Доклады Академии Наук СССР
1954. Том XCV, № 4

МАТЕМАТИКА

С. А. ЧУНИХИН

О РАЗЛОЖЕНИИ П-ОТДЕЛИМЫХ ГРУПП В ПРОИЗВЕДЕНИЕ ПОДГРУПП

(Представлено академиком И. М. Виноградовым 21 I 1954)

§ 1. Произведением $\mathfrak{A}\mathfrak{B}$ некоторых совокупностей $\mathfrak{A}$ и $\mathfrak{B}$ элементов группы $\mathfrak{G}$ (в смысле Фробениуса) называют множество элементов $\mathfrak{G}$, представимых в виде: $G = AB$, $A \in \mathfrak{A}$, $B \in \mathfrak{B}$. Подобные произведения, множителями которых обычно на практике являются некоторые подгруппы, очень часто используются в теории групп и играют в ней весьма важную роль. К ним, в частности, прибегают с целью получения по данным подгруппам новых подгрупп того или иного требуемого вида, а также для установления критериев непростоты или разрешимости группы.

Так например, в 1930 г. нами была доказана ([1]) теорема: если порядки трех классов сопряженных элементов конечной группы попарно взаимно просты, то группа не может быть простой. Для доказательства была сначала получена следующая лемма: если $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$, где $\mathfrak{A}$ и $\mathfrak{B}$ — подгруппы $\mathfrak{G}$, причем $\mathfrak{A} \cap \mathfrak{B} \neq \mathfrak{E}$ ($\mathfrak{E}$ — единичная подгруппа) и $\mathfrak{A} \cap \mathfrak{B}$ содержит собственный нормальный делитель какой-либо из групп $\mathfrak{A}$ и $\mathfrak{B}$, то группа $\mathfrak{G}$ — не простая.

Эта лемма была в 1939 г. вторично доказана Орэ (теорема 12 главы I работы ([2])) и в третий раз — в 1950 г. Сепом и Редеи (теорема 2 работы ([3])).

Представление группы в форме произведения ее подгрупп («факторизация» группы) исследовалось также Ф. Голлом ([4]) Г. Цаппа, Ф. Казадио, Н. Ито, Г. Виландтом, а также и в ряде других работ Сепа и Редеи (обзор литературы см. ([5])).

В настоящей работе показывается возможность разложения в произведение своих подгрупп для введенных нами ранее ([6]) так называемых П-отделимых групп. Мы пользуемся при этом нашими прежними обозначениями и определениями (см., например, ([7])).

§ 2. Теорема 1. *Пусть m — наибольший П-силовский делитель порядка g П-отделимой группы $\mathfrak{G}$. Тогда всякому представлению m в виде произведения двух взаимно простых множителей $m = m_1 m_2$ соответствует представление группы $\mathfrak{G}$ в виде произведения $\mathfrak{G} = \mathfrak{M}_1\mathfrak{M}_2$, где $\mathfrak{M}_1$ и $\mathfrak{M}_2$ — некоторые такие подгруппы $\mathfrak{G}$, для которых числа m_1 и m_2, соответственно, являются наибольшими П-силовскими делителями их порядков.*

Доказательство. Допустим, что теорема неверна. Тогда среди групп, для которых она не выполняется, выберем группу $\mathfrak{G}$, имеющую наименьший порядок g. Это значит, что существует такое множество простых чисел П, что группа $\mathfrak{G}$ является П-отделимой, но утверждение теоремы по отношению к $\mathfrak{G}$ и П не выполняется. Так как при $m = 1$ имеется только одно разложение $m = 1 \cdot 1$, которому соответствует представление $\mathfrak{G} = \mathfrak{G}\mathfrak{G}$ требуемого вида, то $m > 1$. Поэтому П не пусто и $g > 1$.

Далее, так как разбиению $m = m \cdot 1$ тоже соответствует представление $\mathfrak{G} = \mathfrak{G}\mathfrak{E}$ ($\mathfrak{E}$ — единичная подгруппа) требуемого теоремой вида, то $1 < m_1 < m$ и $1 < m_2 < m$.

Отсюда, в силу $(m_1, m_2) = 1$, вытекает, что в разложении числа m на простые множители $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где $p_1, p_2, \ldots, p_k$ — все различные простые делители m, число $k > 1$.

Возьмем теперь предпоследний член $\mathfrak{L} \neq \mathfrak{E}$ главного ряда группы $\mathfrak{G}$. Так как $k > 1$, то нормальный делитель $\mathfrak{L}$ группы $\mathfrak{G}$ отличен от $\mathfrak{G}$.

