

20. ДВАДЦАТАЯ ЛЕКЦИЯ, 21 ФЕВРАЛЯ 2022 Г.

20.1. Коммутант. Пусть $x, y \in G$ — два элемента группы. Их *коммутатором* называется элемент $(x, y) = xyx^{-1}y^{-1}$. Очевидны следующие свойства коммутатора:

- (1) $(x, y) = e$ тогда и только тогда, когда x и y коммутируют.
- (2) $(x, y)^{-1} = (y, x)$ (обратный к коммутатору элемент снова является коммутатором).

Напротив, произведение двух коммутаторов не обязано быть коммутатором.

Все коммутаторы порождают подгруппу в G , которая называется *коммутантом* группы G (или, реже, её *производной группой*) и обозначается через G' :

$$G' := \langle (x, y) \mid x, y \in G \rangle.$$

Ясно, что $G' = \{e\}$ тогда и только тогда, когда G абелева.

Пусть $\varphi: G \rightarrow H$ — гомоморфизм групп. Поскольку $\varphi((x, y)) = (\varphi(x), \varphi(y))$, то $\varphi(G') \subset H'$. Если φ к тому же является эпиморфизмом, то $\varphi(G') = H'$.

Теперь возьмём в качестве H саму G , а в качестве φ — какой-нибудь её внутренний автоморфизм. Получается, что $\varphi(G') = G'$. Это значит, что G' — подгруппа, инвариантная относительно всех внутренних автоморфизмов. Значит, она нормальна в G .

Теорема 20.1. *Всякая подгруппа $H \subset G$, содержащая G' , нормальна. При этом факторгруппа G/H абелева (в частности, G/G' тоже абелева). Обратно, если H — такая нормальная подгруппа в G , что G/H абелева, то G' содержится в H . Другими словами, G' — наименьшая нормальная подгруппа в G , факторгруппа по которой абелева.*

Доказательство. Пусть $H \supset G'$. Пусть $h \in H$, $g \in G$. Тогда

$$ghg^{-1} = ghg^{-1}h^{-1}h = (g, h) \cdot h \in G' \cdot H \subset H,$$

поэтому $H \triangleleft G$.

Далее, пусть H — нормальная подгруппа в G , и $g_1, g_2 \in G$. Докажем, что g_1H и g_2H коммутируют, т.е. G/H коммутативна, тогда и только тогда, когда $G' \subset H$.

$$(g_1H, g_2H) = g_1Hg_2Hg_1^{-1}Hg_2^{-1}H = g_1g_2g_1^{-1}g_2^{-1}H = (g_1, g_2)H.$$

Если факторгруппа G/H абелева, то $(g_1, g_2)H = eH$, т.е. $(g_1, g_2) \in H$. Обратно, если $(g_1, g_2) \in H$, то из приведенного равенства получаем, что элементы факторгруппы g_1H и g_2H коммутируют. Теорема доказана. $\square$

20.2. Коммутанты некоторых групп. Из задач семинаров нам известно следующее

Предложение 20.2. *Группа чётных перестановок A_n порождается тройными циклами (ijk) . При $n \geq 5$ группа A_n порождается парами независимых транспозиций $(ij)(kl)$.*

Пример 20.3. $S'_n = A_n$ при $n \geq 3$. Действительно, $S'_n \subset A_n$, т.к. группа $S_3/A_3 = \mathbb{Z}_2$ абелева. Далее, найдём S'_3 . Эта группа содержится в A_3 . Но в A_3 нет никакой меньшей подгруппы, кроме единичной, поэтому S'_3 совпадает со всей A_3 (он отличен от $\{e\}$, т.к. S_3 некоммутативна). A_3 содержит оба 3-цикла (123) и (132) . Поэтому S'_n содержит всевозможные 3-циклы. Поэтому из предложения 20.2 следует, что $S'_n = A_n$.

Пример 20.4. $A'_4 = V_4$, где $V_4 = \langle (ij)(kl) \rangle$ — четверная группа Клейна. Действительно, $A_4/V_4 \cong \mathbb{Z}_3$ абелева, т.е. $A'_4 \subset V_4$. Но V_4 не содержит никаких нетривиальных подгрупп, нормальных в A_4 (и вообще V_4 — единственная нормальная подгруппа в A_4 , отличная от единичной и её самой), поэтому $A'_4 = V_4$.

Пример 20.5. Предыдущий пример показывает, что при $n \geq 5$ коммутант A'_n содержит все пары независимых транспозиций. Поэтому он совпадает со всей группой A_n .

Замечание 20.6. На прошлом семинаре было показано, что при $n \geq 5$ группа A_n проста, т.е. не содержит нетривиальных нормальных подгрупп. Разумеется, для всякой неабелевой простой группы G верно, что $G' = G$.

Вычислим¹ коммутанты групп $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$. Для этого нам понадобится следующее утверждение.

Предложение 20.7. *Группа $\mathrm{SL}_n(K)$ порождается трансвекциями $E + cE_{ij}$ при $i \neq j$, т.е. матрицами элементарных преобразований первого рода (здесь E — единичная матрица, E_{ij} — матричная единица, т.е. матрица, все элементы которой равны нулю, кроме (i, j) -го, который равен 1).*

Задача 20.1. Докажите предложение 20.7.

