Записки научных
семинаров ПОМИ
Том 301, 2003 г.

И. Шур

К ТЕОРИИ ТРАНЗИТИВНЫХ ГРУПП ПЕРЕСТАНОВОК*

Предисловие переводчика

В статье, перевод которой предлагается вниманию читателя, впервые используется метод исследования групп перестановок с регулярной подгруппой, названный впоследствии методом колец Шура. В дальнейшем этот метод был развит учеником Шура Г. Виландтом в монографии [6] и применен для обобщения результатов Шура, представленных в этой работе. Теория представлений колец Шура была изучена в серии работ О. Тамашке (см. [5]). О связях теории колец Шура и алгебраической комбинаторики см. [1] и [4]. Отметим также полученное в последние годы полное описание колец Шура над конечной циклической группой (см. [2] и [3]).

1. Э. Баннаи, Т. Ито, *Алгебраическая комбинаторика 1. Схемы отношений*, М., Мир (1987).
2. С. Евдокимов, И. Пономаренко, *Характеризация циклотомических схем и нормальные кольца Шура над циклической группой.* — Алгебра и анализ **14**, вып. 2 (2002), 11–55.
3. K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups.* II. — J. Algebra **183** (1996), 273–285.
4. M. Muzychuk, M. Klin, R. Pöschel, *The isomorphism problem for circulant graphs via Schur ring theory.* — DIMACS Ser. Discrete Math. Theor. Comput. Sci. **56** (2001), 241–264.
5. O. Tamaschke, *On Schur-rings which define a proper character theory on finite groups.* — Math. Z. **117** (1970) 340–360.
6. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York–London (1964).

* * *

Следующие два важных утверждения о группах перестановок были доказаны В. Бернсайдом:

---

*I. Schur. Zur Theorie der einfach transitiven Permutationsgruppen. Sitzung der physikalisch-mathematischen Klasse vom. 15. Juni 1933, 598–623. Перевод с немецкого И. Н. Пономаренко.

(I) Транзитивная группа перестановок простой степени является либо дважды транзитивной, либо разрешимой [1, с. 174; 3, с. 171].

(II) Пусть $n = p^a$ – отличная от p степень простого числа p. Если группа перестановок $\mathfrak{G}$ степени n содержит цикл P порядка n, то $\mathfrak{G}$ либо дважды транзитивна, либо импримитивна [2, с. 343].

В связи с этим утверждением Бернсайд высказал предположение, что аналогичный результат справедлив для каждой группы перестановок $\mathfrak{G}$ степени n, содержащей регулярную абелеву подгруппу $\mathfrak{H}$ степени n[1]. В этой общности предположение неверно, как показывает простой контрпример (§6). Однако, оно становится справедливым для каждой натуральной степени n, если группа $\mathfrak{H}$ предполагается циклической, а n не является простым числом:

(III) Если группа перестановок $\mathfrak{G}$, степень n которой не является простым числом, содержит цикл P порядка n, то $\mathfrak{G}$ либо дважды транзитивна, либо импримитивна.

Доказательство этих столь просто формулируемых утверждений представляется довольно сложным. В случае степени простого числа Бернсайдом использовалось утверждение из теории групповых характеров, требующее операции извлечения корня из единицы. Я привожу доказательство, не содержащее ни в какой форме обращения к иррациональным числам. Оно прежде всего направлено на изучение в контексте предположения Бернсайда общего случая произвольной регулярной группы перестановок $\mathfrak{H}$, содержащейся в большей группе $\mathfrak{G}$ той же степени. При этом возникает разложение элементов из $\mathfrak{H}$ в семейство комплексов, которые я называю простыми комплексами на $\mathfrak{H}$. Главную роль играет тот факт, что совокупность этих комплексов обладает "кольцевыми" свойствами (§2).

Преимущество простых комплексов состоит в том, что с каждой группой перестановок $\mathfrak{G}$ связывается кольцо матриц (§1). Однако эти комплексы можно также определить чисто теоретико-групповым образом и исследовать их без использования матриц. Это требует расширения фробениусовского исчисления, которое достигается рассмотрением группы $\mathfrak{H}$ как системы над гиперкомплексными величинами. Использование матричных колец мне ка-

[1] В этом случае группа $\mathfrak{G}$ очевидно должна быть транзитивной.

жется заслуживающим внимания также потому, что эта идея сама по себе может иметь смысл для продолжения исследований. Утверждение III допускает достойные внимания приложения также и к другим проблемам теории групп, равно как и к вопросам из теории чисел и анализа. Из этих приложений я намереваюсь в будущем подготовить работу.

1. Кольцо матриц, связанное с группой перестановок

Пусть $\mathfrak{G}$ – группа перестановок порядка g на множестве символов $1, 2, \ldots, n$. Каждую перестановку

$$S = \binom{\nu}{\nu'} \quad (\nu = 1, 2, \ldots, n) \tag{1}$$

группы $\mathfrak{G}$ мы записываем как матрицу степени n

$$M = (e_{\alpha', \beta}) \quad (\alpha, \beta = 1, 2, \ldots, n),$$

где $e_{\chi,\lambda}$ равно 0 или 1 в зависимости от того, $\chi \neq \lambda$ или $\chi = \lambda$.

Рассмотрим совокупность $\mathfrak{V}$ матриц

$$V = (v_{\alpha,\beta}), \quad (\alpha, \beta = 1, 2, \ldots, n),$$

перестановочных со всеми g матрицами M. Очевидно, что $\mathfrak{V}$ обладает свойствами кольца, то есть вместе с V_1 и V_2 множество $\mathfrak{V}$ содержит также $V_1 V_2$ и $x_1 V_1 + x_2 V_2$ для произвольных постоянных величин x_1 и x_2. Далее $\mathfrak{V}$ будет обозначать матричное кольцо, отвечающее группе $\mathfrak{G}$.

Простое вычисление показывает, что

$$MVM^{-1} = (v_{\alpha', \beta'}).$$

Для того, чтобы V принадлежала $\mathfrak{V}$, необходимо и достаточно, чтобы для каждой перестановки (1) группы $\mathfrak{G}$ удовлетворялись n^2 равенств

$$(v_{\alpha,\beta}) = (v_{\alpha',\beta'}), \quad (\alpha, \beta = 1, 2, \ldots, n). \tag{2}$$

Эти условия выполняются во всяком случае для единичной матрицы E и для матрицы

$$W = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ . & . & \cdots & . \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

Кольцо $\mathfrak{B}$ поэтому содержит все матрицы $aE + bW$, образующие в силу равенства $W^2 = nW$ подкольцо $\mathfrak{B}_0$ кольца $\mathfrak{B}$. Это дает простой критерий проверки дважды транзитивности:

(A) Группа перестановок $\mathfrak{G}$ дважды транзитивна тогда и только тогда, когда $\mathfrak{B} = \mathfrak{B}_0$.[2]

Нас интересует случай, когда группа $\mathfrak{G}$ является однократно транзитивной. Тогда ранг r матричного кольца $\mathfrak{B}$, то есть максимальное число линейно независимых матриц из $\mathfrak{B}$, должен быть по крайней мере 3.[3]

Поскольку условие (2) должно выполняться для всех перестановок S из $\mathfrak{G}$, то ясно, что матрица из $\mathfrak{B}$ характеризуется тем, что n^2 ее позиций разбиваются в r подмножеств, в каждом из которых на соответствующих местах стоит одно и то же число. Поэтому в $\mathfrak{B}$ имеется линейный базис

$$U_1, U_2, \dots, U_r, \tag{3}$$

такой, что выполняются следующие условия:

1. Каждый коэффициент матрицы U_ρ есть либо 0, либо 1.

2. В каждой из n^2 позиций число 1 появляется только в одной из r матриц (3).

Отсюда немедленно следует, что

$$U_1 + U_2 + \cdots + U_r = W. \tag{4}$$

Однозначно определенный базис (3) называется *главным базисом* (Hauptbasis) кольца $\mathfrak{B}$. Далее я называю каждую матрицу U_ρ *простым* (primäres) элементом кольца $\mathfrak{B}$. Каждое матричное кольцо, обладающее базисом со свойствами 1. и 2. и, кроме того, содержащее единичную матрицу, называется *родовым кольцом* (Stammring).

Такое кольцо $\mathfrak{B}$ очевидно обладает следующим свойством:

---

[2] Этот критерий идентичен критерию, которым часто пользовались Фробениус и Бернсайд: группа $\mathfrak{G}$ дважды транзитивна тогда и только тогда, когда группа матриц M имеет в точности две неприводимых составляющих [2, с. 338].

[3] Если группа $\mathfrak{G}$ транзитивна и $\mathfrak{G}_1$ есть совокупность всех перестановок из $\mathfrak{G}$, оставляющих символ 1 неподвижным, то легко понять, что число транзитивных классов, в которые распадается множество $2, 3, \dots, n$ под действием $\mathfrak{G}_1$, равно $r - 1$. Это, однако, не будет использоваться далее.

(B) Если $(v_{\alpha,\beta})$ – матрица из $\mathfrak{B}$ и числа $v_{\alpha,\beta}$ заменяются на другие числа $v_{\alpha',\beta'}$ так, что равные числа остаются равными, то матрица $(v_{\alpha',\beta'})$ также принадлежит $\mathfrak{B}$.

Отсюда, в частности, следует свойство

(C) Пусть $(v_{\alpha,\beta})$ – целочисленная матрица родового кольца $\mathfrak{B}$. Если k – произвольное целое положительное число, то и матрица неотрицательных наименьших остатков $v_{\alpha,\beta}$ по модулю k принадлежит $\mathfrak{B}$.

