Ранги групп центральных единиц целочисленных групповых колец знакопеременных групп

Р. Ж. АЛЕЕВ
Южно-Уральский государственный университет
e-mail: aleev@csu.ru

А. В. КАРГАПОЛОВ
Южно-Уральский государственный университет
e-mail: akargapolov@gmail.com

В. В. СОКОЛОВ
Южно-Уральский государственный университет
e-mail: sokolov@vpkre.ru

УДК 512.552.7+511.622+512.547.214

Ключевые слова: групповое кольцо, центральная единица, знакопеременная группа, разбиение, характер группы, компьютерные вычисления.

Аннотация

Пусть G — конечная группа и $\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ — группа единиц центра $Z(\mathbf{Z}G)$ целочисленного группового кольца $\mathbf{Z}G$ (группа центральных единиц кольца $\mathbf{Z}G$). В работе изучаются ранги r_n групп $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$ центральных единиц целочисленных групповых колец знакопеременных групп A_n. Найдены все значения n, при которых $r_n = 1$, показано, как описать в этих случаях группу $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$, и приведены некоторые результаты вычислений r_n для $n \leqslant 600$.

Abstract

R. Zh. Aleev, A. V. Kargapolov, V. V. Sokolov, The ranks of central unit groups of integral group rings of alternating groups, Fundamentalnaya i prikladnaya matematika, vol. 14 (2008), no. 7, pp. 15—21.

Let G be a finite group and $\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ be the group of units of the center $Z(\mathbf{Z}G)$ of the integral group ring $\mathbf{Z}G$ (the central unit group of the ring $\mathbf{Z}G$). The purpose of the present work is to study the ranks r_n of groups $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$, i.e., of central unit groups of integral group rings of alternating groups A_n. We shall find all values n for $r_n = 1$ and propose an approach how to describe the groups $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$ in these cases, and we will present some results of calculations of r_n for $n \leqslant 600$.

Пусть G — конечная группа, $\mathbf{Z}G$ — её целочисленное групповое кольцо, $Z(\mathbf{Z}G)$ — центр кольца $\mathbf{Z}G$ и $\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ — группа единиц кольца $Z(\mathbf{Z}G)$ (группа центральных единиц кольца $\mathbf{Z}G$). Нетрудно заметить, что группа $\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ совпадает с центром $Z\big(\mathrm{U}(\mathbf{Z}G)\big)$ группы $\mathrm{U}(\mathbf{Z}G)$ всех единиц кольца $\mathbf{Z}G$. Группа

Фундаментальная и прикладная математика, 2008, том 14, № 7, с. 15—21.

$\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ даёт важную информацию о группе $\mathrm{U}(\mathbf{Z}G)$, поскольку в силу [5, 6] в «большинстве» случаев на ней заканчивается верхний центральный ряд группы $\mathrm{U}(\mathbf{Z}G)$. Отметим, что в [4] группа $\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ является конечно порождённой, потому важную информацию о группе $\mathrm{U}\big(Z(\mathbf{Z}G)\big)$ даёт её ранг (число бесконечных прямых сомножителей).

Цель настоящей работы — изучение рангов r_n групп $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$ центральных единиц целочисленных групповых колец знакопеременных групп A_n. Отметим, что для $n \leqslant 6$ группы $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$ полностью описаны в [4]. Р. Ферраз в [7] нашёл, при каких n ранг r_n равен нулю, то есть группа $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$ тривиальна ($\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big) = \langle -1\rangle \times Z(\mathrm{A}_n)$). В развитие этого результата мы найдём, когда $r_n = 1$, покажем, как описать в этих случаях группу $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$, и приведём некоторые результаты вычислений r_n для $n \leqslant 600$.

1. Небольшие ранги

Везде через r_n обозначается ранг группы $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$ центральных единиц целочисленного группового кольца знакопеременной группы A_n. *Разбиением* натурального числа n называется представление его в виде суммы натуральных слагаемых, взятых в неубывающем порядке. Будем говорить, что разбиение является квадратом, если произведение всех его элементов является квадратом натурального числа. Воспользуемся следующим результатом.

Лемма 1 [7, теорема 4.5]. *Ранг r_n равен количеству разбиений*

$$a = [a_1, \ldots, a_k]$$

натурального числа n, удовлетворяющих следующим свойствам:

1) a_i *нечётно,* $1 \leqslant i \leqslant k$;
2) $a_i \neq a_j$ *при* $i \neq j$;
3) $n \equiv k \pmod 4$;
4) $\prod\limits_{i=1}^{k} a_i$ *не является полным квадратом.*

Замечание 1. Этот результат давно был известен первому автору (но не был опубликован). С его использованием были проведены вычисления r_n для $n \leqslant 100$, которые были распространены среди участников Международной алгебраической конференции в Красноярске в 1993 году. Аналогичный результат был получен в [8].

