Доклады Академии Наук СССР

1937. Том XV, № 2

МАТЕМАТИКА

А. П. ДИЦМАН

О p-ГРУППАХ

(Представлено академиком О. Ю. Шмидтом 5 III 1937)

Следуя Шуру (1), периодической группой будем называть группу, каждый элемент которой есть элемент конечного порядка.

Периодическую группу, порядок каждого элемента которой есть некоторая степень простого числа p, будем называть p-группой. Очевидно, порядок конечной p-группы есть некоторая степень числа p. Известно, что p-группа конечного порядка имеет отличный от единицы центр.

В настоящей работе устанавливается необходимое и достаточное условие, при котором p-группа имеет отличный от единицы центр; попутно доказываются некоторые теоремы.

§ 1. Классы сопряженных элементов группы будем в дальнейшем называть кратко классами группы; класс, заключающий конечное число элементов, будем называть конечным классом.

Пусть имеем произведение g некоторых элементов группы:

$$g = a_1 \dots a_{i-1}\, a_i \dots a_{k-1} a_k\, a_{k+1} \dots a_l. \tag{1}$$

Представим g в виде:

$$g = a_1 \dots a_{i-1}\, a_k\, a_i^* \dots a_{k-1}^*\, a_{k+1} \dots a_l, \tag{2}$$

где $a_i^* = a_k^{-1}\, a_i\, a_k$; ... ; $a_{k-1}^* = a_k^{-1}\, a_{k-1} a_k$; в этом случае будем говорить, что произведение (2) получается из произведения (1) путем перемещения элемента a_k на место i.

Пусть M — множество элементов, порождающих группу G. Тогда каждый элемент группы G есть произведение конечного числа степеней некоторых элементов множества M. Очевидно всякое непустое множество элементов группы G порождает подгруппу.

Теорема I. *Пусть M—множество элементов, порождающих группу G, и $\mathfrak{K}$— инвариантный комплекс группы G.*

Если $\mathfrak{H}$ есть подгруппа, порождаемая всеми элементами множества M, не принадлежащими комплексу $\mathfrak{K}$, и Q—инвариантная подгруппа, порождаемая всеми элементами инвариантного комплекса $\mathfrak{K}$, то $\mathfrak{H}\, Q$ совпадает с G.

Доказательство. Если q—элемент подгруппы Q и g—элемент группы G, то $g^{-1}\,qg$ можно представить как произведение конечного числа степеней некоторых элементов инвариантного комплекса $\mathfrak{K}$, т. е. элемент $g^{-1}\,qg$ принадлежит Q, откуда $g^{-1}\,Q\,g=Q$. Следовательно Q—инвариантная подгруппа группы G.

Заметим следующее: если $g_1=q_1 g_2$, где q_1—элемент Q, а g_1 и g_2—элементы группы G, то путем перемещения g_2 можно представить g_1 в виде произведения $g_1=g_2\,q^*$, где q^* есть элемент Q.

Далее, каждый элемент g группы G можно представить в виде произведения конечного числа степеней некоторых элементов множества M:

$$g=m_1^{\alpha_1}\,m_2^{\alpha_2}\ldots m_k^{\alpha k}, \tag{3}$$

где $m_1, m_2, \ldots, m_k$ — элементы множества M и $\alpha_1, \alpha_2, \ldots, \alpha_k$ — некоторые целые числа. Пользуясь вышеизложенным замечанием, заключаем, что путем перемещения в (3) степеней элементов множества M, не принадлежащих инвариантному комплексу $\mathfrak{K}$, можно представить g в виде: $g=hq_2$, где h — элемент подгруппы $\mathfrak{H}$ и q_2 — элемент Q; следовательно $G=\mathfrak{H}Q$. Теорема доказана.