2. Группы перестановок с регулярными подгруппами

Пусть $\mathfrak{G}$ – группа перестановок степени n и

$$\mathfrak{H} = H_1 + H_2 + \cdots + H_n$$

– транзитивная подгруппа порядка n группы $\mathfrak{G}$, заданная так, что вместо символов $1, 2, \ldots, n$ группа $\mathfrak{G}$ переставляет n элементов H_ν. Тогда перестановка S из $\mathfrak{G}$ характеризуется тем, что каждый элемент P из $\mathfrak{H}$ она переводит в элемент P', причем P' одновременно с P пробегает все элементы $\mathfrak{H}$. Мы обозначаем это следующим образом:

$$P_S = P'.$$

Если, в частности, S принадлежит $\mathfrak{H}$, то

$$P_S = PS. \tag{5}$$

Как обычно, под e_R мы понимаем число 1 или 0, в зависимости от того, является ли элемент R из $\mathfrak{H}$ единичным элементом E или отличен от него, так что матрица M, отвечающая R, может быть записана следующим образом:

$$M = (e_{PRQ^{-1}}), \quad (P, Q = H_1, H_2, \ldots, H_n).$$

Матрица V, перестановочная с этими n матрицами, должна тогда иметь вид фробениусовской групповой матрицы

$$V = (v_{PQ^{-1}}).$$

Определяя для каждого элемента из $\mathfrak{H}$

$$R^* = (e_{R^{-1}PQ^{-1}}),$$

имеем
$$V = \sum v_R R^*, \quad (R = H_1, H_2, \ldots, H_n). \tag{6}$$
Матрицы R^* представляют группу $\mathfrak{H}$, то есть для любых двух элементов R и S из $\mathfrak{H}$ выполняется
$$(RS)^* = R^* S^*. \tag{7}$$
Если V, в частности, есть простая матрица, то есть элемент главного базиса (3) кольца $\mathfrak{B}$, то в силу (6) она имеет вид
$$V = R_1^* + R_2^* + \cdots + R_k^*,$$
где $R_1, R_2, \ldots, R_k$ – попарно различные элементы группы $\mathfrak{H}$. Комплекс (Komplex)
$$\mathfrak{R} = R_1 + R_2 + \cdots + R_k$$
я называю *простым комплексом* (primären Komplex).

Таким образом, r матриц главного базиса нашего кольца $\mathfrak{B}$ определяют r соответствующих комплексов
$$\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_r, \tag{8}$$
состоящих из элементов группы $\mathfrak{H}$. Один из них совпадает с единичным элементом E, и каждый элемент из $\mathfrak{H}$ содержится в одном и только одном комплексе $\mathfrak{R}_\rho$. Это следует из равенства (4) и того факта, что в нашем случае матрица W равна сумме всех матриц R^*. Отсюда также имеем
$$\mathfrak{R}_1 + \mathfrak{R}_2 + \cdots + \mathfrak{R}_r = \mathfrak{H}.$$
Наряду с r комплексами (8) мы также рассматриваем суммы
$$\mathfrak{R} = \mathfrak{R}_\alpha + \mathfrak{R}_\beta + \cdots$$
с попарно различными индексами $\alpha, \beta, \ldots$. Такой комплекс из элементов группы $\mathfrak{H}$ я называю *главным комплексом* (Hauptkomplex). Если $K_1, K_2, \ldots, K_m$ – составляющие $\mathfrak{R}$ элементы из $\mathfrak{H}$, то матрица
$$V = K_1^* + K_2^* + \ldots + K_m^* \tag{9}$$
принадлежит кольцу $\mathfrak{B}$. Если снова $V = (v_{PQ^{-1}})$, то v_R равен 0 или 1 в зависимости от того, принадлежит ли R к $\mathfrak{R}$ или нет.

Если теперь матрица V перестановочна с каждой матрицей M, отвечающей перестановке S из $\mathfrak{G}$, то из вышесказанного следует, что для двух элементов P и Q из $\mathfrak{G}$ имеет место равенство

$$v_{PQ^{-1}} = v_{P'Q'^{-1}} \quad (P' = P_S,\ Q' = Q_S).$$

Это означает, что $P'{Q'}^{-1}$ входит в комплекс $\mathfrak{R}$ тогда и только тогда, когда это выполнено для PQ^{-1}. Другое следствие состоит в том, что если P содержится в комплексе $\mathfrak{R}Q$, то P' содержится в комплексе $\mathfrak{R}Q'$. Это условие, очевидно, также достаточно для характеризации $\mathfrak{R}$ как главного комплекса, поскольку из него следует, что соответствущая матрица (9) принадлежит кольцу $\mathfrak{B}$.

Сформулируем все эти результаты в следующем утверждении:

(A) Если $\mathfrak{H}$ – регулярная группа перестановок степени n, то с каждой группой $\mathfrak{G}$ той же степени, содержащей $\mathfrak{H}$ в качестве подгруппы, связано разложение n элементов из $\mathfrak{H}$ в некоторые хорошо определенные комплексы (Teilkomplexe) $\mathfrak{R}_1, \mathfrak{R}_2, \dots, \mathfrak{R}_r$. Эти комплексы и составленные из них сложением главные комплексы $\mathfrak{R}$ характеризуются тем, что если $\mathfrak{R}$ состоит из элементов $K_1, K_2, \dots, K_m$, то для каждого элемента Q из $\mathfrak{H}$ и каждой перестановки S из $\mathfrak{G}$ выполнено

$$(\mathfrak{R}Q)_S = \sum_{\mu=1}^{m}(K_\mu Q)_S = \mathfrak{R}Q_S. \tag{10}$$

Группа $\mathfrak{G}$ дважды транзитивна тогда и только тогда, когда $r = 2$.

Из того, что множество матриц $\mathfrak{B}$ образует кольцо, а также непосредственно из (10) получаем

(B) Любое произведение главных комплексов снова является главным комплексом.

Далее мы будем использовать следующие два простые утверждения, проверяемые непосредственно.

(C) Если $\mathfrak{R}$ и $\mathfrak{L}$ – два главных комплекса, то и их пересечение $\mathfrak{D}$ также является главным комплексом.

(D) Если матрица V кольца $\mathfrak{B}$ записана в виде (6) и слагаемые упорядочены в соответствии со значениями коэффициентов v_R, то она может рассматриваться как комплекс, составленный из главных комплексов.

Следующее новое для нас утверждение играет важную роль, поскольку дает независимое от матричного кольца определение простых комплексов $\mathfrak{R}_\rho$:

(E) Пусть $\mathfrak{G}_1$ – совокупность всех перестановок из $\mathfrak{G}$, которые оставляют неподвижным единичный элемент E из $\mathfrak{H}$ (рассматриваемый как один из переставляемых символов). Если $\mathfrak{G}_1$ раскладывает $n-1$ элемент из $\mathfrak{H}$ в систему транзитивности (Transitivitätssysteme)

$$\mathfrak{T}_1, \mathfrak{T}_2, \ldots, \mathfrak{T}_s,$$

то эта система с присоединенным E совпадает с нашими простыми комплексами $\mathfrak{R}_1, \mathfrak{R}_2, \ldots, \mathfrak{R}_r$.

Именно, если $\mathfrak{R}$ совпадает с одним из $\mathfrak{R}_\rho$ и не равен E, то из (10) получаем для $Q = E$ и произвольного элемента S из $\mathfrak{G}_1$, что $\mathfrak{R}_S = \mathfrak{R}$. Это означает, что каждый $\mathfrak{R}_\rho$ есть либо $\mathfrak{T}_\sigma$, либо сумма нескольких $\mathfrak{T}_\sigma$[4]. Остается показать, что, наоборот, каждая система $\mathfrak{R} = \mathfrak{T}_\sigma$ для каждой Q из $\mathfrak{H}$ и каждого S из $\mathfrak{G}$ удовлетворяет равенству (10).

Из сказанного имеем прежде всего следующее: в силу (10) для любого элемента Q и любых двух перестановок $S = S_1$ и $S = S_2$ имеем

$$\mathfrak{R}Q_{S_1S_2} = \mathfrak{R}(Q_{S_1})_{S_2} = (\mathfrak{R}Q_{S_1})_{S_2} = ((\mathfrak{R}Q)_{S_1})_{S_2} = (\mathfrak{R}Q)_{S_1S_2},$$

и, значит, (10) выполнено также для S_1S_2. Кроме того, в силу (5) равенство (10) выполнено для каждой перестановки S из $\mathfrak{H}$, и потому достаточно проверить (10) в предположении, что S содержится в $\mathfrak{G}_1$.

Пусть снова

$$\mathfrak{R} = \mathfrak{T}_\sigma = \sum_{\mu=1}^{m} K_\mu,$$

так что, очевидно, имеем

$$(K_\mu Q)_S = E_{K_\mu QS}. \tag{11}$$

Любой элемент из $\mathfrak{G} = \mathfrak{G}_1\mathfrak{H}$, скажем QS, может быть записан в виде S_1Q_1, где S_1 – из $\mathfrak{G}_1$ и Q_1 – из $\mathfrak{H}$. Поскольку $E_{S_1} = E$, то

$$Q_S = E_{QS} = E_{S_1Q_1} = (E_{S_1})_{Q_1} = E_{Q_1} = Q_1 \tag{12}$$

[4] Поскольку $r = 1 + s$, то наше утверждение доказано (см. сноску 3).