Докажем, что $\mathrm{GL}_n(K)' = \mathrm{SL}_n(K)' = \mathrm{SL}_n(K)$, в предположении, что поле K содержит более трёх элементов. Во-первых, $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ есть группа скалярных матриц, которая является абелевой, т.е. $\mathrm{GL}_n(K)' \subset \mathrm{SL}_n(K)$. Далее, можно проверить явно, что

$$\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & (\lambda^2 - 1)c \\ 0 & 1 \end{pmatrix}.$$

Поэтому если в K найдётся элемент λ , отличный от 0 и ± 1 , то группа $\mathrm{GL}_n(K)'$ будет содержать все трансвекции. Поэтому она совпадает с $\mathrm{SL}_n(K)$ в силу предыдущего предложения.

20.3. Разрешимые группы. Определим *высшие коммутанты* $G^{(i)}$ группы G по следующему правилу: $G^{(1)} = G'$, $G^{(i)} = (G^{(i-1)})'$. Получим ряд подгрупп, каждая из которых нормальна в предыдущей:

$$G = G^{(0)} \triangleright G^{(1)} \triangleright \dots \triangleright G^{(k)} \triangleright \dots$$

Определение 20.8. Группа G *разрешима*, если $G^{(k)} = \{e\}$ для некоторого k .

Пример 20.9. В предыдущем пункте мы видели, что S_4 разрешима (для неё $S_4^{(3)} = \{e\}$, т.к. $S_4^{(2)} = V_4$ абелева), а при $n \geq 5$ группа S_n уже не является разрешимой.

Справедлива следующая несложная

Теорема 20.10. Пусть $H \triangleleft G$ — нормальная подгруппа. Группа G разрешима тогда и только тогда, когда H и G/H разрешимы.

Задача 20.2. Докажите эту теорему.

¹На лекции этого не было, зато было на семинарах.

20.4. Абелевы группы. Оставшаяся часть этой и следующая лекции будут посвящены описанию структуры и свойств абелевых (коммутативных) групп.

Пусть A — абелева группа. Будем записывать ее аддитивно, т.е. операцию будем обозначать через плюс, а нейтральный элемент будем называть нулём.

Элементы абелевой группы можно умножать на целые числа: если $a \in A$ и $n \in \mathbb{Z}$, то $na = a + \dots + a$ (n раз), если n положительно, и $na = (-a) + \dots + (-a)$ ($-n$ раз), если n отрицательно.

Для любого подмножества $S \subseteq A$ наименьшая абелева подгруппа, содержащая все элементы из S — это

$$\langle S \rangle = \{n_1 a_1 + \dots + n_k a_k \mid n_1, \dots, n_k \in \mathbb{Z}, a_1, \dots, a_k \in S\}.$$

Её будем называть *подгруппой, порождённой множеством S* . Если $\langle S \rangle = A$, то S называется *системой порождающих* группы A . Если у абелевой группы A есть конечная система порождающих, она называется *конечно порожденной*.

20.5. Свободные абелевы группы. Как и для векторных пространств, определим понятие линейной зависимости элементов группы. Так, элементы $a_1, \dots, a_k \in A$ называются *линейно зависимыми*, если существуют такие целые $n_1, \dots, n_k$, не все равные одновременно 0, для которых

$$n_1 a_1 + \dots + n_k a_k = 0,$$

и *линейно независимыми* в противном случае.

Линейно независимая система порождающих группы A называется её *базисом*. Группа, обладающая базисом, называется *свободной*.

В отличие от случая векторных пространств, не всякая (даже конечно порождённая) группа обладает базисом. Простейший пример — это группа $\mathbb{Z}/n\mathbb{Z}$, в которой каждый элемент оказывается «линейно зависим сам с собой»: для любого $a \in \mathbb{Z}/n\mathbb{Z}$ найдётся такое ненулевое число m , для которого $ma = 0$. Действительно, в качестве m можно взять число n или любое его кратное.

Предложение 20.11. *Все базисы свободной абелевой группы A состоят из одинакового числа элементов. Это число называется рангом группы и обозначается через $\text{rk } A$.*

Доказательство. Рассмотрим два каких-то базиса группы A : пусть это $e_1, \dots, e_n$ и $f_1, \dots, f_m$, где $m \geq n$. Выразим элементы f_j через e_i :

$$f_j = \sum_i c_{ij} e_i,$$

где $(c_{ij}) \in \text{Mat}(n \times m, \mathbb{Z})$. Поскольку все f_j линейно независимы с коэффициентами в $\mathbb{Z}$, то и столбцы матрицы C линейно независимы с целыми коэффициентами. Но это значит, что они линейно независимы и над $\mathbb{Q}$, то есть ранг матрицы C над $\mathbb{Q}$ равен m . Но, с другой стороны, из курса линейной алгебры мы знаем, что ранг матрицы размера $m \times n$ над полем не превосходит минимума из m и n , то есть n . Поэтому $m = n$. □

Свободную абелеву группу A ранга k удобно отождествлять с $\mathbb{Z}^k$; отождествление задаётся при помощи базиса. Если $e_1, \dots, e_k$ — базис, то, очевидно, отображение

$$A \rightarrow \mathbb{Z}^k, \quad n_1 a_1 + \dots + n_k a_k \mapsto (n_1, \dots, n_k)$$

будет изоморфизмом групп.