Теорема II. *Если A—конечный класс группы G, заключающий элементы конечного порядка, то все элементы класса A порождают инвариантную подгруппу Q конечного порядка.*

Доказательство. Обозначим через $a_1,\ a_2,\ \ldots,\ a_k$ элементы класса A порядка k, через β — порядок элемента a_1, очевидно имеем:

$$a_i^{\beta}=1; \quad i=1, 2, \ldots, \kappa. \tag{4}$$

Всякий элемент q_j подгруппы Q можно представить в виде произведения конечного числа степеней элементов класса A. Пользуясь (4), заключаем, что для всякого элемента q_j подгруппы Q существует такое наименьшее положительное целое число $m=m(q_j)$, что q_j можно представить в виде произведения m элементов:

$$q_j=a_{i_1}\,a_{i_2}\ldots a_{i_m}, \tag{5}$$

при этом множители $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$ суть некоторые элементы класса A. Если среди элементов $a_{i_1}, a_{i_2}, \ldots, a_{i_m}$ имеется α элементов, равных a_s, то будем говорить, что элемент a_s встречается в произведении (5) α раз.

Представление элемента q_j в виде произведения m элементов класса A будем называть нормальным представлением элемента q_j, число m—длиною элемента q_j. Два нормальных представления элемента q_j будем считать различными, если они отличаются либо множителями либо порядком следования множителей.

Рассмотрим множество П всех нормальных представлений элемента q_j, т. е. множество различных произведений вида (5). Очевидно П содержит конечное число различных таких произведений.

Пусть a_s — элемент класса A; очевидно в каждом из произведений множества П элемент a_s встречается не более m раз. Следовательно паре элементов a_s и q_j можно сопоставить число α_{sj}, удовлетворяющее условиям:

1) Среди произведений множества П имеется по крайней мере одно произведение, в котором элемент a_s встречается α_{sj} раз.

2) В каждом произведении множества П элемент a_s встречается не более α_{sj} раз.

Очевидно $0 \leqslant \alpha_{sj} \leqslant m$.

В частности если $\alpha_{sj} = m$, то $q_j = a_s^{\alpha_{sj}}$.

Заметим теперь, что при $\alpha_{sj} < m$ имеется нормальное представление элемента q_j вида:

$$q_j = a_s^{\alpha_{sj}} q_{j+1}, \tag{6}$$

где q_{j+1} есть произведение $m - \alpha_{sj}$ элементов класса A; при этом $m - \alpha_{sj}$ есть длина элемента q_{j+1} и $\alpha_{sj+1} = 0$. Кроме того для любого элемента a_t класса A имеем $\alpha_{tj} \geqslant \alpha_{t_{j+1}}$, в частности если $\alpha_{tj} = 0$, то и $\alpha_{t_{j+1}} = 0$.

Действительно, рассмотрим нормальное представление элемента q_j, в котором a_s встречается α_{sj} раз; путем последовательного перемещения элементов a_s этого произведения на первое место очевидно получим нормальное представление элемента q_j вида (6). Длина элемента q_{j+1} равна $m - \alpha_{sj}$, так как произведение (6) есть нормальное представление элемента q_j. Далее $\alpha_{sj+1} = 0$, так как, предполагая $\alpha_{sj+1} > 0$, заключаем, что имеется нормальное представление элемента q_j, в котором a_s встречается более α_{sj} раз, что противоречит определению числа α_{sj}. Наконец $\alpha_{tj} \geqslant \alpha_{tj+1}$, так как предположение $\alpha_{tj+1} > \alpha_{tj}$ противоречит определению числа α_{tj}.

Пусть q_1—какой-либо элемент подгруппы Q длины m_1. Если $\alpha_{11} = m_1$, то $q_1 = a_1^{\alpha_{11}}$. Если же $\alpha_{11} < m_1$, то, пользуясь вышеизложенным замечанием, заключаем, что для q_1 существует нормальное представление вида:

$$q_1 = a_1^{\alpha_{11}} q_2,$$

причем $\alpha_{12} = 0$.