и если $(K_\mu)_{S_1} = K_\nu$, то

$$E_{K_\mu QS} = E_{K_\mu S_1 Q_1} = (K_\mu)_{S_1 Q_1} = ((K_\mu)_{S_1})_{Q_1} = (K_\nu)_{Q_1} = K_\nu Q_1. \quad (13)$$

Из трех соотношений (11), (12) и (13) следует, что выражение $(\mathfrak{K}Q)_S$ может быть заменено на $\mathfrak{K}Q_S$.

3. Критерий импримитивности группы $\mathfrak{G}$

Комплекс

$$\mathfrak{K} = K_1 + K_2 + \cdots + K_m \quad (14)$$

из элементов группы $\mathfrak{H}$ называется *вырожденным* (singulär), если элеметы K_μ порождают подгруппу, отличную от E и $\mathfrak{H}$.

Справедливо следующее утверждение:

Пусть $\mathfrak{G}$ – группа перестановок степени n, содержащая регулярную подгруппу $\mathfrak{H}$ той же степени. Тогда группа $\mathfrak{G}$ импримитивна в том и только в том случае, если найдется вырожденный главный комплекс группы $\mathfrak{H}$ (относительно $\mathfrak{G}$).

Если $\mathfrak{G}$ импримитивна и задана некоторая система импримитивности на n элементах $\mathfrak{H}$ (рассматриваемых как переставляемые символы), то блок, содержащий единичный элемет E, совпадающий с комплексом (14), обладает следующими свойствами:

(1) $1 < m < n$ и один из K_μ равен E.

(2) для некоторой перестановки S из $\mathfrak{G}$ комплекс

$$\mathfrak{K} = (K_1)_S + (K_2)_S + \cdots + (K_m)_S$$

содержит по крайней мере один общий элемент с $\mathfrak{K}$ и потому

$$\mathfrak{K}_S = \mathfrak{K}. \quad (15)$$

Поскольку для каждой перестановки S из подгруппы $\mathfrak{G}_1$ выполнено равенство $E_S = E$, утверждение (15) следует. Согласно последнему утверждению предыдущего параграфа $\mathfrak{K}$ является главным комплексом. Кроме того, для каждого элемента K_μ из $\mathfrak{K}$ имеем

$$E_{K_\mu} = K_\mu, \quad \text{откуда} \quad \mathfrak{K}_{K_\mu} = \mathfrak{K}.$$

С другой стороны, из (5) и (10) получаем

$$\mathfrak{K}_{K_\mu} = \mathfrak{K}K_\mu.$$

Следовательно, для каждого μ

$$\mathfrak{R}K_\mu = \mathfrak{R}.$$

Это означает, что комплекс $\mathfrak{R}$ обладает групповым свойством[5]. Поскольку также $1 < m < n$, то этот главный комплекс – вырожденный.

Обратно, пусть $\mathfrak{R}$ – некоторый главный комплекс, элементы которого порождают подгруппу $\mathfrak{U}$ группы $\mathfrak{H}$, отличную от E и $\mathfrak{H}$. Тогда утверждение В из §2 влечет, что $\mathfrak{R}^2$, $\mathfrak{R}^3$, ... – также главные комплексы. Для достаточно большого a степень $\mathfrak{R}^a$ станет равной $\mathfrak{U}$[6], так что можно считать, что сам $\mathfrak{R}$ является подгруппой в $\mathfrak{H}$. Для главного комплекса $\mathfrak{R}$, удовлетворяющего равенству (10), очевидно, что элементы каждого из n/m классов смежности по $\mathfrak{R}$ переводятся любой перестановкой S из $\mathfrak{G}$ в элементы другого класса смежности. Это дает разложение множества из n переставляемых символов в систему импримитивности из n/m блоков, то есть группа $\mathfrak{G}$ импримитивна.

4. Общий случай абелевой группы $\mathfrak{H}$

Следующее утверждение имеет важное значение для нас.

(A) Пусть снова $\mathfrak{H}$ – регулярная группа перестановок степени n, содержащаяся в группе $\mathfrak{G}$ той же степени. Если $\mathfrak{H}$ – абелева группа, то главный комплекс $\mathfrak{R}$ над $\mathfrak{G}$ обладает тем свойством, что для каждого взаимно простого с n числа h наряду с

$$\mathfrak{R} = K_1 + K_2 + \cdots + K_m$$

также и

$$\mathfrak{R}^{(h)} = K_1^h + K_2^h + \cdots + K_m^h$$

является главным комплексом.

Доказательство проводится следующим образом.

1. Очевидно, что

$$\mathfrak{R}^{(h)} = \mathfrak{R}^{(h+n)} = \mathfrak{R}^{(h+2n)} = \cdots,$$

[5] Это утверждение отнюдь не ново, ему соответствует известное свойство импримитивной системы регулярной группы перестановок.

[6] Здесь необходимо оперировать с комплексами по правилам фробениусовского исчисления (Frobeniusschen Komplexkalküls).

поскольку h по предположению является положительным целым числом.

2. Если утверждение верно для каждого главного комплекса и для каждого не делящего n простого числа $h = p$, то оно также выполнено и для каждого положительного целого числа h взаимно простого с n. Действительно, если h является произведением l простых чисел $p, p', p'', \dots$, то из главного комплекса $\mathfrak{K}$ получаются главные комплексы

$$\mathfrak{L} = \mathfrak{K}^{(p)}, \quad \mathfrak{L}^{(p')} = \mathfrak{K}^{(pp')}, \ \dots .$$

Так последовательно получается $\mathfrak{K}^{(h)}$.

3. Если $h = p$ – простое число, рассмотрим целочисленную матрицу

$$V = K_1^* + K_2^* + \dots + K_m^*,$$

принадлежащую матричному кольцу $\mathfrak{B}$. Тогда и матрица

$$V^p = (a_{PQ^{-1}}) \tag{16}$$

содержится в $\mathfrak{B}$. Поскольку для абелевой группы $\mathfrak{H}$ матрицы K_μ^* в силу (7) также попарно перестановочны, то принимая во внимание, что

$$V^p \equiv \sum_\mu (K_\mu^*)^p = \sum_\mu (K_\mu^p)^* = V^{(p)} \pmod p,$$

мы заключаем, что при n взаимно простом с p все m элементов K_μ^p попарно различны и, значит, матрица $V^{(p)}$ получается из (16) заменой каждого целого числа $a_{PQ^{-1}}$ наименьшим положительным остатком по $\bmod p$. Теперь из утверждения (C) параграфа 1 следует, что $V^{(p)}$ содержится в кольце $\mathfrak{B}$. Это в точности означает, что $\mathfrak{K}^{(p)}$ является главным комплексом.

К этому добавим:

(B) Для каждого числа h взаимно простого с n простой комплекс $\mathfrak{K}$ абелевой группы $\mathfrak{H}$ переходит также в простой комплекс $\mathfrak{K}^{(p)}$.

Действительно, если целое число h' удовлетворяет равенству

$$hh' \equiv 1 \pmod n$$

и $\mathfrak{K}^{(h)} = \mathfrak{L}$, то $\mathfrak{L}^{(h')} = \mathfrak{K}$. Если теперь $\mathfrak{L}$ представляется в виде суммы двух главных комплексов, то аналогичное разложение получается и для $\mathfrak{R}$. Однако, для простого комплекса $\mathfrak{R}$ это невозможно.

Предполагая, что число h не является взаимно простым с n, получаем, очевидно, что комплекс $\mathfrak{R}^{(h)}$, не все элементы которого равны единичному элементу E, является вырожденным. Если, в частности, h является степенью простого числа p^ν, делящего n, то для матрицы V, соответствующей $\mathfrak{R}$, получаем сравнение

$$V^{p^\nu} \equiv \sum_\mu (K_\mu^{p^\nu})^* \pmod{p}.$$

Объединяя это с критерием из §3 и вышеупомянутым утверждением (C) из §1, получаем:

(C) Если $\mathfrak{H}$ – абелева группа и $\mathfrak{G}$ – примитивная группа, то каждый простой комплекс $\mathfrak{R}$ группы $\mathfrak{H}$ обладает следующим свойством: для каждой степени простого числа p^ν, делящего n, и каждого отличного от E элемента R из H число различных элементов K_μ из $\mathfrak{R}$, для которых справедливо равенство $K_\mu^{p^\nu} = R$, делится на p.

5. Рациональные главные комплексы абелевых групп

Если h пробегает $\varphi(n)$ чисел среди $1, 2, \dots, n$ взаимно простых с n, то главный комплекс $\mathfrak{R}$ нашей абелевой группы $\mathfrak{H}$ может обладать тем свойством, что $\mathfrak{R}^{(h)} = \mathfrak{R}$. В этом случае я называю $\mathfrak{R}$ *рациональным* главным комплексом.

Если это не так, то найдутся некоторые $e < \varphi(n)$ чисел

$$h_1, h_2, \dots, h_e,$$

для которых $\mathfrak{R}^{(h_w)} = \mathfrak{R}$. Эти числа, очевидно, образуют (мультипликативную) группу по модулю n. Если

$$f = \varphi(n)/e,$$

то среди $\varphi(n)$ комплексов $\mathfrak{R}^{(h)}$ найдется в точности f попарно различных комплексов

$$\mathfrak{R}^{(a_1)}, \mathfrak{R}^{(a_2)}, \dots, \mathfrak{R}^{(a_f)}. \tag{17}$$

Сумму

$$\mathfrak{S} = \mathfrak{R}^{(a_1)} + \mathfrak{R}^{(a_2)} + \dots + \mathfrak{R}^{(a_f)},$$

которая является здесь рациональным главным комплексом, я называю *следом* $\mathfrak{R}$. Если $\mathfrak{R}$ является простым комплексом, то и f комплексов (17) являются простыми. Поскольку эти комплексы должны быть попарно различными, то никакие два из них не содержат общего элемента. След $\mathfrak{S}$ комплекса $\mathfrak{R}$ является неразложимым в том смысле, что не может быть представлен в виде суммы двух рациональных главных комплексов. Обратно, очевидно, что каждый неразложимый рациональный главный комплекс возникает как след некоторого простого комплекса.

