Доклады Академии Наук СССР
1947. Том LVIII, № 4

МАТЕМАТИКА

Д. К. ФАДДЕЕВ

О СТРУКТУРЕ ГРУПП ПОРЯДКА p^nq

(Представлено академиком И. М. Виноградовым 28 IV 1947)

Теорема. *Если группа порядка p^nq не имеет ни нормального делителя порядка p^n, ни нормального делителя порядка q, то p, q удовлетворяют условиям: $q \equiv 1\ (p)$, $p\frac{f}{(p,f)} \leqslant n-1$, где f есть наименьшее из положительных чисел таких, что $p^f \equiv 1\ (q)$. Очевидно, что этим условиям удовлетворяет при данном n лишь конечное число простых чисел p, q, так что и групп порядка p^nq, не имеющих силовских нормальных делителей, существует лишь конечное число при фиксированном n.*

Доказательство. Теорема верна для групп порядка pq, ибо каждая такая группа имеет нормальный делитель порядка p или порядка q. Допустим, что теорема верна для всех групп порядков $p^\alpha q$, $\alpha \leqslant n-1$, и в этом предположении докажем ее справедливость для групп порядка p^nq. Пусть $\mathfrak{G}$ есть группа порядка p^nq и пусть $\mathfrak{P}$ и Q ее силовские подгруппы порядков p^n и q. Допустим далее, что ни $\mathfrak{P}$ ни Q не являются нормальными делителями $\mathfrak{G}$. Тогда, в силу второй теоремы Силова, $q \equiv 1\ (p)$ и остается только доказать, что $p\frac{f}{(p,f)} \leqslant n-1$. Известно, что группа $\mathfrak{G}$ разрешима. Пусть $\mathfrak{A}$ есть нормальный делитель $\mathfrak{G}$, являющийся последним отличным от 1 членом какого-либо главного ряда $\mathfrak{G}$. $\mathfrak{A}$ есть абелева группа, разлагающаяся в прямое произведение циклических групп простого порядка. В силу сделанных предположений относительно $\mathfrak{G}$, порядок $\mathfrak{A}$ не может быть равен ни p^n, ни q и, следовательно, равен p^m, $1 \leqslant m \leqslant n-1$. Пусть $\mathfrak{F} = \mathfrak{G}/\mathfrak{A}$. Порядок $\mathfrak{F}$ равен $p^{n-m}q$. $\mathfrak{F}$ не имеет нормального делителя порядка p^{n-m}, ибо иначе $\mathfrak{G}$ имела бы нормальный делитель порядка p^n. Если, кроме того, $\mathfrak{F}$ не имеет нормального делителя порядка q, то, в силу индукционного предположения, имеет место неравенство $p\frac{f}{(p,f)} \leqslant n-m-1 < n-1$, и теорема доказана для группы $\mathfrak{G}$. Остается предположить, что $\mathfrak{F}$ имеет нормальный делитель $\mathfrak{H}$ порядка q. Пусть $\mathfrak{h}$ есть совокупность всех элементов $\mathfrak{G}$, входящих во все комплексы, образующие $\mathfrak{H}$. $\mathfrak{h}$ есть нормальный делитель $\mathfrak{G}$ порядка p^mq. Все силовские q-подгруппы $\mathfrak{G}$, в частности Q, входят в $\mathfrak{h}$. Следовательно, $\mathfrak{h} = \mathfrak{A} \cdot Q$. Пусть B есть производящий элемент группы Q. B не может быть перестановочен со всеми элементами $\mathfrak{A}$, ибо тогда Q была бы нормальным делителем $\mathfrak{h}$ и, в силу характеристичности, нормальным делителем $\mathfrak{G}$. Далее, $\mathfrak{F} = \mathfrak{H} \cdot \overline{\mathfrak{P}}$, где $\overline{\mathfrak{P}}$ есть силовская p-подгруппа $\mathfrak{F}$. Не все элементы $\overline{\mathfrak{P}}$ перестановочны с производящим элементом $\overline{B} = B\mathfrak{A}$ группы $\mathfrak{H}$, ибо иначе $\overline{\mathfrak{P}}$ была бы нормальным делителем $\mathfrak{F}$. Следовательно, в $\overline{\mathfrak{P}}$ найдется по крайней мере один элемент $\overline{A}$, индуцирующий автоморфизм порядка p в группе $\mathfrak{H}$. Пусть $\overline{A}^{-1}\overline{B}\overline{A} = \overline{B}^\nu$. Тогда $\nu^p \equiv 1\ (q)$, но $\nu \neq 1\ (q)$. Обратимся теперь к рассмотрению автоморфизмов, индуцированных в группе $\mathfrak{A}$ преобразованиями посредством элементов $\mathfrak{G}$. Ввиду того, что $\mathfrak{A}$ есть абелева группа порядка p^m типа $(p, p, \ldots, p)$, каждый ее автоморфизм φ опре-

