

14. ЧЕТЫРНАДЦАТАЯ ЛЕКЦИЯ, 10 ЯНВАРЯ 2022 Г.

14.1. Группы, подгруппы.

Определение 14.1. *Группой* называется множество G с двумя операциями:

- умножения $\mu: G \times G \rightarrow G$, $\mu(g_1, g_2) = g_1 g_2$; и
- взятия обратного $\iota: G \rightarrow G$, $\iota(g) = g^{-1}$,

удовлетворяющими следующим аксиомам:

- $g_1(g_2 g_3) = (g_1 g_2)g_3$ для любых $g_1, g_2, g_3 \in G$ (ассоциативность);
- существует элемент $e \in G$, для которого $eg = ge = g$ для любого $e \in G$ (существование нейтрального элемента);
- $gg^{-1} = g^{-1}g = e$.

Определение 14.2. Группа, в которой для любых двух элементов $g_1, g_2 \in G$ верно, что $g_1 g_2 = g_2 g_1$, называется *коммутативной*, или *абелевой* (в честь норвежского математика Нильса Хендрика Абеля).

Иногда для абелевых групп мы будем обозначать групповую операцию знаком «+» (будем говорить в таком случае про *аддитивную запись* групповой операции).

Приведем примеры групп. Некоторые из них возникали у нас при изучении колец.

Примеры 14.3. (1) Пусть A — произвольное кольцо. Тогда операция сложения определяет на A структуру абелевой группы.

(2) Операция умножения не определяет на кольце A структуру группы, поскольку нуль будет необратимым элементом. Но зато можно взять множество всех *обратимых* элементов кольца A (будем обозначать его через $A^\times$); оно уже будет группой по умножению.

(3) В частности, если $\mathbb{K}$ — поле, то множество $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ является группой; она называется *мультипликативной группой поля* $\mathbb{K}$.

(4) Пусть $GL(n)$ — множество обратимых матриц $n \times n$ (над некоторым полем $\mathbb{K}$). Умножение матриц превращает это множество в (также некоммутативную) группу. Эту группу можно отождествить с группой невырожденных линейных преобразований n -мерного векторного пространства $V \cong \mathbb{K}^n$.

(5) Пусть $\mathbb{E}^2$ — евклидова плоскость (из учебника планиметрии за 8-й класс). Тогда множество всех движений $\text{Isom } \mathbb{E}^2$ (т.е. взаимно однозначных отображений плоскости в себя, сохраняющих расстояние) образует группу, операцией в которой является композиция движений. Обратите внимание, что эта группа уже не будет коммутативной. Разумеется, $\mathbb{E}^2$ можно заменить на $\mathbb{E}^3$ или даже $\mathbb{E}^n$.

(6) Пусть $M \subset \mathbb{E}^n$ — произвольное подмножество в евклидовом пространстве (например, какой-нибудь многогранник). Тогда множество $\text{Isom } M = \{\varphi \in \text{Isom } \mathbb{E}^n \mid \varphi(M) = M\}$ само является группой (оно будет *подгруппой* в $\text{Isom } M$, см. ниже). Это *группа симметрий множества* M .

(7) Важным примером конечной группы является уже знакомая вам *группа перестановок* S_n : это группа всех взаимно-однозначных отображений из множества $\{1, \dots, n\}$ в себя. Число элементов в S_n равно $n!$.

Полезно помнить следующее правило обращения произведения (также известное вам по работе с группой матриц или перестановок):

$$(gh)^{-1} = h^{-1}g^{-1}.$$

Упражнение 14.4. Выведите из аксиом группы, что единица в группе единственна, и к каждому элементу существует ровно один обратный.

Определение 14.5. Непустое подмножество $H \subset G$ называется *подгруппой*, если для любых его элементов $h_1, h_2 \in H$ верно, что $h_1 h_2 \in H$, а также для любого элемента $h \in H$ верно, что $h^{-1} \in H$.

Замечание 14.6. Ясно, что второе условие можно заменить на условие $e \in H$.

Тем самым подгруппа — это подмножество в группе, само являющееся группой относительно той же операции.

14.2. Порядок элемента. Пусть G — произвольная группа, $g \in G$ — некоторый её элемент, $k \in \mathbb{Z}$. Определим k -ю степень элемента g так:

$$g^k = \begin{cases} \underbrace{g \cdots g}_{k \text{ раз}}, & k > 0; \\ e, & k = 0; \\ \underbrace{g^{-1} \cdots g^{-1}}_{-k \text{ раз}}, & k < 0. \end{cases}$$

Ясно, что такая операция удовлетворяет привычным свойствам степени: $g^k g^\ell = g^{k+\ell}$, $(g^k)^\ell = g^{k\ell}$, $(g^k)^{-1} = g^{-k}$.

Все степени данного элемента образуют подгруппу, которую мы будем обозначать через $\langle g \rangle$ и называть *циклической подгруппой, порождённой g* .

Для этой подгруппы есть два варианта: либо все элементы g^k различны, либо среди них есть совпадающие: $g^k = g^\ell$ при $k \neq \ell$. Если имеет место второй вариант, то мы получаем, что $g^{k-\ell} = e$.

Определение 14.7. *Порядком* $\text{ord } g$ элемента $g \in G$, отличного от единицы, называется минимальное положительное число m , для которого $g^m = e$. Если такого числа нет, будем считать $\text{ord } g = \infty$.

Определение 14.8. *Порядком конечной группы* (не обязательно циклической) называется число элементов в этой группе.

Предложение 14.9. Если $\text{ord } g = n$, то:

- (1) $g^m = e$ тогда и только тогда, когда $n \mid m$;
- (2) $g^k = g^\ell$ тогда и только тогда, когда $k \equiv \ell \pmod{n}$.

Доказательство. (1) Часть «тогда» очевидна. Докажем часть «только тогда». Поделим m на n с остатком: $m = qn + r$. По свойствам степени, $e = g^m = (g^n)^q g^r = g^r$. Но $0 \leq r < n$, а n — минимальное положительное число, для которого $g^n = e$. Стало быть, $r = 0$, то есть m делится на n нацело.

(2) Пусть $k \geq \ell$. Домножив обе части равенства $g^k = g^\ell$ на $g^{-\ell}$, получим равенство $g^{k-\ell} = e$. В силу предыдущего пункта, это равносильно тому, что $k - \ell$ делится на n , откуда и следует заявленное сравнение. $\square$

Отсюда получается такое следствие (верное для элементов как конечного, так и бесконечного порядков):

Следствие 14.10. Подгруппа $\langle g \rangle$ содержит ровно $\text{ord } g$ элементов.

Чуть сложнее доказывается такое

Предложение 14.11. Если $\text{ord } g = n$, то $\text{ord } g^k = \frac{n}{(n,k)}$.

Доказательство. Пусть наибольший общий делитель n и k равен $(n, k) = d$, причем $n = n_1 d$ и $k = k_1 d$. Тогда n_1 и k_1 взаимно просты. Поэтому $(g^k)^m = e$ тогда и только

тогда, когда $n \mid km$, что равносильно тому, что $n_1 \mid k_1 m$. В силу взаимной простоты n_1 и k_1 это равносильно тому, что $n_1 \mid m$. А это и значит, что порядок g^k равен $n/d = n_1$. $\square$