Количество попарно различных неразложимых рациональных главных комплексов я обозначаю через s. Поскольку, в частности, единичный элемент представляет целый комплекс, то

$$2 \leqslant s \leqslant r.$$

Если $s = 2$, то отличный от E неразложимый рациональный главный комплекс равен сумме $\mathfrak{M}$ отличных от E $n-1$ элементов группы $\mathfrak{H}$.

Это дает, таким образом, следующее утверждение.

(A) Если $\mathfrak{H}$ – (регулярная) абелева группа, степень которой не является степенью простого числа, то группа $\mathfrak{G}$ дважды транзитивна в том и только в том случае, когда $s = 2$.

Очевидно, достаточно заметить, что при сделанном предположении об n из $s = 2$ следует $r = 2$. Это получается следующим образом.

1. Пусть $\mathfrak{U}$ – отличная от E и $\mathfrak{H}$ подгруппа группы $\mathfrak{H}$. Поскольку $s = 2$, то каждый простой комплекс $\mathfrak{R}$, отличный от E, содержит элемент группы $\mathfrak{U}$. Если бы это было не так, то некоторый элемент группы $\mathfrak{U}$ не содержится ни в каком комплексе $\mathfrak{R}^{(h)}$ при $(h, n) = 1$. Тогда он не содержится и в следе $\mathfrak{S}$ комплекса $\mathfrak{R}$. Но тогда в $\mathfrak{S}$ нашелся бы неразложимый комплекс, отличный от E и $\mathfrak{M}$. Это противоречит предположению $s = 2$.

2. Если d – делитель n, то под $\mathfrak{H}^{(d)}$ будем понимать подгруппу группы $\mathfrak{H}$, содержащую все элементы $\mathfrak{R}$, такие, что $R^d = E$. Пусть $n = ab$ – разложение числа n на взаимно простые множители; рассмотрим подгруппы $\mathfrak{H}^{(a)}$ и $\mathfrak{H}^{(b)}$ группы $\mathfrak{H}$. Группа $\mathfrak{H}^{(a)}$ обладает следующим свойством: если

$$h' \equiv 1 \pmod{a}, \tag{18}$$

то для каждого элемента A этой группы имеем $A^{h'} = A$. Аналогичное свойство выполнено для $\mathfrak{H}^{(b)}$ относительно сравнения

$$h'' \equiv 1 \pmod{b}. \tag{19}$$

Если $s = 2$, то по утверждению 1 каждый простой комплекс $\mathfrak{R}$ группы $\mathfrak{H}$ содержит отличные от E элементы A из $\mathfrak{H}^{(a)}$ и B из $\mathfrak{H}^{(b)}$. Если теперь h' – взаимно простое с n число, для которого выполнено (18), то простой комплекс $\mathfrak{R}^{h'}$ содержит общий с $\mathfrak{R}$ элемент A и потому равен $\mathfrak{R}$. Аналогично для каждого взаимно простого с n числа h'', для которого выполнено (19), имеем $\mathfrak{R}^{(h'')} = \mathfrak{R}$. Отсюда получается, что $\mathfrak{R}^{(h'h'')} = \mathfrak{R}$. Произведение $h'h''$ при этом пробегает каждое взаимно простое с n число. Это означает, что при $s = 2$ каждый простой комплекс должен быть рациональным. Следовательно, $r = s = 2$.

Также получается, что если все элементы комплекса $\mathfrak{R}$ принадлежат некоторой подгруппе $\mathfrak{U}$ группы $\mathfrak{H}$, то это будет выполнено и для каждого комплекса $\mathfrak{R}^{(h)}$. В нашей терминологии это означает, что главный комплекс является вырожденным тогда и только тогда, когда его след является таковым. Вместе с критерием из §3 это дает:

(B) Если $\mathfrak{H}$ – абелева группа, то группа $\mathfrak{G}$ импримитивна тогда и только тогда, когда среди рациональных главных комплексов найдется вырожденный.

Таким образом, вопрос состоит в том, чтобы исследовать множество групп перестановок $\mathfrak{G}$ степени n, содержащих регулярную абелеву подгруппу $\mathfrak{H}$ той же степени и не являющихся ни дважды транзитивными, ни импримитивными, ограничиваясь, в случае n, не являющимся степенью простого, изучением рациональных главных комплексов группы $\mathfrak{H}$. При этом отметим, что совокупность этих комплексов очевидно образует кольцо.

6. Класс групп перестановок с регулярной подгруппой

Пусть

$$\mathfrak{H} = H_1 + H_2 + \cdots + H_n$$

– произвольная регулярная группа перестановок. Все n элементов группы $\mathfrak{H}$ будем рассматривать как переставляемые символы и запишем это как

$$H_\nu = \begin{pmatrix} P \\ PH_\nu \end{pmatrix}, \quad (P = H_1, H_2, \ldots, H_n).$$

Имеется другая группа перестановок $\mathfrak{U}$ на том же самом множестве символов, состоящая из всех автоморфизмов группы $\mathfrak{H}$, и автоморфизм A, переводящий H_ν в H'_ν, задает перестановку

$$A = \begin{pmatrix} P \\ P' \end{pmatrix}.$$

Мы записываем это также как $P' = P_A$. Все эти перестановки оставляют на месте единичный элемент E. Порядок группы $\mathfrak{U}$ обозначим через a.

Единственным общим элеметом групп $\mathfrak{H}$ и $\mathfrak{U}$ является тождественная перестановка и, кроме того, $\mathfrak{U}\mathfrak{H} = \mathfrak{H}\mathfrak{U}$. Поэтому группа

$$\mathfrak{F} = \mathfrak{U}\mathfrak{H}$$

имеет порядок an. Эта группа названа Бернсайдом в [2, S. 85] *голоморфом* группы H.

В $\mathfrak{F}$ подгруппа $\mathfrak{U}$ играет роль $\mathfrak{F}_1$, т.е. совокупности всех перестановок из $\mathfrak{F}$, оставляющих на месте единичный элемент E. Два элемента P и Q из $\mathfrak{H}$ принадлежат одному из r простых комплексов $\mathfrak{R}_\rho$, на которые разлагается регулярная подгруппа $\mathfrak{H}$ группы $\mathfrak{F}$, тогда и только тогда, когда найдется автоморфизм A группы $\mathfrak{H}$, переводящий P в Q. Отсюда следует, что

a) Все элементы простого комплекса $\mathfrak{R}$ имеют один и тот же порядок.

b) Если некоторый элемент из $\mathfrak{R}$ является инвариантным элементом $\mathfrak{H}$, то это верно и для всех элементов из $\mathfrak{R}$.

c) Если K – некоторый элемент из $\mathfrak{R}$, то $\mathfrak{R}$ содержит все элементы из $\mathfrak{H}$, подобные K[7]. Поэтому все элементы из $\mathfrak{R}$ порождают инвариантную подгруппу группы $\mathfrak{H}$.

Если теперь группа $\mathfrak{F}$ дважды транзитивна, то есть $r = 2$, то из a) следует, что все отличные от E элементы группы $\mathfrak{H}$ имеют один и тот же порядок p. При этом p должно быть простым числом, а n – степенью p. Из b) следует, что $\mathfrak{H}$ должна быть абелевой группой типа $(p, p, \ldots)$. Такая группа была названа Фробениусом *элементарной* абелевой группой. В этом случае ясно, что для каждой пары отличных от E элементов P и Q из $\mathfrak{H}$ в самом деле имеется автоморфизм, переводящий P в Q. Отсюда получается известное утверждение, что голоморф $\mathfrak{F}$ группы $\mathfrak{H}$

[7] Это следует из рассмотрения внутренних автоморфизмов группы $\mathfrak{H}$.

дважды транзитивен тогда и только тогда, когда $\mathfrak{H}$ – элементарная абелева группа.

Как пример группы $\mathfrak{G}$ с регулярной подгруппой $\mathfrak{H}$, которая не является ни дважды транзитивной, ни импримитивной, рассмотрим в качестве $\mathfrak{G}$ голоморф $\mathfrak{F}$ простой группы $\mathfrak{H}$ составного порядка. По свойству с) простого комплекса, ни один главный комплекс группы $\mathfrak{H}$ не может быть вырожденным. Поэтому критерий из §3 влечет, что для простой группы $\mathfrak{H}$ голоморф $\mathfrak{F}$ является примитивным, но не дважды транзитивным.

Напротив, из утверждения а) для простых комплексов подгруппы $\mathfrak{H}$, вложенной в собственный голоморф, следует, что ни для какой элементарной абелевой группы $\mathfrak{H}$ группа $\mathfrak{F}$ не может быть импримитивной.

Теперь я перейду к опровержению предположения Бернсайда о регулярных абелевых группах.

