

15. ПЯТНАДЦАТАЯ ЛЕКЦИЯ, 17 ЯНВАРЯ 2023 Г.

15.1. Мультипликативная группа конечного поля. Имеет место следующая замечательная теорема.

Теорема 15.1. *Мультипликативная группа $\mathbb{F}_q^\times$ конечного поля $\mathbb{F}_q$ является циклической.*

Доказательство. Пусть G — мультипликативная группа конечного поля, порядок которой равен n . Пусть d — некоторый делитель n . Обозначим через $\psi(d)$ количество элементов порядка d в группе G . Предположим, что существует элемент $a \in G$, порядок которого равен d . Рассмотрим порождённую им подгруппу $H = \langle a \rangle$. Тогда всякий элемент из H удовлетворяет равенству $x^d = 1$. Поскольку число решений этого уравнения не превосходит d (число корней многочлена не больше его степени!), а порядок подгруппы H равен d (она порождена всеми степенями a), то получаем, что

$$H = \{x \in G \mid x^d = 1\}.$$

Поэтому все элементы порядка в точности d содержатся в H , и их число равняется $\varphi(d)$ — значению функции Эйлера, если такие элементы есть (и нулю в противном случае). Теперь запишем порядок группы G как сумму значений $\psi(d)$ при всевозможных $d \mid n$ и воспользуемся известным равенством для функции Эйлера:

$$\sum_{d \mid n} \psi(d) = n = \sum_{d \mid n} \varphi(d).$$

Отсюда получается, что $\psi(d) = \varphi(d)$ для любого d ; в частности, $\psi(n) = \varphi(n)$, откуда и следует, что в G есть элементы порядка n . $\square$

Заметим, что мы доказали даже больше, чем требовалось: мы не только выяснили, что элементы порядка n существуют, но и доказали, что их число равно $\varphi(n)$.

15.2. Смежные классы. Пусть G — произвольная группа, H — её подгруппа.

Определим на G отношение сравнимости по модулю подгруппы H следующим образом:

$$g_1 \equiv g_2 \pmod{H}, \quad \text{если} \quad g_1^{-1}g_2 \in H.$$

Легко проверить (проделайте это!), что это отношение эквивалентности на G . Классы эквивалентности мы будем называть *левыми смежными классами по подгруппе H* ; ясно, что класс, содержащий элемент g , имеет вид $gH = \{gh \mid h \in H\}$. В частности, сама подгруппа H также будет одним из классов эквивалентности.

Можно определить отношение эквивалентности и по-другому:

$$g_1 \equiv g_2 \pmod{H}, \quad \text{если} \quad g_2g_1^{-1} \in H.$$

Тогда классы имеют вид $Hg = \{hg \mid h \in H\}$; их мы будем называть *правыми смежными классами*.

Ясно, что если группа G коммутативна, то левые смежные классы совпадают с правыми; однако же для некоммутативных групп это, вообще говоря, будет не так.

Примеры 15.2. (1) Пусть $G = \mathbb{C}$, $H = \mathbb{R}$ (с операцией сложения). Тогда левые (они же правые) смежные классы будут иметь вид $\{t + iy \mid t \in \mathbb{R}\}$, т.е. будут горизонтальными прямыми.

(2) Пусть $G = \mathbb{C}^\times$, $H = \mathbb{R}_{>0}$ с операцией умножения. Тогда смежные классы — это (открытые) лучи $\{te^{i\varphi} \mid t \in \mathbb{R}_{>0}\}$, исходящие из начала координат.

(3) Пусть $G = \mathbb{C}^\times$, $H = S^1 = \{z \mid |z| = 1\}$. Тогда смежные классы имеют вид $\{|z| = r\}$, т.е. являются окружностями.

- (4) Пусть $G = \mathrm{GL}_n$, $H = \mathrm{SL}_n$. Тогда две матрицы A, B принадлежат одному левому смежному классу тогда и только тогда, когда $\det A = \det B$. Это же условие определяет и правые смежные классы.

Упражнение 15.3. Пусть $G = S_n$, $H = \{\sigma \in S_n \mid \sigma(n) = n\}$. Опишите левые и правые смежные классы по H и убедитесь, что они не совпадают.