Рассуждая аналогично для q_2 и т. д., предположим, что мы уже получили нормальное представление элемента q_1 вида:

$$q_1 = a_1^{\alpha_{11}} a_2^{\alpha_{22}} \dots a_{r-1}^{\alpha_{r-1r-1}} q_r; \quad 2 \leqslant r < k, \tag{7}$$

причем

$$\alpha_{1r} = 0; \quad \alpha_{2r} = 0; \quad \dots; \quad \alpha_{r-1r} = 0 \quad \text{и} \quad \alpha_{11} + \alpha_{22} + \dots + \alpha_{r-1r-1} < m_1.$$

Тогда если $\alpha_{11} + \alpha_{22} + \dots + \alpha_{rr} = m_1$, то, очевидно, имеем:

$$q_1 = a_1^{\alpha_{11}} a_2^{\alpha_{22}} \dots a_r^{\alpha_{rr}}.$$

Если же $\alpha_{11} + \alpha_{22} + \dots + \alpha_{rr} < m_1$, то для q_r существует нормальное представление:

$$q_r = a_r^{\alpha_{rr}} q_{r+1}, \tag{8}$$

причем

$$\alpha_{1r+1} = 0; \quad \alpha_{2r+1} = 0; \quad \dots; \quad \alpha_{rr+1} = 0.$$

Из (7) и (8) получаем для q_1 нормальное представление:

$$q_1 = a_1^{\alpha_{11}} a_2^{\alpha_{22}} \dots a_r^{\alpha_{rr}} q_{r+1},$$

при этом

$$\alpha_{1r+1} = 0; \quad \alpha_{2r+1} = 0; \quad \dots; \quad \alpha_{rr+1} = 0 \quad \text{и} \quad \alpha_{11} + \alpha_{22} + \dots + \alpha_{rr} < m_1.$$

Таким образом убеждаемся, что для элемента q_1 существует нормальное представление вида:

$$q_1 = a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_k^{\alpha_k},$$

причем

$$0 \leqslant \alpha_i < \beta; \quad i=1, 2, \ldots, k,$$

и

$$\alpha_1 + \alpha_2 + \ldots + \alpha_k = m_1.$$

Следовательно Q есть подгруппа конечного порядка и, по теореме I, инвариантная подгруппа группы G, что и требовалось доказать.

Теорема III. *Если M—множество элементов, порождающих группу G, и $\mathfrak{K}$—инвариантный комплекс, состоящий из конечного числа элементов конечного порядка группы G, то подгруппа, порождаемая всеми элементами множества M, не принадлежащими комплексу $\mathfrak{K}$, есть подгруппа конечного индекса группы G.*

Доказательство. Обозначим через Q подгруппу, порождаемую всеми элементами инвариантного комплекса $\mathfrak{K}$. Пусть комплекс $\mathfrak{K}$ состоит из n конечных классов $A_1, A_2, \ldots, A_n$ группы G.

Из теоремы II заключаем, что все элементы класса A_i (для $i = 1, 2, \ldots, n$) порождают нормальный делитель Q_i конечного порядка группы G; при этом

$$Q = Q_1 Q_2 \cdots Q_n.$$

Следовательно Q есть подгруппа конечного порядка.

Обозначим через $\mathfrak{H}$ подгруппу, порождаемую всеми элементами множества M, не принадлежащими комплексу $\mathfrak{K}$; по теореме I имеем:

$$G = \mathfrak{H}\, Q.$$

Так как Q—подгруппа конечного порядка, то $\mathfrak{H}$ есть подгруппа конечного индекса группы G, что и требовалось доказать.

Отметим одно из следствий теорем II и III:

Группа, порождаемая n элементами конечного порядка, $n-1$ которых принадлежат к конечным классам, есть группа конечная.

§ 2. Укажем сначала некоторые вспомогательные предложения.

Лемма 1. *Пересечение конечного числа подгрупп, каждая из которых есть подгруппа конечного индекса группы G, есть подгруппа конечного индекса группы G.*

Доказательство. Пусть $\mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_k$ — подгруппы конечного индекса группы G. Обозначим через D_1 пересечение подгрупп $\mathfrak{H}_1$ и $\mathfrak{H}_2$, т. е. $D_1 = [\mathfrak{H}_1, \mathfrak{H}_2]$, аналогично $D_2 = [D_3, \mathfrak{H}_3]; \ldots; D_{k-1} = [D_{k-2}, \mathfrak{H}_k]$. Очевидно D_{k-1} есть пересечение подгрупп $\mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_k$. Пользуясь теоремой Пуанкаре([2]), заключаем, что D_{k-1} есть подгруппа конечного индекса группы G. Лемма доказана.