Выберем в качестве $\mathfrak{H}$ элементарную абелеву группу порядка $n = p^\nu$, где p – нечетное простое число и $\nu > 1$. Пусть, кроме того, d – отличный от 1 делитель $p-1$. Сравнение

$$x^d \equiv 1 \pmod p$$

имеет в точности d решений

$$a_1, a_2, \ldots, a_d \tag{20}$$

в множестве целых чисел $1, 2, \ldots, p-1$. Под $\mathfrak{T}$ будем понимать произвольную транзитивную группу перестановок на ν символах $1, 2, \ldots, \nu$. Порядок $\mathfrak{T}$ пусть будет t.

Выберем элементы

$$R_1, R_2, \ldots, R_\nu \tag{21}$$

в качестве базиса группы $\mathfrak{H}$ и положим $b = td^\nu$. Тогда перестановка B

$$R'_\alpha = (R_\alpha)_B = R_{\alpha'}^{x_\alpha} \quad (\alpha = 1, 2, \ldots, \nu) \tag{22}$$

должна быть автоморфизмом группы $\mathfrak{H}$, где $\binom{\alpha}{\alpha'}$ есть перестановка из $\mathfrak{T}$ и x_α – одно из чисел (20). Эти автоморфизмы образуют подгруппу $\mathfrak{B}$ группы автоморфизмов $\mathfrak{U}$. Голоморф $\mathfrak{F}$ группы $\mathfrak{H}$ содержит подгруппу

$$\mathfrak{G} = \mathfrak{H}\mathfrak{B}$$

порядка bn. Она содержит нашу регулярную подгруппу $\mathfrak{H}$.

Я утверждаю, что *группа $\mathfrak{G}$ примитивна, но не дважды транзитивна.*

Чтобы это увидеть, примем во внимание следующее.

1. Совокупность $\mathfrak{G}_1$ перестановок из $\mathfrak{G}$, оставляющих на месте элемент E из $\mathfrak{H}$, в этом случае совпадает с подгруппой $\mathfrak{B}$ группы $\mathfrak{G}$. Отсюда следует, что для любого из r простых комплексов $\mathfrak{R}_\rho$ группы $\mathfrak{H}$ два отличных от E элемента P и Q из $\mathfrak{H}$ принадлежат комплексу $\mathfrak{R}_\rho$ в том и только в том случае, если найдется такой автоморфизм B из $\mathfrak{B}$, что $P_B = Q$.

2. Отсюда, в частности, следует, что

$$\mathfrak{R} = \sum_{\alpha=1}^{\nu}(R_\alpha^{a_1} + R_\alpha^{a_2} + \cdots + R_\alpha^{a_\alpha})$$

является простым комплексом. Он не содержит, например, элемент R_1R_2. Следовательно, $r > 2$. Таким образом, группа $\mathfrak{G}$ не является дважды транзитивной.

3. Для любого главного комплекса $\mathfrak{R}$ обозначим через $\mathfrak{L}$ подгруппу группы $\mathfrak{H}$, порожденную элементами из $\mathfrak{R}$. Исключим случай $\mathfrak{R} = E$. Если

$$R = R_1^{z_1}R_2^{z_2}\cdots R_\nu^{z_\nu} \quad (z_\alpha = 0, 1, \ldots, p-1)$$

является элементом из $\mathfrak{R}$, отличным от E, то не для всех ν число z_α может быть нулем. Пусть $z_1 > 0$. Выберем автоморфизм B так, чтобы

$$R_1' = R_1^{x_1},\ R_2' = R_2, \ldots, R_\nu' = R_\nu \quad (x_1 \neq 1),$$

и тогда

$$R' = R_B = R_1^{x_1z_1}R_2^{z_2}\cdots R_\nu^{z_\nu}.$$

Этот элемент принадлежит $\mathfrak{R}$, и потому группа $\mathfrak{L}$ содержит элемент

$$R'R^{-1} = R_1^{(x_1-1)z_1}.$$

Поскольку показатель не делится на p, то и R_1 принадлежит $\mathfrak{L}$.

С другой стороны, в силу транзитивности группы $\mathfrak{T}$ для каждого индекса α из множества $1, 2, \ldots, \nu$ можно выбрать автоморфизм

$$C = \begin{pmatrix} P \\ P'' \end{pmatrix}$$

так, чтобы
$$R_1'' = R_\alpha, R_2'' = R_\beta, \ldots, R_\nu'' = R_\lambda.$$

Тогда комплекс $\mathfrak{R}$ содержит элемент
$$R'' = R_\alpha^{z_1} R_\beta^{z_2} \cdots R_\lambda^{z_\nu}.$$

Как и раньше, отсюда получаем, что R_α принадлежит группе $\mathfrak{L}$.

Это показывает, что группа $\mathfrak{L}$ содержит все базисные элементы (21) и потому $\mathfrak{L} = \mathfrak{H}$. Следовательно, нет вырожденных главных комплексов. Поэтому согласно §3 наша группа $\mathfrak{G}$ является примитивной[8].

Простейший пример получается для
$$p = 3,\ d = 2,\ t = 2.$$

Это группа порядка 72 и степени 9.

7. Циклическая группа $\mathfrak{H}$. Случай Бернсайда $n = p^a$

Мы подошли к нашей главной задаче. Пусть $\mathfrak{G}$ – группа перестановок степени n, содержащая цикл P порядка n. Здесь n не является простым числом. Чтобы доказать сформулированное во введении утверждение (III), мы предположим, что группа $\mathfrak{G}$ примитивна, но не дважды транзитивна и попытаемся найти противоречие.

Обозначим через $\mathfrak{H}$ регулярную группу, порожденную циклом P, и разложим $n-1$ отличных от E элементов из $\mathfrak{H}$ в $r-1$ простых комплексов $\mathfrak{R}_\rho$. Каждый из них имеет вид
$$\mathfrak{R} = P^{\lambda_1} + P^{\lambda_2} + \cdots + P^{\lambda_m} \quad (\lambda_\mu = 1, 2, \ldots, n-1). \qquad (23)$$

Сделанные предположения о группе $\mathfrak{G}$ означают в силу результатов §§2 и 3 следующее:

a) $m < n-1$;

b) наибольший общий делитель чисел
$$\lambda_1, \lambda_2, \ldots, \lambda_m, n$$

равен 1.

---

[8]Доказательство того, что построенная здесь группа $\mathfrak{G}$ примитивна, но не дважды транзитивна, можно провести и без использования введенных нами понятий.

Рассмотрим теперь простые комплексы $\mathfrak{K}$ как матрицы V кольца $\mathfrak{B}$. Обозначим через Q матрицу P^*, как в §2, так что Q^n есть первая степень Q, совпадающая с единичной матрицей E. Тогда каждая матрица V имеет вид

$$V = c_0 E + c_1 Q + c_2 Q_2 + \cdots + c_{n-1} Q^{n-1}.$$

Если среди $c_1, c_2, \ldots, c_{n-1}$ коэффициенты

$$c_{\mu_1}, c_{\mu_2}, \ldots, c_{\mu_k}$$

отличны от нуля, то мы также должны иметь

$$(\mu_1, \mu_2, \ldots, \mu_k, n) = 1. \tag{24}$$

В противном случае комплекс

$$P^{\mu_1} + P^{\mu_2} + \cdots + P^{\mu_k}$$

содержится в вырожденном комплексе, что невозможно. Матрицу V, для которой (24) не выполнено, будем для краткости называть *вырожденной матрицей*.

Чтобы наш метод доказательства сделать понятным, я хочу прежде всего разобрать другим способом случай Бернсайда для степени простого $n = p^a$ (с $a > 1$). Мы пойдем к цели шаг за шагом.

1. Пусть (23) – отличный от E простой комплекс группы $\mathfrak{H}$. Мы знаем, что по крайней мере один из m показателей λ_μ не делится на p. Поэтому, я утверждаю следующее: среди m чисел (λ_μ, p^a) должны встретиться все степени $p^0, p, p^2, \ldots, p^{a-1}$. Действительно (ср. §5), след $\mathfrak{S}$ комплекса $\mathfrak{K}$ содержит все $\varphi(p^a)$ степеней P^x с $(x, p) = 1$ и потому все отличные от E элементы из $\mathfrak{H}$. В противном случае совокупность всех степеней P, не входящих в $\mathfrak{S}$, образовывала бы вырожденный главный комплекс, что невозможно. Таким образом, имеем

$$\mathfrak{S} = \mathfrak{M} = P + P^2 + \cdots + P^{n-1}. \tag{25}$$

2. Рассмотрим множество всех взаимно простых с p чисел

$$h_1, h_2, \ldots, h_k \tag{26}$$

из ряда $1, 2, \ldots, p^a - 1$, для которых в обозначениях §5 выполнено

$$\mathfrak{K}^{(h_\chi)} = \mathfrak{K} \quad (\chi = 1, 2, \ldots, k).$$

Все k чисел из (26) образуют группу $\mathfrak{N}$ по модулю p^a, и из (25) получаем

$$m\varphi(p^a) = k(p^a - 1). \tag{27}$$

Теперь из 1. следует, что $\mathfrak{R}$ содержит элемент R вида $P^{p^{a-1}u}$ и для каждого числа

$$h = 1 + xp \quad (x = 0, 1, \ldots, p^{a-1}) \tag{28}$$

выполнено $R^h = R$, и потому $\mathfrak{R}^{(h)} = \mathfrak{R}$. Последнее верно, поскольку эти комплексы простые и имеют общий элемент R. Все p^{a-1} чисел (28) образуют подгруппу группы $\mathfrak{N}$. Поэтому

$$k = p^{a-1}f,$$

откуда, поскольку $k|\varphi(p^a)$, число f должно быть делителем $p-1$. Для $p = 2$ это дает $f = 1$, $k = p^{a-1} = \varphi(p^a)$. Тогда из (27) имеем $m = p^a - 1$, что невозможно. Поэтому можно считать, что $p > 2$. Предположение $f = p - 1$ приводит к противоречию, ибо тогда опять $m = p^a - 1$, и потому

$$2 \leqslant 2f \leqslant p - 1. \tag{29}$$

3. Беря все k чисел из (26) по модулю p, получаем f целых различных остатков

$$r_1, r_2, \ldots, r_f \quad (r_i = 1, 2, \ldots, p-1),$$

которые образуют группу по модулю p. Тогда числа (26) выражаются следующим образом:

$$r_i + pz \quad (i = 1, 2, \ldots, f,\ z = 0, 1, \ldots, p^a - 1).$$

Полагая для $\alpha = 1, 2, \ldots, a-1$

$$\mathfrak{U}_\alpha = E + P^{p^\alpha} + P^{2p^\alpha} + \cdots + P^{p^a - p^\alpha}, \tag{30}$$

