Доклады Академии Наук СССР
1953. Том XCI, № 1

МАТЕМАТИКА

С. Д. БЕРМАН

О НЕКОТОРЫХ СВОЙСТВАХ ЦЕЛОЧИСЛЕННЫХ ГРУППОВЫХ КОЛЕЦ

(Представлено академиком О. Ю. Шмидтом 21 IV 1953)

В настоящей заметке исследуется уравнение $x^m = 1$ в целочисленном групповом кольце.

Пусть G — конечная группа, e_0 (единица), $e_1, \ldots, e_{n-1}$ — ее элементы. Обозначим через $R(G, C)$ и $R(G, K)$ групповые кольца группы G, соответственно, над кольцом целых рациональных и полем рациональных чисел.

В групповом кольце естественным образом определяется инволюция. Если

$$x = \alpha_0 e_0 + \ldots + \alpha_{n-1} e_{n-1},$$

то положим

$$x^* = \alpha_0 e_0^{-1} + \ldots + \alpha_{n-1} e_{n-1}^{-1}.$$

Назовем нормальным элемент x группового кольца, удовлетворяющий условию $xx^* = x^*x$.

Будем говорить, что $u \in R(G, K)$ является элементом конечного порядка или корнем из единицы, если $u^m = e_0$ для некоторого положительного целого m. Порядком корня из единицы u назовем наименьшее из положительных целых t, для которых $u^t = \pm e_0$. Тривиальными корнями из единицы будем называть элементы $\pm e_j$ $(j = 0, \ldots, n-1)$. Если $x = \alpha_0 e_0 + \ldots + \alpha_{n-1} e_{n-1}$, то матрицу, соответствующую x в регулярном представлении группового кольца, обозначим через $\overline{X}$.

Имеет место формула ([2])

$$\alpha_0 = \frac{S(\overline{X})}{n}. \qquad (1)$$

Лемма 1. *Пусть* $x = \alpha_0 e_0 + \ldots + \alpha_{n-1} e_{n-1}$ — *идемпотентный элемент группового кольца группы* G *над полем комплексных чисел. Тогда* $\alpha_0 = p/n$, *где* p — *число характеристических корней матрицы* $\overline{X}$, *равных* 1.

Следствие. $R(G, C)$ *неразложимо в прямую сумму нетривиальных идеалов* (*правых или левых*).

В самом деле, кольцо с единицей разлагается в прямую сумму нетривиальных идеалов тогда и только тогда, когда оно содержит идемпотенты, отличные от 0 и 1 ([2]). Но из леммы 1 вытекает, что единственными идемпотентами в $R(G, C)$ являются 0 и 1.

Лемма 2. *Если* $u = \alpha_0 e_0 + \ldots + \alpha_{n-1} e_{n-1}$ — *корень из единицы в* $R(G, C)$ и $\alpha_0 \neq 0$, *то* $u = \pm e_0$.

Доказательство получается путем перехода к регулярному представлению с последующим использованием формулы (1).

Теорема 1. *Всякий нормальный элемент конечного порядка в $R(G, C)$ с точностью до знака совпадает с элементом группы.*

Действительно, если $x = \alpha_0 e_0 + \ldots + \alpha_{n-1} e_{n-1}$ — нормальный корень из единицы, то $xx^* = (\alpha_0^2 + \ldots + \alpha_{n-1}^2) e_0 + \ldots$ — элемент конечного порядка, удовлетворяющий условиям леммы 2.

Следствие 1. *Если G — абелева группа или гамильтонова группа порядка 2^m, то $R(G, C)$ содержит только тривиальные корни из единицы.*

Нормальность каждого элемента группового кольца абелевой группы является тривиальным фактом. Можно проверить, что все элементы группового кольца гамильтоновой группы порядка 2^m также нормальны (другое доказательство этой теоремы содержится в [3]).

Следствие 2. *Если целочисленные групповые кольца групп G_1 и G_2 изоморфны, то центры этих групп изоморфны.*

Теорема 2. *Порядок корня из единицы в кольце $R(G, C)$ является делителем порядка группы.*

Доказательство. Пусть $u = \alpha_0 e_0 + \ldots + \alpha_{n-1} e_{n-1}$ — *корень из единицы порядка m в $R(G, C)$. Если $u^m = -e_0$, то $(\alpha_0 + \ldots + \alpha_{n-1})^m = -1$, откуда вытекает, что m — нечетное число и $(-u)^m = e_0$.*

Образуем элемент

$$e = \frac{e_0 + (-1)^m u + \ldots + [(-1)^m u]^{m-1}}{m} = \gamma_0 e_0 + \ldots + \gamma_{n-1} e_{n-1}.$$

Очевидно, e — идемпотент в $R(G, K)$.

Положим $u^r = \beta_0^{(r)} e_0 + \ldots + \beta_{n-1}^{(r)} e_{n-1}$ $(r = 1, 2, \ldots)$. Если для некоторого $r < m$ $\beta_0^{(r)} \neq 0$, то, в силу леммы 2, $u^r = \pm e_0$, что противоречит тому, что m — порядок элемента u. Значит, $\gamma_0 = \frac{1}{m}$. На основании леммы 1 $\frac{1}{m} = \frac{p}{n}$, откуда следует, что m является делителем n-го порядка группы.