Группа $\mathfrak{G}$ является П-отделимой, поэтому легко доказать — подобно предложению (H) работы (8), — что наибольший П-силовский делитель порядка l группы $\mathfrak{L}$ или имеет вид $p_i^{\omega_i} > 1$, где p_i — одно из чисел $p_1, p_2, \ldots, p_k$, или же равен единице.

Рассмотрим отдельно оба этих возможных случая.

1) Порядок $\mathfrak{L}$ равен $l = p_i^{\omega_i} t > 1$, где $(m, t) = 1$ и $p_i^{\omega_i} > 1$, $1 \leqslant \omega_i \leqslant \alpha_i$.

Рассмотрим сначала случай $t = 1$. Тогда $l = p_i^{\omega_i} > 1$. Число p_i должно делить одно из чисел m_1 и m_2. Пусть p_i делит m_1. Тогда фактор-группа $\mathfrak{G}/\mathfrak{L}$ будет П-отделимой группой (6) порядка $g/p_i^{\omega_i}$. Так как $\mathfrak{L} \neq \mathfrak{E}$ и $\mathfrak{L} \neq \mathfrak{G}$, то $1 < g/p_i^{\omega_i} < g$. Поэтому теорема для $\mathfrak{G}/\mathfrak{L}$ справедлива. Так как наибольший П-силовский делитель порядка группы $\mathfrak{G}/\mathfrak{L}$, очевидно, равен $m/p_i^{\omega_i}$ и допускает разложение $m/p_i^{\omega_i} = (m_1/p_i^{\omega_i}) m_2$, то это означает, что $\mathfrak{G}/\mathfrak{L} = (\mathfrak{M}_1/\mathfrak{L})(\mathfrak{M}_2/\mathfrak{L})$, где $\mathfrak{M}_1/\mathfrak{L}$ и $\mathfrak{M}_2/\mathfrak{L}$ — подгруппы $\mathfrak{G}/\mathfrak{L}$, наибольшими П-силовскими делителями порядков которых являются, соответственно, числа $m_1/p_i^{\omega_i}$ и m_2. Но тогда $\mathfrak{G} = \mathfrak{M}_1 \mathfrak{M}_2$ и наибольшим П-силовским делителем порядка $\overset{*}{m_1}$ подгруппы $\mathfrak{M}_1$ будет m_1, а наибольшим П-силовским делителем порядка $\overset{*}{m_2}$ подгруппы $\mathfrak{M}_2$ будет $p_i^{\omega_i} m_2$.

Так как $(m_1, m_2) = 1$ и $p_i^{\omega_i}$ делит по условию m_1, то и $(p_i^{\omega_i}, m_2) = 1$. Подгруппа $\mathfrak{L}$ является нормальным делителем $\mathfrak{G}$ и входит, очевидно, в $\mathfrak{M}_2$. Поэтому она инвариантна и в $\mathfrak{M}_2$. Применяя к $\mathfrak{M}_2$ и $\mathfrak{L}$ теорему Шура (7), заключаем, в силу $(p_i^{\omega_i}, m_2) = 1$, что $\mathfrak{M}_2$ имеет подгруппу $\mathfrak{M}_2'$ порядка $\overset{*}{m_2}/p_i^{\omega_i}$. Таким образом, наибольший П-силовский делитель порядка $\mathfrak{M}_2'$ равен m_2 и $\mathfrak{M}_2 = \mathfrak{L}\mathfrak{M}_2'$. Тогда $\mathfrak{G} = \mathfrak{M}_1(\mathfrak{L}\mathfrak{M}_2')$. Но $\mathfrak{L}$ входит и в $\mathfrak{M}_1$. Поэтому $\mathfrak{G} = \mathfrak{M}_1 \mathfrak{M}_2'$, где $\mathfrak{M}_1$ и $\mathfrak{M}_2'$ — подгруппы требуемого теоремой вида.

Получилось противоречие. Так как m_1 и m_2 равноправны, то так же рассматривается и случай, когда $p_i^{\omega_i}$ делит m_2.