Лемма 2. *Число k_n элементов разбиения, удовлетворяющего лемме* 1, *не превосходит* $[\sqrt{n}\,]$.

Доказательство. Этот факт легко проверяется и был отмечен Фробениусом [2, с. 179]. □

Лемма 3. *Ранги r_n для $n \leqslant 36$ представлены в следующей таблице*:

n	r_n	n	r_n	n	r_n	n	r_n
1	0	2	0	3	0	4	0
5	1	6	1	7	0	8	0
9	0	10	1	11	1	12	0
13	1	14	3	15	3	16	1
17	1	18	4	19	5	20	2
21	1	22	5	23	7	24	4
25	1	26	6	27	12	28	9
29	3	30	6	31	14	32	13
33	5	34	7	35	20	36	23

.

Доказательство. Для нахождения рангов используем леммы 1 и 2. Рассмотрение проведём по остаткам от деления на 4.

1. $n \equiv 1 \pmod 4$. Если $n \leqslant 36$ и $n \equiv 1 \pmod 4$, то $k_n \leqslant [\sqrt{33}] = 5$ и $k_n \in \{1, 5\}$. Поскольку рассуждения очень просты и могут быть легко воспроизведены, мы не будем полностью разбирать все случаи, а подробно рассмотрим только некоторые, аналогично которым можно разобрать оставшиеся.

   $k_n = 1$. Имеем следующие случаи.

   $n = 1$. Разбиение одно: $[1]$, квадрат; $r_1 = 0$.

   $n = 5$. Разбиение одно: $[5]$, неквадрат; $r_5 = 1$.

   $n = 9$. Разбиение одно: $[9]$, квадрат; $r_9 = 0$.

   Аналогично легко получим, что

   $$r_{13} = 1, \quad r_{17} = 1, \quad r_{21} = 1.$$

   $k_n \in \{1, 5\}$. Имеем следующие случаи.

   $n = 25$. Два разбиения: $[25]$ и $[9, 7, 5, 3, 1]$, но неквадрат только второе; $r_{25} = 1$.

   $n = 29$. Три разбиения: $[29]$, $[13, 7, 5, 3, 1]$ и $[11, 9, 5, 3, 1]$, все — неквадраты; $r_{29} = 3$.

   Также получим $r_{33} = 5$.

2. $n \equiv 2 \pmod 4$. В этом случае $n \leqslant 34$ и $k_n \leqslant [\sqrt{34}] = 5$, поэтому $k_n = 2$. Наименьшее разбиение — $[3, 1]$, поэтому $n \geqslant 4$.

   $n = 2$. Нет нужных разбиений; $r_2 = 0$.

   $n = 6$. Разбиение одно: $[5, 1]$, неквадрат; $r_6 = 1$.

$n = 10$. Два разбиения: $[9,1]$ и $[7,3]$, но неквадрат только второе; $r_{10} = 1$.

Аналогично получим

$$r_{14} = 3, \quad r_{18} = 4, \quad r_{22} = 5, \quad r_{26} = 5, \quad r_{30} = 6, \quad r_{34} = 7.$$

3. $n \equiv 3 \pmod 4$. В данном случае $n \leqslant 35$, $k_n \leqslant [\sqrt{35}] = 5$, и по лемме 2 $k_n = 3$. Наименьшее разбиение — $[5,3,1]$, поэтому $n \geqslant 9$.

   $n \in \{3,7\}$. Нет нужных разбиений; $r_3 = r_7 = 0$.

   $n = 11$. Разбиение $[7,3,1]$, неквадрат; $r_{11} = 1$.

   Точно так же получаем

   $$r_{15} = 3, \quad r_{19} = 5, \quad r_{23} = 7, \quad r_{27} = 12, \quad r_{31} = 14, \quad r_{35} = 20.$$

4. $n \equiv 0 \pmod 4$. В этом случае $n \leqslant 36$ и $k_n \leqslant [\sqrt{36}] = 6$, поэтому $k_n = 4$. Наименьшее разбиение $[7,5,3,1]$, и $n \geqslant 16$.

   $n \in \{4,8,12\}$. Нет нужных разбиений; $r_4 = r_8 = r_{12} = 0$.

   $n = 16$. Разбиение $[7,5,3,1]$, неквадрат; ранг $r_{16} = 1$.