Теорема 2 является обобщением теоремы о порядках элементов конечной группы.

Лемма 3. *Пусть гамильтонова группа G представляется в виде прямого произведения абелевой группы G' на группу кватернионов S [1]. Если разложение кольца $R(G', K)$ в прямую сумму полей деления круга имеет вид $R(G', K) = I_1 + \ldots + I_s$, то имеет место разложение:*

$$R(G, K) = 4(I_1 + \ldots + I_s) + K_1 + \ldots + K_s, \qquad (2)$$

*где K_j $(j = 1, \ldots, s)$ — кольцо кватернионов над полем I_j *.*

Теорема 3. *$R(G, K)$ тогда и только тогда не содержит нильпотентных элементов (т. е. разлагается в прямую сумму тел), когда G является либо абелевой группой, либо гамильтоновой группой порядка $t2^m$, где 2 принадлежит по модулю t нечетному показателю.*

Пусть e_i и e_j — произвольные элементы группы G, причем порядок e_i равен s. Элемент $y = (e_0 - e_i) e_j (e_0 + e_i + \ldots + e_i^{s-1}) \in R(G, C)$ удовлетворяет уравнению $x^2 = 0$ и, значит, равен нулю. Отсюда заключаем, что каждая циклическая подгруппа группы G является нормальным делителем. Значит, G — гамильтонова группа.

---

* Коэффициент 4 перед суммой $(I_1 + \ldots + I_s)$ означает, что каждое из полей I_j $(j = 1, \ldots, s)$ в прямом разложении (2) встречается 4 раза.

Использование леммы 3 и результатов о полях разложения тела кватернионов над полем рациональных чисел ([4]) завершает доказательство теоремы.

Теорема 4. *Пусть G — конечная группа. Тогда эквивалентны следующие предложения*:

I. *Все корни из единицы в $R(G, C)$ тривиальны.*

II. *Все элементы кольца $R(G, C)$ нормальны.*

III. *G либо абелева группа, либо гамильтонова группа порядка 2^m.*

В силу теоремы 1 и следствия 1 этой теоремы для доказательства теоремы 4 достаточно показать, что из II вытекает III.

Пусть $R(G, C)$ содержит только тривиальные корни из единицы. Рассмотрим элемент $a \in R(G, C)$, удовлетворяющий условию $a^2 = 0$. При любом целом k

$$(e_0 + ka)(e_0 - ka) = (e_0 - ka)(e_0 + ka) = e_0. \tag{3}$$

В силу (3) для произвольного $e_i \in G$ и любого целого k

$$e^{(k)} = (e_0 + ka)\, e_i\, (e_0 - ka) = e_i + k\,[(ae_i - e_i a) + kae_i a]$$

является элементом конечного порядка в $R(G, C)$ и, значит, с точностью до знака совпадает с элементом группового базиса.

Это может быть только в том случае, когда

$$ae_i - e_i a = 0; \quad ae_i a = 0 \quad (i = 0, \ldots, n-1). \tag{4}$$

Из (4) вытекает, что a — элемент центра $R(G, C)$. $R(G, K)$ разлагается в прямую сумму полных матричных колец над некоторыми телами. Если порядок хотя бы одного из этих колец отличен от 1, то в $R(G, C)$ всегда найдутся элементы a, удовлетворяющие условию $a^2 = 0$ и не принадлежащие центру. Значит, $R(G, K)$ — прямая сумма тел и, на основании теоремы 3, G — гамильтонова группа порядка $t\,2^m$, где 2 принадлежит по модулю t нечетному показателю.

Пусть G разлагается в прямое произведение: $G = P_1 \times P_2 \times S$, где P_1 — абелева группа порядка t; P_2 — прямое произведение r циклических групп второго порядка $(0 \leqslant r)$; S — группа кватернионов. S задается определяющими соотношениями

$$p^4 = e_0; \quad q^4 = e_0; \quad q^{-1}pq = p^3; \quad p^2 = q^2.$$

Если $t \neq 1$, то $R(G, C)$ содержит нетривиальные делители единицы ([3]). Можно показать, что в этом случае в $R(G, C)$ найдется обратимый элемент c такой, что $c^{-1}pc$ уже не будет тривиальным корнем из единицы. В качестве c можно, например, взять элемент (c задается как некоторая степень элемента из $R(G, K)$)

$$c = \left[e_0 + \frac{(aq + a^2q^2)(e_0 - q^2)\,((s-1)\,e_0 - a - \ldots - a^{s-1})}{2s}\right]^{t_1},$$

где a — элемент простого порядка s группы P_1; t_1 — число классов вычетов по модулю $4s$ в поле $K(\varepsilon)$, взаимно простых с $4s$; ε — первообразный корень степени $4s$ из единицы.

Выражаю благодарность чл.-корр. АН УССР Я. Б. Лопатинскому за ряд ценных указаний.

Поступило
29 IV 1952

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] О. Ю. Шмидт, Абстрактная теория групп, 1933. [2] Ван-дер-Варден, Современная алгебра, 2, 1947. [3] G. Higman, Proc. London Math. Soc., **46** (1940). [4] H. Hasse, Math. Ann., **107** (1932).