получаем, что $\mathfrak{R}$ имеет вид

$$\mathfrak{R} = \mathfrak{U}_1\mathfrak{B}_0 + \mathfrak{U}_2\mathfrak{B}_1 + \cdots + \mathfrak{U}_{a-1}\mathfrak{B}_{a-2} + \mathfrak{B}_{a-1},$$

где $\mathfrak{B}_\beta$ есть

$$\mathfrak{B}_\beta = P^{p^\beta r_1 b_\beta} + \cdots + P^{p^\beta r_f b_\beta} \quad (\beta = 0, 1, \ldots, a-1) \tag{31}$$

с числами b_β, сравнимыми с единицей по модулю p.

4. Я рассмотрю теперь матрицу V кольца $\mathfrak{B}$, соответствующую $\mathfrak{R}$. Записывая аналог формул (30) и (31)

$$A_\alpha = E + Q^{p^\alpha} + Q^{2p^\alpha} + \cdots + Q^{p^a - p^\alpha},$$

$$B_\beta = Q^{p^\beta r_1 b_\beta} + \cdots + Q^{p^\beta r_f b_\beta},$$

имеем

$$V = A_1 B_0 + A_2 B_1 + \cdots + A_{a-1} B_{a-2} + B_{a-1}. \tag{32}$$

Заметим, что для $\chi \leqslant \lambda$ и $\chi \leqslant \mu$ имеют место соотношения

$$A_\chi A_\lambda = p^{a-\lambda} A_\chi, \quad A_\chi B_\mu = f A_\chi.$$

Используя (32), вычислим квадрат целочисленной матрицы V; приводя результат по модулю p, имеем

$$V^2 \equiv 2fA_1 B_0 + 2fA_2 B_1 + \cdots + 2fA_{a-1} B_{a-2} + B_{a-1}^2 \pmod p,$$

откуда

$$V_1 = V^2 - 2fV \equiv B_{a-1}^2 - 2fB_{a-1} \pmod p. \tag{33}$$

Полагая

$$Q^{p^{a-1} b_{a-1}} = R,$$

разложим эту матрицу в виде

$$B_{a-1}^2 - 2fB_{a-1} = d_0 E + d_1 R + d_2 R^2 + \cdots + d_{p-1} R^{p-1}.$$

Здесь все числа $d_1, d_2, \ldots, d_{p-1}$ должны одновременно делиться на p. В противном случае, если δ_i – наименьший положительный остаток для d_i по модулю p, то в силу сравнения (33) и утверждения (C) из §1 матрица

$$V_2 = \delta_1 R + \delta_2 R^2 + \cdots + \delta_{p-1} R^{p-1}$$

принадлежит кольцу $\mathfrak{B}$. Но этого не может быть, поскольку это, очевидно, вырожденная матрица этого кольца.

Числа $d_1, d_2, \ldots, d_{p-1}$ не могут иметь требуемого свойства. Если

$$B_{a-1}^2 = c_0 E + c_1 R + \cdots + c_{p-1} R^{p-1},$$

то, поскольку все коэффициенты здесь неотрицательные целые числа, получаем равенство

$$c_0 + c_1 + \cdots + c_{p-1} = f^2. \tag{34}$$

Поскольку B_{a-1}^2[9] остается на месте под действием f подстановок $R \to R^{r_\lambda}$, мы имеем

$$c_{r_1} = c_{r_2} = \cdots = c_{r_f}.$$

Отсюда следует, что эти числа в силу (34) не превосходят f. Для $i = r_1, r_2, \ldots, r_f$ это влечет, что число

$$d_i = c_i - 2f$$

является целым числом между $-2f$ и $-f$. В силу (29) это означает, что числа d_i не могут делиться на p.

8. Общий случай циклической группы $\mathfrak{H}$

Рассмотрим теперь число

$$n = p^a q^b r^c \cdots$$

с по крайней мере двумя различными простыми делителями $p, q, r, \cdots$. Из результатов §5 следует, что можно ограничиться изучением рациональных главных комплексов группы $\mathfrak{G}$ над нашей циклической группой $\mathfrak{H} = \{P\}$. Поскольку $\mathfrak{G}$ примитивна, но не дважды транзитивна, группа $\mathfrak{H}$ разлагается в $s > 2$ неразложимых рациональных главных комплексов

$$\mathfrak{L}_1, \mathfrak{L}_2, \ldots, \mathfrak{L}_s, \tag{35}$$

среди которых не имеется вырожденных. Мы хотим доказать, что такое разложение в нашем случае невозможно. Доказательство разделим на последовательность шагов.

1. Для каждого делителя d числа n обозначим через $\mathfrak{F}_d$ сумму из $\varphi(n/d)$ степеней P^{dx} с

[9] В оригинале R_{a-1}^2. – *Прим. перев.*

$$x = 0, 1, \ldots, n/d - 1, \quad (x, d) = 1,^{10}$$

так, что каждый отличный от E комплекс $\mathfrak{L}_\sigma$ имеет вид

$$\mathfrak{L}_\sigma = \mathfrak{F}_{d_1} + \mathfrak{F}_{d_2} + \cdots,$$

где $d_1, d_2, \ldots$ являются попарно различными делителями n, отличными от n и удовлетворяющими равенству

$$(d_1, d_2, \ldots) = 1.$$

Чтобы лучше понять поведение произведения $\mathfrak{F}_d \mathfrak{F}_t$, сделаем следующее. Рассмотрим порожденные элементами

$$A = P^{n/p^a}, \quad B = P^{n/q^b}, \quad C = P^{n/r^c}, \ldots$$

циклические подгруппы

$$\mathfrak{A}, \ \mathfrak{B}, \ \mathfrak{C}, \ldots$$

порядков $p^a, q^b, r^c, \ldots$. Тогда группа

$$\mathfrak{H} = \mathfrak{A}\mathfrak{B}\mathfrak{C} \cdots$$

является прямым произведением. Положим для $\alpha = 0, 1, \ldots, a$

$$\mathfrak{A}_\alpha = \sum A^{p^\alpha x} \quad (x = 0, 1, \ldots, p^{a-\alpha} - 1, \ (x, p) = 1)$$

и определим $\mathfrak{B}_\beta, \mathfrak{C}_\gamma, \ldots$ аналогичным образом. В частности, определенные так $\mathfrak{A}_a, \mathfrak{B}_b, \mathfrak{C}_c, \ldots$ приводят к единичному элементу E.

Если теперь

$$d = p^\alpha q^\beta r^\gamma \cdots$$

является делителем n, то, очевидно, имеем

$$\mathfrak{F}_d = A_\alpha \mathfrak{B}_\beta \mathfrak{C}_\gamma, \ldots.$$

2. Среди s комплексов (35) положим $\mathfrak{L}_s = E$ и обозначим через $\mathfrak{L}_1$ тот комплекс, в котором содержится

$$\mathfrak{F}_{n/p} = \mathfrak{A}_{a-1} \mathfrak{B}_b \mathfrak{C}_c \ldots.$$

Я построю новые комплексы

$$\mathfrak{M}_1 = \mathfrak{L}_1 + E, \ \mathfrak{M}_2 = \mathfrak{L}_2, \ \ldots, \ \mathfrak{M}_{s-1} = \mathfrak{L}_{s-1},$$

[10] В оригинале $(x, p) = 1$. – *Прим. перев.*

сумма которых также равна $\mathfrak{H}$. Обозначая через $\mathfrak{R}$ подгруппу

$$\mathfrak{R} = \mathfrak{B}\mathfrak{C}\dots,$$

запишем каждый $\mathfrak{M}_\sigma$ в виде

$$\mathfrak{M}_\sigma = \mathfrak{A}_0\mathfrak{R}_0 + \mathfrak{A}_1\mathfrak{R}_1 + \dots + \mathfrak{A}_{a-1}\mathfrak{R}_{a-1} + \mathfrak{A}_a\mathfrak{R}_a,$$

где каждый $\mathfrak{R}_\alpha$ является либо рациональным комплексом на $\mathfrak{R}$, либо равен 0 (т.е. пуст). Эти комплексы могут иметь общие элементы; кроме того, $\mathfrak{R}_0$ отличен от нуля, поскольку $\mathfrak{M}_\sigma$ невырожден, и $\mathfrak{R}_a$ содержит элемент E только при $\sigma = 1$.

