы ещё не делает их подгруппой.

Критерий. Непустое подмножество $H \subseteq G$ является подгруппой тогда и только тогда, когда для любых $a, b \in H$ элемент ab^{-1} принадлежит H.

Доказательство. Необходимость следует из замкнутости подгруппы относительно умножения и обращения. Для достаточности выберем $a \in H$. Тогда $aa^{-1} = e \in H$. Для любого $b \in H$ имеем $eb^{-1} = b^{-1} \in H$. Наконец, для $a, b \in H$ элемент $a(b^{-1})^{-1} = ab$ также лежит в H. Ассоциативность наследуется от G, поэтому все свойства группы выполнены.

Например, в аддитивной группе вычетов $\mathbb{Z}_{12}$ множество $\{0,4,8\}$ является подгруппой: разности его элементов по модулю 12 снова лежат в этом множестве. Множество $\{0,1,2\}$ подгруппой не является, поскольку $2 + 2 = 4$ в него не входит.

4.2 Порядок элемента и циклическая подгруппа

Порядок конечной группы или подгруппы — число её элементов. **Порядок элемента** g — наименьшее положительное целое t, для которого $g^t = e$. Если такого числа нет, порядок бесконечен. В конечной группе порядок каждого элемента конечен: среди степеней неизбежно появится повторение, которое после сокращения даёт положительную степень, равную e.

Все целые степени одного элемента образуют циклическую подгруппу

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}.$$

Замкнутость следует из $g^i(g^j)^{-1} = g^{i-j}$. Если порядок g равен t, то элементы $e, g, \dots, g^{t-1}$ различны, а любая другая степень совпадает с одной из них. Следовательно,

$$|\langle g \rangle| = \operatorname{ord}(g) = t.$$

Группа называется **циклической**, если совпадает с $\langle g \rangle$ для некоторого элемента g, называемого образующим. Любая циклическая группа коммутативна, поскольку $g^i g^j = g^{i+j} = g^j g^i$. Обратное утверждение неверно: группа $U(8) = \{1,3,5,7\}$ коммутативна, но не циклична, так как каждый её неединичный элемент имеет порядок 2.

4.3 Порядок подстановки и её степени

Цикл длины l возвращает свои элементы на исходные места именно при показателях, кратных l. Поэтому для непересекающихся циклов длин $l_1, \dots, l_c$ одновременно вернуться к тождественной подстановке можно при общем кратном этих длин. Наименьшее такое число равно

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(l_1, \dots, l_c).$$

Для $\sigma = (1\ 3\ 5)(2\ 4)$ порядок равен 6. Степень σ^{2026} удобно вычислить по отдельным циклам: $2026 \equiv 1 \pmod 3$ и $2026 \equiv 0 \pmod 2$, откуда $\sigma^{2026} = (1\ 3\ 5)$. Тот же результат получается после уменьшения показателя по модулю 6: $\sigma^{2026} = \sigma^4$.

Если g имеет порядок t, то для целого r справедливо

$$\operatorname{ord}(g^r) = \frac{t}{\gcd(t, r)}.$$

Действительно, $(g^r)^k = e$ равносильно делимости $t \mid rk$. Если $d = \gcd(t, r)$, то после сокращения на d получаем $t/d \mid k$, поскольку t/d и r/d взаимно просты. Наименьшее положительное k равно t/d.

В частности, g^r порождает всю группу $\langle g \rangle$ тогда и только тогда, когда $\gcd(r, t) = 1$. Поэтому циклическая группа порядка t имеет $\varphi(t)$ образующих. У подгруппы $\langle \sigma \rangle$ порядка 6 образующими являются σ и σ^5.

5 Смежные классы и теорема Лагранжа

Пусть $H \leq G$. **Левым смежным классом** называется множество $aH = \{ah : h \in H\}$, а правым — $Ha = \{ha : h \in H\}$. В некоммутативной группе эти множества могут различаться. Смежный класс, не содержащий e, сам подгруппой не является.

Для доказательства основной теоремы нужны два свойства.

Свойство 1. Каждый левый класс содержит столько же элементов, сколько H. Отображение $h \mapsto ah$ задаёт биекцию $H \to aH$: оно сюръективно по определению класса и инъективно благодаря сокращению слева.

Свойство 2. Два левых класса либо не пересекаются, либо совпадают. Если $ah_1 = bh_2$, то $a = bh_2h_1^{-1} \in bH$. Поэтому любой ah лежит в bH, то есть $aH \subseteq bH$. Перестановка ролей a и b даёт обратное включение.

Каждый $a \in G$ лежит в aH, так как $e \in H$. Следовательно, левые классы образуют разбиение группы. Число классов называют **индексом подгруппы** и обозначают $[G : H]$.

Теорема Лагранжа. Если группа G конечна и $H \leq G$, то

$$|G| = |H|[G : H].$$

Доказательство. Разобьём G на $[G:H]$ непересекающихся левых классов. В каждом классе ровно $|H|$ элементов. Подсчёт элементов этого разбиения даёт указанное равенство. В частности, $|H|$ делит $|G|$.

В аддитивной группе $\mathbb{Z}_{12}$ подгруппа $H = \{0,4,8\}$ задаёт четыре класса. Здесь запись $a + H$ заменяет мультипликативную запись aH.