   Проведя аналогичные вычисления, получим

   $$r_{20} = 2, \quad r_{24} = 4, \quad r_{28} = 9, \quad r_{32} = 13, \quad r_{36} = 23. \qquad \square$$

Лемма 4. *$r_n \geqslant 2$ при $n > 36$.*

Доказательство. Рассмотрим по отдельности четыре случая в соответствии с остатком от деления n на 4. В каждом из случаев явно укажем два различных разбиения, удовлетворяющих лемме 1.

1. Пусть $n \equiv 1 \pmod 4$ и $n > 33$. Рассмотрим два подслучая:

   если $n \not\equiv 1 \pmod 3$, то подойдут разбиения $[n-16,7,5,3,1]$ и $[n-22,13,5,3,1]$ (здесь 3 будет в первой степени), для $n \geqslant 41$ имеем $n - 22 \geqslant 19$;

   если $n \equiv 1 \pmod 3$, то подойдут разбиения $[n-20,11,5,3,1]$ и $[n-20,9,7,3,1]$, так как $n - 20 > 11$ при $n > 36$.

2. Пусть $n \equiv 2 \pmod 4$. Тогда $n \geqslant 38$. Допустим, что разбиения $[n-9,9]$ и $[n-25,25]$ не годятся. Тогда $n = s^2 + 9 = m^2 + 25$, и оба числа s и m нечётны. Однако

   $$(s-m)(s+m) = 16 \iff (s-m=2)\ \&\ (s+m=8),$$

   поэтому $n = 34$, что невозможно.

   Итак, можем взять одно из разбиений $[n-9,9]$ и $[n-25,25]$. Так как $n-1$ нечётно, найдётся нечётное простое p, которое делит $n-1$. Если $p = n-1$, то возьмём $[n-1,1]$. Иначе возьмём $[n-p,p]$, так как p не делит $n-p$.

3. Пусть $n \equiv 3 \pmod 4$. Тогда $n \geqslant 39$. Рассмотрим два подслучая:

   если $n \not\equiv 1 \pmod 3$, то подойдут разбиения $[n-4, 3, 1]$ и $[n-10, 7, 3]$;
   если $n \equiv 1 \pmod 3$, то подойдут разбиения $[n-8, 5, 3]$ и $[n-14, 11, 3]$.

4. Если $n \equiv 0 \pmod 4$ и $n > 36$, то имеем следующие подслучаи:

   если $n \not\equiv 0 \pmod 3$, то подойдут $[n-9, 5, 3, 1]$ и $[n-15, 11, 3, 1]$;
   если $n \equiv 0 \pmod 3$, то подойдут $[n-11, 7, 3, 1]$ и $[n-17, 13, 3, 1]$. □

Замечание 2. Из доказательства этой леммы видно, что можно для $n > 36$ извлечь более точную, чем $r_n \geqslant 2$, оценку для r_n. Однако нам это не потребуется.

В итоге получаем следующий результат.

Теорема 1. *Пусть r_n — ранг группы центральных единиц целочисленного группового кольца знакопеременной группы A_n. Тогда*

1) *для $n \leqslant 36$ имеем*

n	r_n	n	r_n	n	r_n	n	r_n
1	0	2	0	3	0	4	0
5	1	6	1	7	0	8	0
9	0	10	1	11	1	12	0
13	1	14	3	15	3	16	1
17	1	18	4	19	5	20	2
21	1	22	5	23	7	24	4
25	1	26	5	27	12	28	9
29	3	30	6	31	14	32	13
33	6	34	7	35	20	36	23

;

2) *при $n \geqslant 36$ имеем $r_n \geqslant 2$;*
3) $r_n = 0 \iff n \in \{1, 2, 3, 4, 7, 8, 9, 12\}$, $r_n = 1 \iff n \in \{5, 6, 10, 11, 13, 16, 17, 21, 25\}$.

Доказательство. Теорема следует из лемм 3 и 4. Утверждение для $r_n = 0$ также доказано в [7]. □

2. Случай ранга 1

Первым и третьим авторами были описаны все группы $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_n)\big)$, имеющие ранг 1. Согласно теореме 1 в этом случае $n \in \{10, 11, 13, 16, 17, 21, 25\}$. Полное описание весьма велико, и ему будет посвящена отдельная статья. Здесь же для создания целостной картины приведём описание для $n = 10$, указав без доказательства только основные моменты.

Мы будем пользоваться таблицей характеров группы A_{10}, приведённой в GAP [9]. Все характеры группы A_{10} кроме пары алгебраически сопряжённых характеров χ и χ^* степени 384, значения которых принадлежат квадратичному полю $\mathbf{Q}(\sqrt{21}\,)$, целочисленны.

Обозначение. Следуя [1], обозначим через $u(\lambda)$ локальную единицу, определяемую характером χ и единицей $\lambda \in \mathbf{Q}(\sqrt{21}\,)$.