Я утверждаю, что для каждого σ

$$\mathfrak{R}_{a-1} = \mathfrak{R}_a. \tag{36}$$

Мы воспользуемся утверждением (C) из §4. Предположим, что $\mathfrak{M}_\sigma$ содержит m элементов

$$M_1, M_2, \dots, M_m$$

из $\mathfrak{H}$ и рассмотрим

$$M_1^p, M_2^p, \dots, M_m^p. \tag{37}$$

Очевидно, в каждом произведении $\mathfrak{A}_\alpha\mathfrak{R}_\alpha$ элементы из $\mathfrak{A}_\alpha$ и $\mathfrak{R}_\alpha$ заменяются на p-е степени. При этом $\mathfrak{R}_\alpha$ не изменяется, поскольку порядки элементов из $\mathfrak{R}$ взаимно просты с p и комплекс $\mathfrak{R}_\alpha$ либо равен 0, либо рационален. Напротив, $\mathfrak{A}_\alpha$ ведет себя следуюшим образом: для $\alpha = 0, 1, \dots, a-2$ совокупности из p элементов переходят при возведении в p-ю степень в некоторый элемент из $\mathfrak{A}_{a+1}$, $p-1$ элемент из $\mathfrak{A}_{a-1}$ переходит в E и $\mathfrak{U}_a$ остается неизменным.

Если теперь равенство (36) не выполнено, то среди элементов (37) некоторый элемент R, отличный от E, появляется либо $p-1$ раз, либо один раз. Это выполняется в зависимости от того, принадлежит R к $\mathfrak{R}_{a-1}$, но не к $\mathfrak{R}_a$, или принадлежит R к $\mathfrak{R}_a$, но не к $\mathfrak{R}_{a-1}$. Это, однако, невозможно в силу примитивности группы $\mathfrak{G}$.

3. Для комплекса $\mathfrak{M}_\sigma$ определим целое число $\chi \geqslant 0$ так, чтобы

$$\mathfrak{R}_\chi = \mathfrak{R}_{\chi+1} = \dots = \mathfrak{R}_a$$

и для $\chi > 0$ также

$$\mathfrak{R}_{\chi-1} \neq \mathfrak{R}_\chi.$$

Положим

$$\mathfrak{A}'_\alpha = \mathfrak{A}_\alpha + \mathfrak{A}_{\alpha+1} + \cdots + \mathfrak{A}_a = \sum_{y=0}^{p^{a-\alpha}-1} A^{p^\alpha y},$$

так что

$$\mathfrak{M}_\sigma = \mathfrak{A}_0\mathfrak{R}_0 + \cdots + \mathfrak{A}_{\chi-1}\mathfrak{R}_{\chi-1} + \mathfrak{A}'_\chi\mathfrak{R}_\chi \quad \text{или} \quad \mathfrak{M}_\sigma = \mathfrak{A}'_0\mathfrak{R}_0$$

в зависимости от того, $\chi > 0$ или $\chi = 0$. Это число χ я называю *связывающим числом* (Verknüpfungszahl) для простого числа p. Равенство (36) показывает, что $\chi < a$. Поэтому комплекс $\mathfrak{A}'_\chi\mathfrak{R}_\chi$ во всяком случае отличен от E.

Для простого числа q построим аналогичным способом группы

$$\mathfrak{R} = \mathfrak{A}\mathfrak{C}\cdots, \quad \mathfrak{B}'_\beta = \mathfrak{B}_\beta + \mathfrak{B}_{\beta+1} + \cdots + \mathfrak{B}_b.$$

Тогда наш комплекс $\mathfrak{M}_\sigma$ можно представить в виде

$$\mathfrak{M}_\sigma = \mathfrak{B}_0\mathfrak{R}_0 + \cdots + \mathfrak{B}_{\lambda-1}\mathfrak{R}_{\lambda-1} + \mathfrak{B}'_\lambda\mathfrak{R}_\lambda,$$

где каждый $\mathfrak{R}_\beta$ обозначает либо ноль, либо рациональный комплекс с элементами из $\mathfrak{R}$. Здесь, поскольку $\lambda > 0$, комплекс $\mathfrak{R}_{\lambda-1}$ должен быть отличен от $\mathfrak{R}_\lambda$. Число λ здесь обозначает связывающее число для простого числа q. Разложение комплекса $\mathfrak{M}_\sigma$, как и в случае простого числа p, показывает, что можно считать, что $\lambda \leqslant b$.

Аналогично определим связывающие числа $\mu, \ldots$ для простых чисел $r, \ldots$.

4. Мы утверждаем, что для комплекса $\mathfrak{M}_\sigma$ должны выполняться равенства

$$\chi = 0,\ \lambda = 0,\ \mu = 0, \ldots \tag{38}$$

Если это доказать, то тогда

$$\mathfrak{M}_\sigma = \mathfrak{A}'_0\mathfrak{B}'_0\mathfrak{C}'_0\cdots = \mathfrak{A}\mathfrak{B}\mathfrak{C}\cdots = \mathfrak{H}.$$

Отсюда следует, что $s - 1 = 1$, что противоречит нашему предположению.

Примем во внимание, что равенство (38) достаточно доказать только для нечетных простых чисел. Действительно, если $q = 2$ и мы знаем, что $\chi = 0$, $\mu = 0$, $\ldots$, то рассмотрим два различных комплекса $\mathfrak{M}_\sigma$ и $\mathfrak{M}_\tau$. Во введенных обозначениях мы имеем

$$\mathfrak{M}_\sigma = (\mathfrak{B}_\beta + \mathfrak{B}_\gamma + \cdots)\mathfrak{N}, \quad \mathfrak{M}_\tau = (\mathfrak{B}_\delta + \mathfrak{B}_\epsilon + \cdots)\mathfrak{N}.$$

Поскольку ни $\mathfrak{M}_\sigma$, ни $\mathfrak{M}_\tau$ не являются вырожденными, то как среди $\beta, \gamma, \ldots$, так и среди $\delta, \epsilon, \ldots$ должен найтись индекс 0. Это приводит к противоречию, поскольку $\mathfrak{M}_\sigma$ и $\mathfrak{M}_\tau$ не могут иметь общих элементов.

5. Чтобы доказать равенство (38), мы подсчитаем кратности вхождения элементов группы $\mathfrak{H}$ в комплекс $\mathfrak{M}_\sigma^2$. Здесь будет удобно вместо комплекса $\mathfrak{M}_\sigma$ рассматривать соответствующую матрицу M_σ из кольца $\mathfrak{B}$.

Как и раньше, будем обозначать соответствующие элементам $A, B, C, \ldots$ группы $\mathfrak{H}$ матрицы $A^*, B^*, C^*, \ldots$ кольца $\mathfrak{B}$ через $F, G, H, \ldots$ и аналоги комплексов $\mathfrak{A}_\alpha$, $\mathfrak{A}'_\alpha$ суммами

$$S_\alpha = \sum F^{p^\alpha x}, \quad S'_\alpha = \sum F^{p^\alpha y} \quad (x, y = 0, 1, \ldots, p^{a-\alpha} - 1,\ (x, p) = 1),$$

так что

$$S'_\alpha = S_\alpha + S_{\alpha+1} + \cdots + S_a, \quad S'_a = S_a = E.$$

Описанным способом сопоставим степеням простых чисел q^b, $r^c, \ldots$ матрицы T_β, T'_β, U_γ, $U'_\gamma, \ldots$.

Пусть $\chi, \lambda, \mu, \ldots$ – связывающие числа комплекса $\mathfrak{M}_\sigma$, так что M_σ представляется суммой произведений матриц $S_\alpha T_\beta U_\gamma \cdots$, где

$$0 \leqslant \alpha \leqslant \chi, \quad 0 \leqslant \beta \leqslant \lambda, \quad 0 \leqslant \gamma \leqslant \mu, \quad \ldots$$

с заменой S_χ на S'_χ, а также T_λ на T'_λ и т.д. Кроме того, поскольку $\mathfrak{M}_\sigma$ не является вырожденным комплексом, необходимо также рассматривать произведения[11] вида

$$S_0 T_\beta U_\gamma \cdots,\ S_\alpha T_0 U_\gamma \cdots,\ S_\alpha T_\beta U_0 \cdots,\ \ldots$$

6. Матрицы S'_α обладают тем свойством (см. §7), что для $\alpha \leqslant \alpha_1$

$$S'_\alpha S'_{\alpha_1} = p^{a-\alpha_1} S'_\alpha.$$

Отсюда легко следует, что матрицы

$$S''_0 = S'_0,\ S''_1 = -S'_0 + pS'_1,\ \cdots,\ S''_a = -S'_{a-1} + pS'_a$$

[11] Для нас важно, что, поскольку $\chi < a$, то ни одна из матриц $S_\alpha T_\beta U_\gamma \cdots$ не равна E.