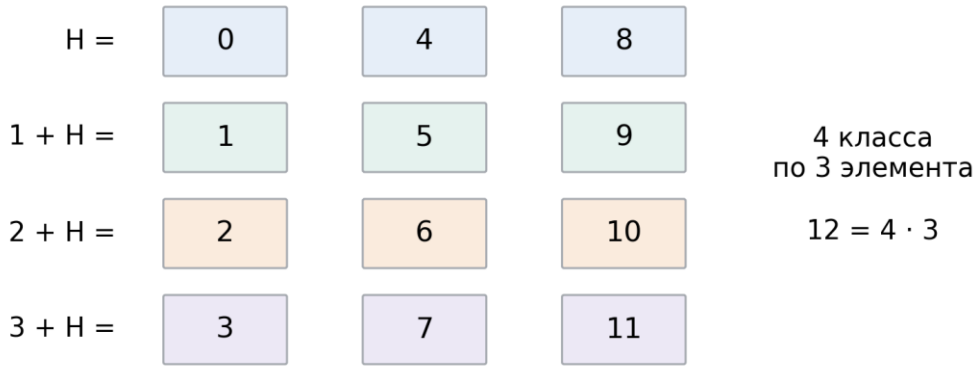


Рисунок 2. Теорема Лагранжа как подсчёт элементов одинаковых по размеру смежных классов.

Следствия. Поскольку $|\langle g\rangle| = \mathrm{ord}(g)$, порядок любого элемента конечной группы делит $|G|$, а значит, $g^{|G|} = e$. Если порядок группы — простое число p, любой неединичный элемент имеет порядок p и порождает всю группу.

Для нашей подстановки $\sigma \in S_5$ подгруппа $H = \langle\sigma\rangle$ имеет порядок 6, а её индекс равен $120/6 = 20$. Здесь 5 — степень подстановки, 6 — порядок элемента, 120 — порядок группы. Эти три числа описывают разные свойства.

Граница применения. Делимость является необходимым условием. Из $d \mid |G|$ в произвольной конечной группе нельзя заключить, что обязательно существует элемент или подгруппа порядка d. Например, в S_3 число 6 делит порядок группы, но элемента порядка 6 нет: возможны только порядки 1, 2 и 3. Для циклической группы подгруппа каждого порядка, делящего порядок группы, существует.

6 Теоретико-числовой смысл и криптографические преобразования

Применим теорему Лагранжа к группе $U(m)$, содержащей $\varphi(m)$ элементов. Для каждого обратимого вычета a получаем $a^{\varphi(m)} = 1$ в этой группе, то есть

$$a^{\varphi(m)} \equiv 1 \pmod{m}, \qquad \gcd(a,m) = 1.$$

Так теорема Эйлера из предыдущей лекции оказывается частным случаем общего утверждения о конечных группах. При простом модуле p группа ненулевых вычетов имеет порядок $p - 1$, что даёт малую теорему Ферма.

Для обратимого шифрующего преобразования на конечном множестве сообщений каждый фиксированный ключ задаёт подстановку этого множества. Если шифрование состоит из последовательных обратимых шагов, расшифрование выполняет обратные шаги в обратной последовательности. Это та же формула $(ab)^{-1} = b^{-1}a^{-1}$. Само по себе свойство биективности обеспечивает возможность восстановления, но не доказывает криптографическую стойкость.

7 Закрепление и самостоятельная работа

1. В S_4 заданы $\rho = (1\ 2\ 4)$ и $\eta = (1\ 3)$. Найдите $\rho\eta$, $\eta\rho$ и ρ^{-1}. Проверьте порядок выполнения действий на образе элемента 1.
2. Для $\pi = (1\ 4\ 2)(3\ 5)(6\ 7)$ найдите знак, порядок и степень π^{2026}.
3. Выпишите все элементы $H = \langle (1\ 3\ 5)(2\ 4) \rangle \leq S_5$. Найдите образующие и $[S_5 : H]$.
4. В аддитивной группе $\mathbb{Z}_{12}$ постройте $\langle 8 \rangle$. Найдите её порядок, образующие и все смежные классы.
5. Докажите, что $U(8)$ не циклична. Какой наименьший положительный показатель k даёт $a^k = 1$ для всех $a \in U(8)$? Почему теорема Эйлера остаётся верной?
6. Пусть $|G| = 11$. Определите порядки неединичных элементов, число образующих и возможные порядки подгрупп. Обоснуйте ответ теоремой Лагранжа.

Контрольные вопросы

1. Какие условия определяют группу? Чем коммутативность отличается от ассоциативности?
2. Почему подстановки степени n образуют группу и почему их число равно $n!$?
3. Какой порядок композиции принят в этом курсе?
4. Как получить обратную подстановку по её циклам?
5. Что такое инверсия? Почему чётность числа транспозиций не зависит от разложения?
6. Как определить знак по длинам циклов? Нужно ли учитывать неподвижные точки в формуле $(-1)^{n-c}$?
7. Почему A_n — подгруппа и чему равен её порядок при $n \geq 2$?
8. Сформулируйте критерий подгруппы через ab^{-1}.
9. Чем отличаются степень подстановки, порядок элемента и порядок группы?
10. Как найти порядок подстановки и число образующих циклической группы?
11. Почему смежные классы дают доказательство теоремы Лагранжа?
12. Как получить теоремы Эйлера и Ферма из теоремы Лагранжа?

Литература

1. Мартынов Л. М. **Алгебра и теория чисел для криптографии.** 2020. §1.7 «Чётность перестановок и подстановок»; §2.3 «Группы и их простейшие свойства»; §2.7.1–2.7.2 о подгруппах и циклических группах; §12.1 «Смежные классы группы по подгруппе». При чтении примеров композиции учитывайте соглашение раздела 2.1 этой лекции.
2. Trappe W., Washington L. C. **Introduction to Cryptography with Coding Theory.** 2nd ed., 2006. §3.6 — теоремы Ферма и Эйлера; §3.11 — конечные поля и связь с последующей темой.

Изложение и учебные примеры подготовлены для курса по указанным источникам; формулировки и обозначения согласованы с предыдущими материалами.