

С. А. ЧУНИХИН

## О ФАКТОРИЗАЦИИ КОНЕЧНЫХ ГРУПП

(Представлено академиком И. М. Виноградовым 25 V 1954)

§ 1. Интерес к конечным группам и, в частности, к вопросам их факторизации, т. е. к возможности представления конечных групп в виде произведений (в смысле Фробениуса) некоторых их подгрупп, в последние годы значительно повысился. Исследуются как возможности факторизовать тем или иным способом определенные известные классы конечных групп, так и свойства конечных групп, допускающих некоторую определенную заданную факторизацию (прямая и обратная задачи факторизации). Некоторыми авторами рассматриваются также и возможности представления конечных групп в виде произведений определенных комплексов их элементов, не являющихся уже обязательно подгруппами.

В настоящей работе показывается, что известные результаты Ф. Голла (разрешимые группы) и Шура (факторизационная теорема) являются частными проявлениями некоторых общих закономерностей, присущих всем вообще конечным группам.

§ 2. Определение 1. Пусть дана некоторая конечная совокупность положительных  $> 1$  целых чисел  $N$ , среди которых могут быть и равные. Пусть  $n_1$  и  $n_2$  — два числа, каждое из которых входит в  $N$  (поэтому они могут быть равными даже тогда, когда среди чисел  $N$  нет равных). Если при этом из чисел, входящих в  $N$ , можно образовать такую конечную последовательность, что ее первым членом будет  $n_1$ , а последним — число  $n_2$  и каждые два соседних члена которой не будут взаимно простыми, то число  $n_1$  назовем связанным с числом  $n_2$  в совокупности  $N$  или при помощи совокупности  $N$ .

В частности, если  $(n_1, n_2) > 1$ , то  $n_1$  связано с  $n_2$  в совокупности  $n_1, n_2$ . Далее, из  $(n, n) = n > 1$  следует, что любое положительное целое  $> 1$  число связано само с собой в любой совокупности чисел, куда оно входит.

Очевидно, что свойство связности чисел рефлексивно, симметрично и транзитивно. Следовательно, по отношению к нему совокупность  $N$  распадается на попарно не пересекающиеся классы взаимно связанных чисел. Очевидно, что все числа любого такого класса связаны уже в самом этом классе.

Определение 2. Произведение всех чисел одного какого-либо класса связанных чисел совокупности  $N$  назовем блоком этого класса чисел совокупности  $N$ .

Так как каждое число одного класса взаимно просто с каждым числом отличного от него другого класса, то блоки различных классов будут взаимно простыми, а потому и различными числами. Вследствие этого можно говорить просто о блоках совокупности чисел  $N$ . Очевидно, что каждый такой блок больше единицы. Применим теперь определения 1 и 2 к индексам композиционного ряда конечной группы  $\mathfrak{G}$  порядка  $g > 1$ .

Определение 3. Блоки совокупности всех индексов композиционного ряда группы  $\mathfrak{G}$  назовем композиционными блоками группы  $\mathfrak{G}$ .

Очевидно, что произведение всех композиционных блоков группы  $\mathfrak{G}$  равно ее порядку.

Ниже приводятся основные моменты дальнейшего исследования и полученные при этом результаты.

§ 3. Пусть  $\mathfrak{E}$  обозначает единичную подгруппу  $\mathfrak{G}$ .

Лемма 1. Каждый композиционный блок подгруппы  $\mathfrak{H} \neq \mathfrak{E}$  группы  $\mathfrak{G}$  является делителем некоторого единственного композиционного блока группы  $\mathfrak{G}$ .

Лемма 2. Если  $\mathfrak{H}$  — нормальный делитель группы  $\mathfrak{G}$  и  $\mathfrak{H} \neq \mathfrak{G}$ , то каждый композиционный блок фактор-группы  $\mathfrak{G}/\mathfrak{H}$  является делителем некоторого единственного композиционного блока группы  $\mathfrak{G}$ .

