УДК 512.542.1

В. А. Казинец, А. Ю. Разумовская

УМНОЖЕНИЯ В КОНЕЧНЫХ ГРУППАХ, ЗАДАННЫХ ГЕНЕТИЧЕСКИМ КОДОМ

В работе рассмотрены свойства умножения в конечной группе, заданной генетическим кодом.

Ключевые слова: группы, представления групп, умножение в группе.

Одним из методов определения группы является ее задание с указанием множества порождающих элементов и множества определяющих соотношений между порождающими элементами, которое получило название копредставление или генетический код. Такое задание групп имеет свои плюсы и минусы. С одной стороны, оно дает возможность изучить некоторые ее свойства. С другой стороны, по нему мало что можно сказать об абстрактном строении группы, и даже ответ на вопрос, не задают ли два множества определяющих соотношений одну и ту же группу, часто оказывается достаточно трудным.

Группа перестановок S_n (симметрическая группа), которая состоит из всех перестановок n объектов, представляет собой неотъемлемую часть всей теории групп. Она была введена в науку Эваристом Галуа для изучения условий разрешимости алгебраических уравнений в радикалах: с каждым алгебраическим уравнением он связал некоторую группу перестановок корней, свойства которой и определяют ответ на вопрос о разрешимости. Вообще, группы перестановок возникают всюду, где изучается симметрия, конечно, определенных объектов — например, с каждым кристаллом можно связать группу его вращений, записываемых перестановками вершин (кристалл рассматривается как многогранник).

Симметрическая группа связана с конечными группами так называемой теоремой Кэли, согласно которой любая конечная группа изоморфна некоторой подгруппе группы перестановок множества элементов этой группы.

Первые генетические коды группы S_n нашли Бернсайд и Мур. Код Бернсайда

Казинец Виктор Алексеевич — кандидат физико-математических наук, доцент, заведующий кафедрой математики и информационных технологий (Дальневосточный государственный гуманитарный университет, г. Хабаровск); e-mail: matan@khspu.ru

Разумовская Анастасия Юрьевна — студент (Дальневосточный государственный гуманитарный университет, г. Хабаровск); e-mail: ayan_nastya@mail.ru

$$R^n = R_1^2 = (RR_1)^{n-1} = [R^{-r+1}(RR_1)^{r-1}]^r = (R^{-j}R_1R^jR_1)^2 = E, \quad 2 \le r \le n, \quad 2 \le j \le \frac{n}{2}$$

в порождающих $R = (1\,2\,3\,\ldots\,n)$ и $R_1 = (1\,2)$ содержит на самом деле много лишних соотношений. В терминах тех же порождающих Мур дал более простой код

$$R^n = R_1^2 = (RR_1)^{n-1} = (R_1R^{-1}R_1R)^3 = \left(R_1R^{-j}R_1R^j\right)^2 = E, \ 2 \le j \le n-2.$$

Мур также указал код

$$R_1^2 = R_2^2 = \cdots = R_{n-1}^2 = E,$$
$$(R_iR_{i+1})^2 = E \ при\, 1 \le i \le n-2,$$
$$(R_iR_k)^2 = E \, при\, i \le k-2$$

в порождающих $R_1 = (12),\ R_2 = (23), \ldots, R_{n-1} = (n-1\ n)$.

В настоящее время широко используется сходный генетический код, состоящий из трех множеств соотношений:

$$R_1^2 = E$$
$$R_iR_{i+1}R_i = R_{i+1}R_iR_{i+1}, \quad 1 \le i \le n-2$$
$$R_iR_j = R_jR_{i,} \qquad i \le j-2$$

В работе [1] предложен следующий генетический код

$$x_i^{i+1} = e, \qquad i = \overline{1, n-1}$$
$$x_kx_i = x_1x_{i+1}x_k, \qquad k > i,$$

где $x_i = R_1R_2 \ldots R_i$,

Такой код симметрической группы наиболее интересен, потому что в нем любой элемент g группы S_n однозначно представляется в виде

$$g = x_1^{\alpha_1}x_2^{\alpha_2} \ldots x_{n-1}^{\alpha_{n-1}}, \ 0 \le \alpha_i \le i \qquad (1)$$

В таком представлении возникает много нерешенных задач, например:

- Нахождение обратного элемента g^{-1} по данным $(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$;
- Вычисление сопряженных элементов группы;
- Нахождение произведения элементов.

