

15. ПЯТНАДЦАТАЯ ЛЕКЦИЯ, 17 ЯНВАРЯ 2022 Г.

15.1. Циклические подгруппы.

Определение 15.1. Группа G называется *циклической*, если она порождена одним элементом, т.е. если существует $g \in G$, для которого $\langle g \rangle = G$. Всякий такой элемент g называется *порождающим*.

Примеры 15.2. (1) $\mathbb{Z}$ как группа по сложению циклична; она порождается элементом 1 или элементом -1 .

(2) Группа $\mathbb{Z}/m\mathbb{Z}$ циклична: она порождается, например, классом элемента 1.

Упражнение 15.3. Найдите все порождающие элементы группы $\mathbb{Z}/m\mathbb{Z}$. Сколько их?

В прошлом семестре мы доказывали следующую теорему.

Теорема 15.4. Мультипликативная группа $\mathbb{F}_q^\times$ конечного поля $\mathbb{F}_q$ является циклической.

Несложно доказать следующую теорему, описывающую строение всех подгрупп циклической группы.

Теорема 15.5. (1) Всякая подгруппа циклической группы циклическая.

(2) В циклической подгруппе G порядка n порядок любой подгруппы делит n ; обратно, для любого $q \mid n$ существует ровно одна подгруппа в G порядка q .

Доказательство. (1) Пусть $G = \langle g \rangle$, и $H \neq \{e\}$ — подгруппа в G . Заметим, что если $g^{-m} \in H$, то и $g^m \in H$. Поэтому в H обязательно есть положительные степени элемента g .

Пусть m — минимальное положительное число, обладающее тем свойством, что $g^m \in H$. Докажем, что $\langle g^m \rangle = H$. Действительно, надо показать, что для всякого k , для которого $g^k \in H$, верно, что $m \mid k$. Действительно, поделим k на m с остатком: $k = mq + r$; тогда $g^r = g^k (g^m)^{-q} \in H$, откуда в силу минимальности m получаем, что $r = 0$.

(2) Если $|G| = n$, то при $k = m$ получаем, что $n = qt$. Поэтому

$$H = \{e, g^m, g^{2m}, \dots, g^{(q-1)m}\},$$

и H — единственная подгруппа в G порядка q . Обратно, если q — делитель n , и $n = qt$, то определенная так H — это подгруппа порядка q . $\square$

Следствие 15.6. Все подгруппы в группе G простого порядка — это $\{e\}$ и сама G .

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 15.7. (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 $G = \text{GL}_n$, $H = \text{SL}_n$. 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 15.8. 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 15.9. 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 15.10 (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 15.11. $|H| \mid |G|$: порядок подгруппы делит порядок группы.

Следствие 15.12. $\text{ord } g \mid |G|$: порядок каждого элемента делит порядок группы.

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

Следствие 15.13. *Всякая конечная подгруппа простого порядка циклическа.*

Следствие 15.14. *Если $|G| = n$, то $g^n = e$ для любого $g \in G$.*

Пример 15.15. 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*.