Лемма 3. Если порядок подгруппы  $\mathfrak{H}$  группы  $\mathfrak{G}$  имеет общий наибольший делитель  $m' > 1$  с композиционным блоком  $t$  группы  $\mathfrak{G}$ , то  $m'$  является произведением всех тех композиционных блоков  $\mathfrak{H}$ , которые делят  $t$ .

Лемма 4. Если  $\mathfrak{H}$  — нормальный делитель  $\mathfrak{G}$ , и если порядок фактор-группы  $\mathfrak{G}/\mathfrak{H}$  имеет общий наибольший делитель  $m' > 1$  с композиционным блоком  $t$  группы  $\mathfrak{G}$ , то  $m'$  является произведением всех тех композиционных блоков  $\mathfrak{G}/\mathfrak{H}$ , которые делят  $t$ .

Теорема 1. Если делитель  $h > 1$  порядка  $g$  группы  $\mathfrak{G}$  является композиционным блоком группы  $\mathfrak{G}$  или произведением каких-либо нескольких композиционных блоков  $\mathfrak{G}$ , то группа  $\mathfrak{G}$  имеет по крайней мере одну подгруппу порядка  $h$ .

Доказательство теоремы 1 проводится по схеме доказательства теоремы 1 работы (1) с использованием леммы 4, а также следующего предложения: порядок предпоследнего члена главного ряда  $\mathfrak{G}$  является делителем некоторого единственного блока  $\mathfrak{G}$ .

Теорема 2. Всякому представлению порядка  $g > 1$  конечной группы  $\mathfrak{G}$  в виде произведения  $g = h_1 h_2 \dots h_\sigma$ , где  $h_1, h_2, \dots, h_\sigma$  являются композиционными блоками группы  $\mathfrak{G}$  или произведениями каких-либо нескольких композиционных блоков  $\mathfrak{G}$ , соответствует представление группы  $\mathfrak{G}$  в виде произведения  $\mathfrak{G} = \mathfrak{H}_1 \mathfrak{H}_2 \dots \mathfrak{H}_\sigma$ , где  $\mathfrak{H}_1, \mathfrak{H}_2, \dots, \mathfrak{H}_\sigma$  — некоторые подгруппы  $\mathfrak{G}$ , имеющие своими порядками, соответственно, числа  $h_1, h_2, \dots, h_\sigma$ .

Доказательство проводится тем же путем, что и доказательство теоремы 2 работы (1).

Нужным для дальнейшего частным случаем теоремы 2 является нижеследующая

Теорема 3. Если  $g = m_1 m_2 \dots m_k$  есть представление порядка  $g > 1$  конечной группы  $\mathfrak{G}$  в виде произведения ее композиционных блоков, то группу  $\mathfrak{G}$  можно представить в виде произведения  $\mathfrak{G} = \mathfrak{M}_1 \mathfrak{M}_2 \dots \mathfrak{M}_k$ , где  $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_k$  — некоторые подгруппы  $\mathfrak{G}$  соответственно порядков  $m_1, m_2, \dots, m_k$ .

§ 4. Определение 4. Подгруппы  $\mathfrak{M}_1, \mathfrak{M}_2, \dots, \mathfrak{M}_k$  теоремы 3 назовем компонентами группы  $\mathfrak{G}$ , а их совокупность — полной системой компонент  $\mathfrak{G}$ . Полных систем компонент у группы  $\mathfrak{G}$  может быть и несколько.

Исследуем полные системы компонент, используя прием, аналогичный методу Ф. Голла (2).