Пусть теперь $t > 1$. Рассмотрим силовскую подгруппу $\mathfrak{P}$ порядка $p_i^{\omega_i} > 1$ группы $\mathfrak{L}$. Так как $\mathfrak{L}$ — нормальный делитель $\mathfrak{G}$, то все подгруппы $\mathfrak{G}$, сопряженные с $\mathfrak{P}$ в $\mathfrak{G}$, входят в $\mathfrak{L}$ и, как силовские подгруппы $\mathfrak{L}$, будут сопряжены с $\mathfrak{P}$ и в $\mathfrak{L}$. Если $\mathfrak{B}_{\mathfrak{P}}'$ и $\mathfrak{B}_{\mathfrak{P}}$ — нормализаторы $\mathfrak{P}$, соответственно, в $\mathfrak{L}$ и в $\mathfrak{G}$, то из предыдущего следует, что индекс $\mathfrak{B}_{\mathfrak{P}}'$ в $\mathfrak{L}$ равен индексу $\mathfrak{B}_{\mathfrak{P}}$ в $\mathfrak{G}$. Но индекс $\mathfrak{B}_{\mathfrak{P}}'$ в $\mathfrak{L}$, очевидно, взаимно прост с m. Поэтому порядок $\mathfrak{B}_{\mathfrak{P}}$ делится на m. Так как $\mathfrak{L}$ является предпоследним членом главного ряда $\mathfrak{G}$ и так как, в силу $t > 1$, $\mathfrak{P} \neq \mathfrak{L}$, то $\mathfrak{P}$ не может быть инвариантной в $\mathfrak{G}$, и поэтому порядок $\mathfrak{B}_{\mathfrak{P}}$ меньше g. Кроме того, $\mathfrak{B}_{\mathfrak{P}}$, как подгруппа П-отделимой группы $\mathfrak{G}$, тоже П-отделима. Следовательно, теорема для $\mathfrak{B}_{\mathfrak{P}}$ справедлива. Из всего предыдущего вытекает, что для $\mathfrak{B}_{\mathfrak{P}}$ существует представление в виде $\mathfrak{B}^{\mathfrak{P}} = \mathfrak{M}_1 \mathfrak{M}_2$, причем наибольший П-силовский делитель порядка $\mathfrak{M}_1$ равен m_1, а наибольший П-силовский делитель порядка $\mathfrak{M}_2$ равен m_2. Рассмотрим теперь подгруппу $\mathfrak{B}_{\mathfrak{P}}\mathfrak{L}$. Для нее имеем $[\mathfrak{B}_{\mathfrak{P}}\mathfrak{L}] = [\mathfrak{B}_{\mathfrak{P}}][\mathfrak{L}]/[\mathfrak{B}_{\mathfrak{P}} \cap \mathfrak{L}]$, где $[\mathfrak{B}_{\mathfrak{P}}\mathfrak{L}]$, $[\mathfrak{B}_{\mathfrak{P}}]$, $[\mathfrak{L}]$ и $[\mathfrak{B}_{\mathfrak{P}} \cap \mathfrak{L}]$ обозначают порядки соответствующих групп. Но $\mathfrak{B}_{\mathfrak{P}} \cap \mathfrak{L} = \mathfrak{B}'_{\mathfrak{P}}$. Поэтому $[\mathfrak{B}_{\mathfrak{P}}\mathfrak{L}] = [\mathfrak{B}_{\mathfrak{P}}][\mathfrak{L}]/[\mathfrak{B}'_{\mathfrak{P}}] = [\mathfrak{B}_{\mathfrak{P}}]([\mathfrak{L}]/[\mathfrak{B}'_{\mathfrak{P}}])$. Но индекс $\mathfrak{B}_{\mathfrak{P}}$ в $\mathfrak{G}$, как мы видели выше, равен $[\mathfrak{L}]/[\mathfrak{B}'_{\mathfrak{P}}]$. Поэтому порядок $\mathfrak{B}_{\mathfrak{P}}\mathfrak{L}$ равен g, т. е. $\mathfrak{G} = \mathfrak{B}_{\mathfrak{P}}\mathfrak{L}$. Следовательно, $\mathfrak{G} = (\mathfrak{M}_1\mathfrak{M}_2)\mathfrak{L}$. Если p_i делит m_1, то тогда $\mathfrak{G} = (\mathfrak{M}_1\mathfrak{L})\mathfrak{M}_2$ и $\mathfrak{M}_1\mathfrak{L}$ и $\mathfrak{M}_2$ будут подгруппами требуемого вида. Если же p_i делит m_2, то тогда $\mathfrak{G} = \mathfrak{M}_1(\mathfrak{M}_2\mathfrak{L})$ и $\mathfrak{M}_1$ и $\mathfrak{M}_2\mathfrak{L}$ опять будут подгруппами требуемого вида.