Определение 15.4. Число смежных классов называется *индексом* группы G по подгруппе H и обозначается через $|G : H|$. (Это число может быть как конечным, так и бесконечным).

Теорема 15.5 (Лагранж). *Если группа G конечна, то*

$$|G| = |G : H| \cdot |H|.$$

Доказательство. Все смежные классы, очевидно, состоят из одинакового числа элементов, равного $|H|$. Действительно, отображение $H \rightarrow gH$, $h \mapsto gh$ является биекцией. $\square$

Отсюда получается множество следствий.

Следствие 15.6. $|H| \mid |G|$: порядок подгруппы делит порядок группы.

Следствие 15.7. $\mathrm{ord} g \mid |G|$: порядок каждого элемента делит порядок группы.

Доказательство. Рассмотрим циклическую подгруппу, порождённую g , и применим предыдущее следствие. $\square$

Следствие 15.8. Всякая конечная подгруппа простого порядка циклическа.

Следствие 15.9. Если $|G| = n$, то $g^n = e$ для любого $g \in G$.

Пример 15.10. Если p простое, то мультипликативная группа $(\mathbb{Z}/p\mathbb{Z})^\times$ будет группой порядка $p - 1$. Предыдущее следствие утверждает, что $g^{p-1} = 1$ для любого $g \in (\mathbb{Z}/p\mathbb{Z})^\times$. Это не что иное, как *малая теорема Ферма*.

Пример 15.11. Пусть теперь число m не обязательно простое. Мультипликативная группа $(\mathbb{Z}/m\mathbb{Z})^\times$ состоит из обратимых элементов кольца $\mathbb{Z}/m\mathbb{Z}$, т.е. таких классов $[k] \in \mathbb{Z}/m\mathbb{Z}$, для которых $(k, m) = 1$. Число таких классов равно функции Эйлера $\varphi(m)$. Применение предыдущего следствия даёт результат, известный как *теорема Эйлера*: для любого m и для любого a , взаимно простого с m , верно, что

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

15.3. Действия групп. Орбиты и стабилизаторы. Пусть G — группа, X — произвольное множество.

Определение 15.12. Будем говорить, что группа G *действует* на множестве X (обозначение: $G \curvearrowright X$, раньше еще иногда писали $G : X$), если задано отображение

$$G \times X \rightarrow X, \quad (g, x) \mapsto g \circ x,$$

для которого верно следующее:

- (1) $(g_1 g_2) \circ x = g_1 \circ (g_2 \circ x)$;
- (2) $e \circ x = x$ для любого $x \in X$ (единица группы действует тривиально).

Можно думать, что каждый элемент группы $g \in G$ задаёт перестановку элементов множества X , причем это отображение согласовано с умножением в группе.

Пример 15.13. Симметрическая группа S_n действует на множестве $\{1, \dots, n\}$ перестановками.

Пример 15.14. Группа движений плоскости $\text{Isom } \mathbb{R}^2$ действует на множестве точек в $\mathbb{R}^2$. Она же действует на множестве прямых в этой плоскости, на множестве треугольников, и так далее.

Примеры 15.15. Каждая группа G действует на себе следующими способами:

- *левое действие*: $g \circ h = gh$ (действие задается умножением элементов группы);
- *правое действие*: $g \circ h = hg^{-1}$ (подумайте, зачем здесь минус первая степень, и что «сломается», если ее не будет);
- *действие сопряжениями*: $g \circ h = ghg^{-1}$.

Проверьте, что это действительно будут действия.

Определение 15.16. Пусть группа G действует на множестве X . *Орбитой* элемента $x \in X$ называется множество

$$Gx = \{g \circ x \mid g \in G\} \subset X.$$

Стабилизатором элемента $x \in X$ называется подмножество в группе G :

$$\text{Stab}_G x = \{g \in G \mid g \circ x = x\} \subset G.$$

Иногда стабилизатор элемента x также обозначается через G_x . Нетрудно видеть, что $\text{Stab}_G x$ является *подгруппой* в G .

Упражнение 15.17. Докажите, что отношение «принадлежать одной орбите» является отношением эквивалентности на X .

Действие, для которого все множество X является одной орбитой (т.е. любые два элемента можно перевести друг в друга подходящим элементом группы G), называется *транзитивным*.