Определение 5. Если  $m_1, m_2, \dots, m_k$  — совокупность всех композиционных блоков группы  $\mathfrak{G}$  и  $m_i$  — какой-либо из них, то каждую подгруппу индекса  $m_i$  группы  $\mathfrak{G}$ , существующую на основании теоремы 1, назовем  $m_i$ -дополнением группы  $\mathfrak{G}$ . Пусть теперь для каждого  $i$  ( $1 \leq i \leq k$ ) среди всех имеющихся  $m_i$ -дополнений группы  $\mathfrak{G}$

выбрано одно какое-либо  $\mathcal{M}'_i$ . Тогда совокупность подгрупп  $\mathcal{M}'_1, \mathcal{M}'_2, \dots, \mathcal{M}'_k$  назовем полной системой  $m_i$ -дополнений группы  $\mathcal{G}$ . Очевидно, что таких систем в группе  $\mathcal{G}$ , вообще говоря, существует несколько.

Обозначим теперь через  $\mathcal{M}_A$  пересечение всех тех подгрупп некоторой данной полной системы  $m_i$ -дополнений  $\mathcal{M}'_1, \mathcal{M}'_2, \dots, \mathcal{M}'_k$ , у которых индексы входят в некоторое заданное подмножество  $A$  множества чисел  $1, 2, \dots, k$ . Таким образом, получаем следующее

Определение 6.  $\mathcal{M}_A = \bigcap_{i \in A} \mathcal{M}'_i$ . В частности, если  $A$  состоит только из одного числа  $i$ , то  $\mathcal{M}_A = \mathcal{M}'_i$ . Наконец, если  $A$  — пустое множество, то положим, по определению,  $\mathcal{M}_A = \mathcal{G}$ .

Определение 7. Множество всех  $2^k$  подгрупп вида  $\mathcal{M}_A$ , где  $A$  пробегает все подмножества множества чисел  $1, 2, \dots, k$ , назовем блок-системой группы  $\mathcal{G}$ , порожденной заданной полной системой  $m_i$ -дополнений  $\mathcal{M}'_1, \mathcal{M}'_2, \dots, \mathcal{M}'_k$ .

Лемма 5. Порядок  $\mathcal{M}_A$  равен  $\prod_{i \in A} m_i$ .

Лемма 6. Если  $A$  и  $B$  — произвольные подмножества множества чисел  $1, 2, \dots, k$ , то  $\mathcal{M}_{A \cup B} = \mathcal{M}_A \cap \mathcal{M}_B$  и  $\mathcal{M}_A \cap \mathcal{M}_B = \mathcal{M}_A \mathcal{M}_B = \mathcal{M}_B \mathcal{M}_A$ , т. е. все подгруппы данной блок-системы группы  $\mathcal{G}$  попарно перестановочны.

Из этих лемм следует

Теорема 4. У всякой конечной группы существует такая полная система компонент, что любые две входящие в нее компоненты перестановочны.

§ 5. Отметим еще некоторые свойства конечных групп, связанных с понятием композиционного блока.

Теорема 5. Если делитель  $h$  порядка  $g > 1$  группы  $\mathcal{G}$  является композиционным блоком группы  $\mathcal{G}$  или произведением каких-либо нескольких композиционных блоков  $\mathcal{G}$ , то всякая разрешимая подгруппа  $\mathcal{H}_1$  порядка  $h_1$ , делящего  $h$ , группы  $\mathcal{G}$  входит по крайней мере в одну из подгрупп порядка  $h$  группы  $\mathcal{G}$ .

Доказательство теоремы 5 проводится подобно доказательству теоремы XII нашей работы <sup>(3)</sup> с использованием замечания, приведенного выше по поводу доказательства теоремы I, а также и нашей основной теоремы о П-отделимых группах <sup>(4)</sup>.

Лемма 7. Пусть  $t$  — некоторый композиционный блок конечной группы  $\mathcal{G}$  порядка  $g > 1$  и пусть  $\mathcal{M}$  — подгруппа порядка  $t$  группы  $\mathcal{G}$ . Тогда индексы композиционного ряда  $\mathcal{M}$  являются также и индексами композиционного ряда  $\mathcal{G}$  и притом как раз теми, произведение которых равно  $t$ . При этом соответствующие одному и тому же индексу фактор-группы композиционных рядов групп  $\mathcal{G}$  и  $\mathcal{M}$  изоморфны.