Первый основной результат показывает, что достаточно рассматривать локальные единицы.

Лемма 5. *Пусть u — произвольная центральная единица из $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_{10})\big)$. Тогда $u = \beta u(\lambda)$ для $\beta \in \{1, -1\}$ и локальной единицы $u(\lambda)$, определяемой некоторой подходящей единицей λ из группы единиц кольца целых поля $\mathbf{Q}(\sqrt{21}\,)$.*

Итак, мы имеем чисто локальный случай. Поэтому надо изучать $u(\lambda)$ для характера χ степени 384.

Обозначения.

1. $\omega = \frac{1+\sqrt{21}}{2}$.
2. $z = z(\chi) = \frac{|\mathrm{A}_{10}|}{\deg \chi} = \frac{2^7 \cdot 3^4 \cdot 5^2 \cdot 7}{2^7 \cdot 3} = 3^3 \cdot 5^2 \cdot 7 = 4725$.

Значение числа z показывает следующая лемма.

Лемма 6. *Пусть $\lambda = \alpha + \beta\omega$. Локальная единица $u(\lambda)$ принадлежит $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_{10})\big)$ тогда и только тогда, когда $z = 4725$ делит $\alpha - 1$ и делит β. Другими словами, $u(\lambda) \in \mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_{10})\big)$ тогда и только тогда, когда $\lambda \in 1 + z\mathbf{Z}[\omega]$.*

Лемма 7. *Допустим, что $u(\lambda) \in \mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_{10})\big)$. Тогда $\lambda = (2+\omega)^{3780n}$ для подходящего целого n.*

Теперь сформулируем основной результат.

Теорема 2. $\mathrm{U}\big(Z(\mathbf{Z}\mathrm{A}_{10})\big) = \langle -1 \rangle \times \langle (2+\omega)^{3780} \rangle$.

Доказательство. Утверждение сразу следует из лемм 5 и 7. □

3. Поведение рангов при больших n

Как уже отмечалось, сначала были вычислены ранги r_n для $n \leqslant 100$, вычисления были очень долгими и занимали в то время несколько суток. Потом ранги были вычислены для $n \leqslant 200$, но снова на персональных компьютерах вычисления занимали очень длительное время, и дальнейшее продвижение было очень трудоёмко по времени.

В этом году вторым автором были произведены вычисления на кластере «Infinity» Южно-Уральского госуниверситета. За счёт применения параллельных

вычислений и предельной оптимизации программы удалось получить ранги для $n \leqslant 600$:

n	r_n	n	r_n
100	1006	400	172468858
200	171988	500	3044489334
300	6521918	600	40127403414

.

Дальнейшие вычисления становятся затруднительными даже на кластере, поскольку требуют очень большого времени, ведь порядок вычислений растёт примерно как $e^{\sqrt{n}}$. Более точно, мы имеем следующую экспериментальную формулу для вычисления рангов r_n групп центральных единиц целочисленных групповых колец знакопеременных групп:

$$r_n \approx \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{10,9}}},$$

которая согласуется с известной формулой Радемахера [3] для числа $p(n)$ всех разбиений числа n:

$$p(n) \approx \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}.$$

Литература

[1] Алеев Р. Ж. Единицы полей характеров и центральные единицы целочисленных групповых колец конечных групп // Мат. труды. — 2000. — Т. 3, № 1. — С. 3—37.

[2] Фробениус Г. Теория характеров и представлений групп. — Харьков: Гос. науч.-техн. изд. Украины, 1937. — (Харьковская мат. библиотека. Книга третья).

[3] Эндрюс Г. Теория разбиений. — М.: Наука, 1982.

[4] Aleev R. Ž. Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers // Internat. J. Algebra Comput. — 1994. — Vol. 4, no. 3. — P. 309—358.

[5] Arora S. R., Hales A. W., Passi I. B. S. Jordan decomposition and hypercentral units in integral group ring // Commun. Algebra. — 1993. — Vol. 21, no. 1. — P. 25—35.

[6] Arora S. R., Passi I. B. S. Central height of the unit group of integral group ring // Commun. Algebra. — 1993. — Vol. 21, no. 10. — P. 3673—3683.

[7] Ferraz R. A. Simple components and central units in group rings // J. Algebra. — 2004. — Vol. 279, no. 1. — P. 191—203.

[8] Giambruno A., Jespers E. Central idempotents and units in rational group algebras of alternating groups // Internat. J. Algebra Comput. — 1998. — Vol. 8, no. 4. — P. 467—477.

[9] The GAP Group, GAP — Groups, Algorithms, and Programming. Version 4.4.2; 2004. — `http://www.gap-system.org`.