В обоих случаях получается противоречие.

2) Порядок $l > 1$ группы $\mathfrak{L}$ взаимно прост с m.

Тогда фактор-группа $\mathfrak{G}/\mathfrak{L}$ будет П-отделимой группой порядка g/l. Так как $\mathfrak{L} \neq \mathfrak{E}$ и $\mathfrak{L} \neq \mathfrak{G}$, то $1 < g/l < g$.

Поэтому теорема для $\mathfrak{G}/\mathfrak{L}$ справедлива. Так как наибольший П-силовский делитель порядка группы $\mathfrak{G}/\mathfrak{L}$ в данном случае, очевидно, равен m и допускает разложение $m = m_1m_2$, то поэтому и для $\mathfrak{G}/\mathfrak{L}$ имеем представление в виде $\mathfrak{G}/\mathfrak{L} = (\mathfrak{M}_1/\mathfrak{L})(\mathfrak{M}_2/\mathfrak{L})$, где $\mathfrak{M}_1/\mathfrak{L}$ и $\mathfrak{M}_2/\mathfrak{L}$ — подгруппы $\mathfrak{G}/\mathfrak{L}$, наибольшими П-силовскими делителями порядков которых являются, соответственно, числа m_1 и m_2. Но тогда $\mathfrak{G} = \mathfrak{M}_1\mathfrak{M}_2$, где, в силу $(m, l) = 1$, наибольшим П-силовским делителем порядка $\overset{*}{m}_1$ подгруппы $\mathfrak{M}_1$ является опять m_1, а наибольшим П-силовским делителем порядка $\overset{*}{m}_2$ подгруппы $\mathfrak{M}_2$ служит число m_2. Таким образом, разложение $\mathfrak{G} = \mathfrak{M}_1\mathfrak{M}_2$ имеет требуемый теоремой вид.

Опять получилось противоречие.

Теорема доказана.

Теорема 2. *Пусть $m > 1$ — наибольший П-силовский делитель порядка g П-отделимой группы $\mathfrak{G}$, и пусть $m = p_1^{\alpha_1}p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, где $p_1, p_2, \ldots, p_k$ — все различные простые делители m. Тогда группу $\mathfrak{G}$ можно представить в виде произведения $\mathfrak{G} = \mathfrak{P}_1\mathfrak{P}_2 \ldots \mathfrak{P}_k$, где $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_k$ — некоторые подгруппы $\mathfrak{G}$, имеющие наибольшими П-силовскими делителями своих порядков, соответственно, числа $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}$.*

Доказательство. При $k=1$ теорема очевидна. Поэтому пусть $k > 1$. Согласно теореме 1 имеем $\mathfrak{G} = \mathfrak{P}_1\mathfrak{M}_1$, причем наибольшим П-силовским делителем порядка $\mathfrak{P}_1$ является $p_1^{\alpha_1}$, а наибольшим П-силовским делителем порядка $\mathfrak{M}_1$ является число $p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Прилагая теперь теорему 1 к $\mathfrak{M}_1$, имеем: $\mathfrak{M}_1 = \mathfrak{P}_2\mathfrak{M}_2$. Поэтому $\mathfrak{G} = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{M}_2$. Продолжая так и дальше, придем после k шагов к требуемому разложению $\mathfrak{G}$ на множители.

§ 3. Вопрос о возможности выбора систем подгрупп, удовлетворяющих требованиям теоремы 2, а также и остальным условиям (перестановочность, сопряженность) работы Ф. Голла ([4]), остается открытым.

Пример простой группы порядка 60 показывает при $\Pi=\{2,5\}$ невозможность обращения теоремы 2.

Поступило
11 I 1954

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] С. Чунихин, C. R., **191**, 397 (1930). [2] O. Ore, Duke Math. J., **5**, 431 (1939). [3] J. Szep, L. Rédei, Acta Sci. Math. Szeged, **13**, 3—4, 235 (1950). [4] Ph. Hall, Proc. London Math. Soc., **43**, 316 (1937). [5] Math. Rev., **14**, No. 1, 13 (1953). [6] С. А. Чунихин, ДАН, 59, № 3, 443 (1948). [7] С. А. Чунихин, Матем. сборн., **33** (75) : 1, 111 (1953). [8] С. А. Чунихин, Матем. сборн., **25** (67) : 3, 321 (1949).