Теорема 6. Пусть  $t$  — некоторый композиционный блок конечной группы  $\mathcal{G}$  порядка  $g > 1$  и пусть  $\mathcal{M}$  — подгруппа порядка  $t$  группы  $\mathcal{G}$ . Пусть еще  $\Pi$  — некоторое непустое множество простых чисел, делящих  $t$ . Если  $\mathcal{M}$  является П-отделимой группой, то и группа  $\mathcal{G}$  тоже будет П-отделимой. Обратное предложение очевидно.

Теорема 7. Пусть  $t$  — некоторый композиционный блок конечной группы  $\mathcal{G}$  порядка  $g > 1$ , и пусть  $\mathcal{M}$  — подгруппа порядка  $t$  группы  $\mathcal{G}$ . Если  $\mathcal{M}$  разрешима, то  $t = p^\alpha$ , где  $p$  — некоторое простое число и группа  $\mathcal{G}$  будет тогда  $p$ -разрешимой. Обратное предложение очевидно.

Теорема 8. Если конечная группа  $\mathcal{G}$  порядка  $g > 1$  имеет разрешимые подгруппы  $\mathcal{M}_1, \mathcal{M}_2, \dots, \mathcal{M}_k$  соответственно порядков

$m_1, m_2, \dots, m_k$ , где  $m_1, m_2, \dots, m_k$  — все композиционные блоки  $\mathfrak{G}$ , то и  $\mathfrak{G}$  разрешима. Обратное предложение очевидно.

Теорема 9. Пусть  $\Pi$  — некоторое непустое множество простых делителей порядка  $g > 1$  конечной группы  $\mathfrak{G}$ , причем никакие два различных из них не делят какой-либо один и тот же композиционный блок  $\mathfrak{G}$ . Тогда  $\mathfrak{G}$  является  $\Pi$ -отделимой группой.

Теорема 10. Пусть делитель  $h$  порядка  $g > 1$  группы  $\mathfrak{G}$  является композиционным блоком группы  $\mathfrak{G}$  или произведением нескольких каких-либо композиционных блоков  $\mathfrak{G}$ . Если одна из подгрупп порядка  $h$  группы  $\mathfrak{G}$  разрешима, то тогда и все остальные подгруппы порядка  $h$  из  $\mathfrak{G}$  разрешимы и сопряжены с ней.

§ 6. Допустим, что рассматриваемая конечная группа  $\mathfrak{G}$  разрешима. Тогда, по теореме 7, все ее композиционные блоки будут степенями различных простых чисел.

Следовательно, основные результаты Ф. Голла о разрешимых группах являются частными случаями вышеприведенных теорем 1—5 и теоремы 10.

Рассмотрим еще случай теоремы Шура.

Пусть группа  $\mathfrak{G}$  порядка  $mn > 1$ ,  $(m, n) = 1$ , имеет нормальный делитель  $\mathfrak{H}$  порядка  $n$ . Уплотняя ряд  $\mathfrak{G} \supset \mathfrak{H} \supset \mathfrak{E}$  до композиционного, видим, что  $m$  и  $n$  будут или композиционными блоками  $\mathfrak{G}$  или же произведениями таких блоков. По теореме 1,  $\mathfrak{G}$  будет иметь подгруппу порядка  $m$ . Отсюда заключаем, что частным случаем приведенной выше теоремы 1 является факторизационная теорема Шура.

Белорусский институт  
инженеров железнодорожного  
транспорта

Поступило  
24 V 1954

#### ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- <sup>1</sup> С. А. Чунихин, ДАН, 95, № 4 (1954). <sup>2</sup> Ph. Hall, Proc. Lond. Math. Soc., 43, 316 (1937). <sup>3</sup> С. А. Чунихин, Матем. сборн., 25 (67), № 3, 321 (1949). <sup>4</sup> С. А. Чунихин, ДАН, 59, № 3, 443 (1948).