удовлетворяют соотношениям

$$S''^2_\alpha = a_\alpha S''_\alpha, \quad S''_\alpha S''_{\alpha_1} = 0 \quad (\alpha \neq \alpha_1) \tag{39}$$

с

$$\alpha_0 = \alpha_1 = p^a,\ \alpha_2 = p^{a-1},\ \alpha_3 = p^{a-2},\ \dots ,\alpha_a = p.$$

Очевидно, что вместе с каждой матрицей S'_α каждая матрица

$$S_\alpha = S'_\alpha - S'_{\alpha+1} \quad (S_{a+1} = 0)$$

представляется линейным однородным уравнением от $S''_0, S''_1, \dots,$ S''_a с рациональными коэффициентами. Мы воспользуемся, кроме того, формами

$$\begin{cases} S''_0 = S_0 + S_1 + \dots + S_{\chi-1} + S'_\chi, \\ S''_1 = -S_0 + (p-1)(S_1 + \dots + S_{\chi-1} + S'_\chi), \\ S''_2 = -S_1 + (p-1)(S_2 + \dots + S_{\chi-1} + S'_\chi), \\ S''_\chi = -S_{\chi-1} + (p-1)S'_\chi, \end{cases} \tag{40}$$

которые можно записать короче в виде

$$S''_\alpha = a_{\alpha_0}S_0 + a_{\alpha_1}S_1 + \dots + a_{\alpha_{\chi-1}}S_{\chi-1} + a_{\alpha_\chi}S'_\chi \quad (\alpha = 0, 1, \dots, \chi). \tag{41}$$

Аналогичным способом для $q^b, r^c, \dots$ определим $T''_\beta, U''_\gamma, \dots$ и числа $b_\beta, c_\gamma, \dots$. Тогда имеем

$$\begin{cases} T''_\beta = b_{\beta_0}T_0 + b_{\beta_1}T_1 + \dots + b_{\beta_{\lambda-1}}T_{\lambda-1} + b_{\beta_\lambda}T'_\lambda \quad (\beta = 0, 1, \dots, \lambda), \\ U''_\gamma = c_{\gamma_0}U_0 + c_{\gamma_1}U_1 + \dots + c_{\gamma_{\mu-1}}U_{\mu-1} + c_{\gamma_\mu}U'_\mu, \quad \text{и т.д.} \end{cases} \tag{42}$$

7. Теперь матрица M_σ представляется с помощью $S''_\alpha, T''_\beta,$ $U''_\gamma, \dots$ в виде

$$M_\sigma = \sum x_{\alpha,\beta,\gamma,\dots} S''_\alpha T''_\beta U''_\gamma, \dots \qquad (\alpha = 0, 1, \dots, \chi,\ \beta = 0, 1, \dots, \lambda,\ \dots). \tag{43}$$

Здесь коэффициенты $x_{\alpha,\beta,\gamma,\dots}$ суть рациональные числа, которые могут принимать отрицательные значения. Тогда по (39) имеем

$$M^2_\sigma = \sum x^2_{\alpha,\beta,\gamma,\dots} a_\alpha b_\beta c_\gamma \dots S''_\alpha T''_\beta U''_\gamma, \dots$$

Выражая S''_α, T''_β, $U''_\gamma, \dots$ через S_α, T_β, $U_\gamma, \dots$ с помощью формул (41) и (42), получаем выражение

$$M^2_\sigma = \sum c_{\delta\epsilon\nu\dots} S_\delta T_\epsilon U_\nu \dots \qquad (\delta = 0, 1, \dots, \chi,\ \epsilon = 0, 1, \dots, \lambda,\ \dots), \tag{44}$$

где

$$c_{\delta\epsilon\nu\ldots} = \sum x^2_{\alpha,\beta,\gamma,\ldots} a_\alpha b_\beta c_\gamma \ldots a_{\alpha_\delta} b_{\beta_\epsilon} c_{\gamma_\nu} \ldots \tag{45}$$

В (44) также $S_\chi, T_\lambda, U_\mu, \ldots$ везде заменяются на $S'_\chi, T'_\lambda, U'_\mu, \ldots$

Из уравнений (40) и их аналогов для простых чисел $q, r, \ldots$ вытекает, что $c_{\chi\lambda\mu\ldots} > 0$. Кроме того, множители, отвечающие $S'_\chi, T'_\lambda, U'_\mu, \ldots$, отличаются от единичной матрицы, поскольку $\chi < a$.

Теперь мы найдем в сумме (44) такие слагаемые, что

$$c_{\delta\epsilon\nu\ldots} = c_{\chi\lambda\mu\ldots} \tag{46}$$

Поскольку M_σ^2, как и M_σ, принадлежит матричному кольцу $\mathfrak{B}$, которое является родовым кольцом, то и сумма V тех произведений $S_\delta T_\epsilon U_\nu \ldots$, для которых выполнено (46), также содержится в $\mathfrak{B}$ (см. §1). Но V не принадлежит вырожденному комплексу группы $\mathfrak{H}$, и потому найдутся некоторые коэффициенты вида

$$c_{0\epsilon\nu\ldots},\ c_{\delta 0\nu\ldots},\ c_{\delta\epsilon 0\ldots},\ \ldots,$$

равные $c_{\chi\lambda\mu\ldots}$.

Из(46), в силу (45) получается, что всякий раз, когда выполнено

$$x_{\alpha\beta\gamma\ldots} \neq 0,$$

имеет место равенство

$$a_{\alpha_\chi} b_{\beta_\lambda} c_{\gamma_\mu} \cdots = a_{\alpha_\delta} b_{\beta_\epsilon} c_{\gamma_\nu} \cdots \tag{47}$$

При этом используя формулу (40), мы также имеем:

$$a_{\alpha_\chi} \geqslant |a_{\alpha_\delta}|,\ b_{\beta_\lambda} \geqslant |b_{\beta_\epsilon}|,\ c_{\gamma_\mu} \geqslant |c_{\gamma_\nu}|,\ \ldots \tag{48}$$

Пусть теперь $p > 2$ и $\chi > 0$. Среди отличных от нуля коэффициентов $x_{\alpha\beta\gamma\ldots}$ должны встретиться коэффициенты вида $x_{\chi\beta\gamma\ldots}$. Поскольку $\alpha < \chi$, то в (43) присутствуют только $S''_0, \ldots, S''_{\chi-1}$. Поэтому $S_0, S_1, \ldots$ появляются только в выражении

$$S_{\chi-1} + S_\chi + \cdots + S_a.$$

Это невозможно, если χ – связывающее число для p.

Среди равенств (47) должно встретиться и равенство

$$a_{\chi_\chi} b_{\beta_\lambda} c_{\gamma_\mu} \ldots = a_{\chi_0} b_{\beta_\epsilon} c_{\gamma_\nu} \ldots \tag{49}$$

Поэтому по (40) при $p > 2$, $\chi > 0$ мы получаем, что

$$a_{\chi_\chi} = p - 1 > 1, \ b_{\beta_\lambda} = q - 1 \text{ или } 1, \ \dots ,$$

откуда следует, что коэффициент a_{χ_0} принимает значение -1 или 0. Из формулы (48) теперь очевидно, что (49) не может быть справедливым. Поэтому для $p > 2$ должно быть $\chi = 0$.[12]

Таким образом для каждого нечетного простого делителя n соответствующее связывающее число должно иметь значение 0. Из сказанного следует, что наше предположение о том, что группа $\mathfrak{G}$ примитивна, но не дважды транзитивна, – неверно. Поэтому утверждение III полностью доказано.

9. Одно следствие утверждения III

Пусть $\mathfrak{G}$ – группа перестановок степени n, содержащая цикл P порядка n. Рассмотрим в качестве переставляемых символов n элементов группы $\mathfrak{H}$, порожденной P. Если n не простое число и $\mathfrak{G}$ не является дважды транзитивной, то из утверждения III и результата §3 следует, что найдется подгруппа

$$\mathfrak{U} = E + P^d + P^{2d} + \dots + P^{n-d}$$

группы $\mathfrak{H}$ с делителем d числа n, отличным от 1 и n, такая, что элементы d классов смежности

$$\mathfrak{U}, \mathfrak{U}P, \dots , \mathfrak{U}P^{d-1}$$

образуют систему импримитивности группы $\mathfrak{G}$.

Отметим, что при этом те перестановки S из $\mathfrak{G}$, которые переставляют символы только внутри каждого блока, образуют инвариантную подгруппу $\mathfrak{Z}$ группы $\mathfrak{G}$. В частности, $S = P^d$ циклически переставляет n/d элементов класса смежности $\mathfrak{U}P^\lambda$ (ср. §2). Поскольку группа $\mathfrak{Z}$ содержит элемент P^d, ее порядок не может быть меньше, чем n/d.

Если n – простое число и группа $\mathfrak{G}$ не является дважды транзитивной, то из утверждения I, доказанного Бернсайдом, следует, что группа $\mathfrak{G}$ содержит инвариантную подгруппу $\mathfrak{H} = \{P\}$.

---

[12] Надо иметь в виду, что хотя в этом рассуждении p играет привилегированную роль для комплекса $\mathfrak{M}_\sigma$, никакого ограничения на самом деле нет.

Это все вместе дает следующее утверждение:

IV. *Если группа перестановок $\mathfrak{G}$ степени n, не являющаяся дважды транзитивной, содержит цикл порядка n, то она обладает инвариантной подгруппой, которая содержит отличную от E степень этого цикла.*

Это утверждение для случая, когда n является степенью простого числа, может быть найдено в [2, с. 343].

Литература

1. W. Burnside, *On the properties of groups of odd order.* — Proc. London Math. Soc. **33** (1900).
2. W. Burnside, *Theory of Groups of Finite Order,* 2. Auflage (1911).
3. I. Schur, *Neuer Beweis eines Satzes von W. Burnside.* — Jahresbericht der Deutschen Mathematiker-Vereinigung **17** (1908).

Schur I. Zur Theorie der einfach transitiven Permutationsgruppen (A contribution to theory of transitive permutation groups).

This is a Russian translation of the famous paper by I. Schur in which the method of Schur rings is introduced. The method is used to prove that every primitive permutation group containing a regular cyclic subgroup of composite order is 2-transitive.