деляет матрицу порядка m с элементами из конечного поля R_p вычетов по модулю p. В качестве элементов такой матрицы должно взять показатели a_{ij} в равенствах

$$A_i^{\varphi} = \prod_{j=1}^{m} A_j^{a_{ij}^{\varphi}},$$

где $A_1 \dots A_m$ — какой-либо базис $\mathfrak{A}$. Группа автоморфизмов $\mathfrak{A}$, индуцированная посредством преобразований элементами $\mathfrak{G}$, является, очевидно, гомоморфным образом $\mathfrak{F} = \mathfrak{G}/\mathfrak{A}$. При этом циклический нормальный делитель $\mathfrak{H}$ группы $\mathfrak{F}$ отображается изоморфно, так как производящий элемент $\overline{B} = B\mathfrak{A}$ группы $\mathfrak{H}$ содержит элемент B, перестановочный не со всеми элементами $\mathfrak{A}$, как было сказано выше. Пусть Γ есть матрица, соответствующая элементу B, Δ — матрица, соответствующая элементу $\overline{A}$. Тогда $\Delta^{-1}\Gamma\Delta = \Gamma^{\nu}$, $\nu \not\equiv 1\ (q)$, $\nu^p \equiv 1\ (q)$. Расширим поле R_p до поля K_p степени f над R_p. Как известно, поле K_p содержит все корни из единицы степени q, причем каждый такой корень, отличный от 1, является корнем неприводимого уравнения степени f с коэффициентами из R_p. Далее, матрица Γ может быть преобразована посредством некоторой матрицы M с элементами из K_p к диагональному виду:

$$\Gamma' = M^{-1}\Gamma M = \begin{pmatrix} \varepsilon_1 & & & \\ & \varepsilon_2 & & \\ & & \ddots & \\ & & & \varepsilon_m \end{pmatrix}.$$

Здесь $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_m$ — характеристические числа матрицы Γ, т. е. некоторые корни q-й степени из 1. Среди них имеется по крайней мере один, отличный от 1, иначе Γ была бы единичной матрицей. Пусть $\Delta' = M^{-1}\Delta M$. Тогда

$$\Delta'^{-1}\Gamma'\Delta' = \Gamma'^{\nu} = \begin{pmatrix} \varepsilon_1^{\nu} & & & \\ & \varepsilon_2^{\nu} & & \\ & & \ddots & \\ & & & \varepsilon_m^{\nu} \end{pmatrix}.$$

Но, с другой стороны, характеристические числа матриц Γ' и $\Delta'^{-1}\Gamma'\Delta'$ в совокупности совпадают, так как эти матрицы подобны. Таким образом, среди характеристических чисел матрицы Γ вместе с каждым числом ε имеется также ε^{ν}, а следовательно, и $\varepsilon^{\nu^2}, \dots \varepsilon^{\nu^{p-1}}$. Далее, в силу того, что вековое уравнение матрицы Γ имеет коэффициенты из R_p, оно имеет вместе с каждым корнем ε также корни $\varepsilon^p, \varepsilon^{p^2}, \dots \varepsilon^{p^{f-1}}$. Итак, матрица Γ имеет вместе с каждым характеристическим числом ε также характеристические числа ε^b, где b пробегает подгруппу мультипликативной группы по модулю q, порожденную элементами p и ν. Мультипликативная группа по модулю q циклична. Число p порождает в ней подгруппу порядка f, число ν — подгруппу порядка p, а оба вместе порождают подгруппу, порядок t которой есть $\frac{pf}{(p, f)}$. Матрица Γ, как было сказано выше, имеет хотя бы одно характеристическое число ε, не равное 1, а вместе с ним по крайней мере t попарно различных. Следовательно, порядок m матрицы Γ должен быть $\geqslant t$. Итак, $t = \frac{pf}{(p, f)} \leqslant m \leqslant n - 1$, ч. и т. д.

Заметим, что изложенный здесь результат может быть распространен на произвольные разрешимые группы в следующей форме: при фиксированных показателях $\alpha_1, \alpha_2, \dots \alpha_k$ среди разрешимых групп порядка $p_1^{\alpha_1} \dots p_k^{\alpha_k}$ существует лишь конечное число групп, длина специального ряда каждой из которых больше k.

Ленинградское отделение
Математического института им. В. А. Стеклова
Академии Наук СССР

Поступило
28 IV 1947