Далее имеем очевидное предложение.

Лемма 2. *Если $\mathfrak{H}$—подгруппа группы G, D—подгруппа $\mathfrak{H}$ и нормальный делитель G, то множество смежных систем разложения G по модулю $\mathfrak{H}$ эквивалентно множеству смежных систем разложения факторгруппы $\frac{G}{D}$ по модулю $\frac{\mathfrak{H}}{D}$.*

Лемма 3. *Если $\mathfrak{H}$—подгруппа конечного индекса группы G, то $\mathfrak{H}$ имеет подгруппу D, являющуюся инвариантной подгруппой конечного индекса группы G, при этом индекс $\mathfrak{H}$ равен индексу $\frac{\mathfrak{H}}{D}$, т. е.:*

$$(G, \mathfrak{H}) = \left(\frac{G}{D}, \frac{\mathfrak{H}}{D}\right).$$

Доказательство. Очевидно, G содержит конечное число различных, сопряженных с $\mathfrak{H}$ подгрупп. Обозначим через D пересечение всех подгрупп, сопряженных с $\mathfrak{H}$. Пользуясь леммой 1, заключаем, что D есть инвариантная подгруппа конечного индекса группы G. По лемме 2 имеем:

$$(G, \mathfrak{H}) = \left(\frac{G}{D}, \frac{\mathfrak{H}}{D}\right).$$

Лемма 3 доказана.

Следствие. *Если $\mathfrak{H}$—подгруппа конечного индекса некоторой p-группы P, то индекс $\mathfrak{H}$ есть степень числа p.*

Действительно, пусть D есть пересечение всех подгрупп, сопряженных с $\mathfrak{H}$; по лемме 3 D—инвариантная подгруппа конечного индекса группы P и

$$\left(\frac{P}{D}, \frac{\mathfrak{H}}{D}\right) = (P, \mathfrak{H}). \tag{9}$$

Далее, факторгруппа $\frac{P}{D}$ есть группа конечного порядка, при этом порядок каждого ее элемента есть степень числа p, т. е. факторгруппа $\frac{P}{D}$ есть конечная p-группа. Вследствие (9) индекс $\mathfrak{H}$ есть степень числа p, что и требовалось доказать.

Теорема IV. *p-группа имеет отличный от единицы центр, если она содержит по крайней мере один отличный от единицы конечный класс.*

Доказательство. Пусть A—конечный класс p-группы P. Элементы класса A по теореме II порождают нормальный делитель $\mathfrak{A}$ конечного порядка p^n группы P. Обозначим через a какой-либо элемент нормального делителя $\mathfrak{A}$. Элемент a принадлежит к конечному классу группы P, так как множество всех элементов нормального делителя $\mathfrak{A}$ есть совокупность некоторых конечных классов группы P. Нормализатор V элемента a в группе P есть следовательно подгруппа конечного индекса группы P. По следствию леммы 3 индекс подгруппы V есть степень числа p. Следовательно, порядок класса сопряженных с a элементов группы P есть степень числа p.

Пусть нормальный делитель $\mathfrak{A}$ распадается на k классов группы P, причем порядки этих классов суть числа $\alpha_1, \alpha_2, \ldots, \alpha_k$, тогда

$$p^n = \alpha_1 + \alpha_2 + \ldots + \alpha_k.$$

Числа $\alpha_1, \alpha_2, \ldots, \alpha_k$ суть степени числа p, и так как $\alpha_1 = 1$ (элемент единица составляет класс), то кроме единицы группа P должна иметь еще и другие инвариантные элементы, что и доказывает теорему.

Из теоремы IV следует, что p-группа, центр которой равен единице, не содержит ни одного отличного от единицы конечного класса.

Поступило
5 III 1937.

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] J. Schur, Sitzungsberichte Berl. Akademie, S. 619 (1911). [2] H. Poincaré, Journal de mathématiques, série 4, **3**, 409 (1887); см. также О. Ю. Шмидт, Абстрактная теория групп, стр. 33 (1933).