Рассмотрим произведение $x_k \cdot g$. Так как любой элемент группы S_n однозначно представляется в виде (1), то

$$g' = x_k \cdot g = x_1^{\varphi_1}x_2^{\varphi_2} \ldots x_{k-1}^{\varphi_{k-1}}x_k^{\varphi_k}x_{k+1}^{\alpha_{k+1}} \ldots x_{n-1}^{\alpha_{n-1}},$$

где $\varphi_i = \varphi_i(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

С помощью разработанных программ были найдены закономерности и описаны формулы нахождения элемента $g' = x_kg = x_1^{\alpha_1'}x_2^{\alpha_1'} \ldots x_{k-1}^{\alpha_{k-1}'}x_k^{\alpha_k'}x_{k+1}^{\alpha_{k+1}} \ldots x_{n-1}^{\alpha_{n-1}}$:

$$\alpha_i' = \left[\frac{(\alpha_i + (\alpha_{i+1} + \ldots + (\alpha_{k-2} + \alpha_{k-1}) \bmod (k-1)\ldots) \bmod (i+2)) \bmod (i+1) + (i+1)\cdot\alpha_{i-1}}{i}\right], \ i < k$$

$$\alpha_k' = (\alpha_{k-1} + \alpha_k + 1) \bmod (k+1).$$

Где $[a]$ — это целая часть числа a и $\alpha_0 = 0$.

Теорема. Для всех целых $k \in [1, n-1]$ имеет место равенство

$$x_k g = x_1^{[\alpha_1 + \ldots + [\alpha_{k-2} + \alpha_{k-1}]_{k-1} \ldots]_2} \cdot \ldots \cdot x_{k-1}^{[[\alpha_{k-1}]_k + k \cdot \alpha_{k-2}]^{k-1}} x_k^{[\alpha_{k-1} + \alpha_k + 1]_{k+1}} \ldots x_{n-1}^{\alpha_{n-1}} \quad (2)$$

где $[a]_i$ – остаток от деления числа a на i, $[a]^i$ – частное от деления числа a на i.

Доказательство.

В работе [2] была доказана формула умножения R_i на $g = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{n-1}^{\alpha_{n-1}}$:

$$R_i x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{n-1}^{\alpha_{n-1}} = x_1^{\alpha_1} \ldots x_{i-2}^{[\alpha_{i-2} + [\alpha_{i-1}]_i]_{i-1}} \cdot x_{i-1}^{i-1-\alpha_{i-1}} \cdot x_i^{[\alpha_i + [\alpha_{i-1}]+1]_{i+1}} \ldots x_{n-1}^{\alpha_{n-1}}.$$

В связи с тем, что $x_i = R_1 R_2 \ldots R_i$ $x_i = R_1 R_2 \ldots R_i$, доказательство будем проводить методом математической индукции.

1) Проверим формулу при $i = 1$:

$$x_1 g = R_1 \cdot x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{n-1}^{\alpha_{n-1}} = x_1^{\alpha_1 + 1} x_2^{\alpha_2} \ldots x_{n-1}^{n-1} = x_1^{[\alpha_1 + 1]_2} \ldots x_{n-1}^{n-1}.$$

2) Предположим, что формула справедлива для $i = k$, то есть

$$x_k g = x_1^{[\alpha_1 + \ldots + [\alpha_{k-2} + \alpha_{k-1}]_{k-1} \ldots]_2} \cdot \ldots \cdot x_{k-1}^{[[\alpha_{k-1}]_k + k \cdot \alpha_{k-2}]^{k-1}} x_k^{[\alpha_{k-1} + \alpha_k + 1]_{k+1}} \ldots x_{n-1}^{\alpha_{n-1}}$$

3) Докажем, что формула верна для $i = k + 1$:

$$x_{k+1} g = x_k R_{k+1} g = x_k (R_{k+1} g) = x_k \cdot x_1^{\alpha_1} \ldots x_{k-1}^{[\alpha_{k-1} + \alpha_k]_k} x_k^{k - \alpha_k} x_{k+1}^{[\alpha_{k+1} + \alpha_k + 1]_{k+2}} \ldots x_{n-1}^{\alpha_{n-1}} =$$

$$= x_1^{[\alpha_1 + \ldots + [\alpha_{k-2} + [\alpha_{k-1} + \alpha_k]_k]_{k-1} \ldots]_2} \ldots x_{k-2}^{[[\alpha_{k-2} + [\alpha_{k-1} + \alpha_k]_k]_{k-1} + (k-1) \cdot \alpha_{k-3}]^{k-2}} \cdot x_{k-1}^{[[\alpha_{k-1} + \alpha_k]_k + k \cdot \alpha_{k-2}]^{k-1}} \times$$

$$\times x_k^{[k - \alpha_k + [\alpha_{k-1} + \alpha_k]_k + 1]_{k+1}} \cdot x_{k+1}^{[\alpha_{k+1} + \alpha_k + 1]_{k+2}} \ldots x_{n-1}^{\alpha_{n-1}} = x_1^{[\alpha_1 + \ldots + [\alpha_{k-2} + [\alpha_{k-1} + \alpha_k]_k]_{k-1} \ldots]_2} \ldots \times$$

$$\times x_k^{[\alpha_k + (k+1) \cdot \alpha_{k-1}]^k} \cdot x_{k+1}^{[\alpha_{k+1} + \alpha_k + 1]_{k+2}}$$

Теорема доказана.

Данная теорема позволяет получить в явном виде формулы нахождения произведения элементов, вычисление обратного элемента, определять сопряженные элементы группы. К сожалению, вид этих формул достаточно громоздкий и сложный, поэтому мы не приводим их в этой работе. Но в некоторых частных случаях формула (2) позволяет получить ряд интересных результатов.

Следствие 1. *И*меют место равенства:

1) $x_n^{\alpha} \cdot x_k = x_{\alpha}^{\alpha} \cdot x_{\alpha + k} \cdot x_n^{\alpha}$, $\alpha + k \le n$;

2) $x_n \cdot x_k^k = x_k \cdot x_{k+1}^k \cdot x_n$, $k < n$;

3) $x_n^n \cdot x_n^k = x_{k-1}^{k-1} \cdot x_{n-1} \cdot x_n^{n-1}$, $k < n$;

4) $x_n^n \cdot x_k = x_{n-1}^k \cdot x_n^{n-k}$, $k < n$;

5) $\sum_{g \in G} g = \prod_{i=1}^{n-1} \frac{(1 - x_i^{i+1})}{(1 - x_i)}$;

***Следствие* 2.** Элемент группы S_n принадлежит знакопеременной подгруппе тогда и только тогда, когда $\sum_{i=1}^{n-1} \alpha_i \cdot i \equiv 0 \bmod 2 \cdot$

СПИСОК ЛИТЕРАТУРЫ

1. *Казинец В. А.* Копредставление симметрической группы // XXXIV Дальневосточная математическая школа-семинар имени академика Е. В. Золотова «Фундаментальные проблемы математики и информационных наук»: тезисы докладов / Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2009. С. 33—35.
2. *Казинец В. А.* Умножение в симметрической группе, заданной генетическим кодом // Действия торов: топология, геометрия, теория чисел: тезисы докладов Международной открытой российско-китайской конференции, Хабаровск, 2—7 сентября 2013 г. / под науч. ред. Бухштабера В.М., Быковского В.А. Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2013. С. 89—90.
3. *Коксетер Г. С. М., Мозер У. О. Дж.* Порождающие элементы и определяющие соотношения дискретных групп: пер. с англ. М.: Наука, 1980. 240 с.
4. *Супруненко Д. А.* Группы подстановок. Мн.: Навука і тэхніка, 1996. 366 с.

* * *

Kazinets Victor A., Razumovskaya Anastasia Yu.
MULTIPLICATION IN FINITE GROUPS SPECIFIED BY THE GENETIC CODE
(Far Easten State University of Humanities, Khabarovsk)

The paper discusses the properties of multiplication in a finite group, given by the genetic code.

Keywords: group, presentations of groups, multiplication group.

REFERENCES

1. Kazinets V. A. A Presentation of the Symmetric Group [Kopredstavlenie simmetricheskoy gruppy]. *XXXIV Dal'nevostochnaya matematicheskaya shkola-seminar imeni akademika E. V. Zolotova «Fundamental'nye problemy matematiki i informatsionnykh nauk»: tezisy dokladov* (Far Eastern Mathematical School Seminar, named after E. V. Zolotov "Fundamental Problems of Mathematics and Information Science": Book of abstracts). Khabarovsk, TOGU Publ., 2009, pp. 33—35.
2. Kazinets V. A. Multiplication in the Symmetric Group, Given by the Genetic Code [Umnozhenie v simmetricheskoy gruppe, zadannoy geneticheskim kodom]. *Deystviya torov: topologiya, geometriya, teoriya chisel: tezisy dokladov Mezhdunarodnoy otkrytoy rossiysko-kitayskoy konferentsii (*Torus Actions: Topology, Geometry, Number Theory: Book of abstracts of International Conference of the Russian-Chinese). Khabarovsk, TOGU Publ., 2013, pp. 89—90.
3. Coxeter H. S. M., Moser W. O. J. *Porozhdayushchie elementy i opredelyayushchie sootnosheniya diskretnykh grupp* (Generators and Relations for Discrete Groups): translation from English, Moscow, Nauka, 1980. 240 p.
4. Suprunenko D. A. *Gruppy podstanovok* (Groups of substitutions), Minsk, Navuka i tjehnika, 1996. 366 p.

* * *