Вестник Ивановского государственного университета

Серия «Биология, Химия, Физика, Математика»

Вып. 3 / 2005 С. 96 – 101

Н. И. Яцкин

ОПИСАНИЕ СЛОВАРНЫХ ГРУПП НАД НЕКОТОРЫМИ КОНЕЧНЫМИ ГРУППАМИ

Рассматривается конструкция $\mathbb{Z}$-словарной группы над конечной группой. Для словарной группы данная группа служит алфавитом; слово в групповом алфавите считается тривиальным, если все его "литеральные степени"равны групповой единице. Для некоторых групп небольшого порядка с помощью компьютерных вычислений получается (исчерпывающая либо частичная) информация о соответствующих словарных группах.

The construction of $\mathbb{Z}$-vocabulary groups over a finite groups is described. A given group is considered as an alphabet for its $\mathbb{Z}$-vocabulary. A word over this alphabet is considered as trivial if all its "literal powers"are equal to the group unit. Using computer calculations we get some information (exhaustive or partial) about $\mathbb{Z}$-vocabulary groups for some finite groups of a small order.

УДК 512.54.

1. Группы, порожденные гомоморфизмами групп. Пусть A и B — группы. В случае, когда группа B является неабелевой, подмножество $\mathrm{Hom}(A,B)$, вообще говоря, не будет подгруппой в группе $\mathrm{Map}(A,B)$ всех отображений из A в B (с поточечным умножением).

Рассмотрим подгруппу

$$\mathrm{GHom}(A,B) = \langle \mathrm{Hom}(A,B) \rangle \leqslant \mathrm{Map}(A,B), \tag{1}$$

порожденную множеством гомоморфизмов из A в B.

Идея использования такого рода подгрупп в (некоммутативной) гомологической алгебре высказывалась в работах А.Фрёлиха (см., напр., [3]).

Элементы группы $\mathrm{GHom}(A,B)$, т. е. поточечные конечные произведения гомоморфизмов и антигомоморфизмов, будем называть G-*гомоморфизмами* из A в B.

Общий вид G-гомоморфизма $h \in \mathrm{GHom}(A,B)$:

$$h = f_1^{\varepsilon_1} \cdot f_2^{\varepsilon_2} \cdot \dots \cdot f_s^{\varepsilon_s}, \tag{2}$$

где $f_i \in \mathrm{Hom}(A,B)$; $\varepsilon_i = \pm 1$; $i = 1, ..., s$; $s \in \mathbb{N}$.

Представление (2) определено неоднозначно. Два произведения типа (2) определяют один и тот же G-гомоморфизм, т. е.

$$f_1^{\varepsilon_1} \cdot f_2^{\varepsilon_2} \cdot \dots \cdot f_s^{\varepsilon_s} = g_1^{\delta_1} \cdot g_2^{\delta_2} \cdot \dots \cdot g_t^{\delta_t}, \tag{3}$$

тогда и только тогда, когда для любого элемента $a \in A$ справедливо равенство:

$$(f_1(a))^{\varepsilon_1} \cdot (f_2(a))^{\varepsilon_2} \cdot \dots \cdot (f_s(a))^{\varepsilon_s} = (g_1(a))^{\delta_1} \cdot (g_2(a))^{\delta_2} \cdot \dots \cdot (g_t(a))^{\delta_t}.$$

Из представления (2) ясно, что композиция двух G-гомоморфизмов является G-гомоморфизмом.

Далее, всякий гомоморфизм групп $\varphi : A \to A'$ определяет гомоморфизм групп G-гомоморфизмов:

$$\varphi^* : \mathrm{GHom}(A', B) \longrightarrow \mathrm{GHom}(A, B);\ \varphi^*(h) = h \circ \varphi;\ h \in \mathrm{GHom}(A', B).$$

Аналогично, гомоморфизм $\psi : B \to B'$ определяет гомоморфизм

$$\psi_* : \mathrm{GHom}(A, B) \longrightarrow \mathrm{GHom}(A, B');\ \psi_*(h) = \psi \circ h;\ h \in \mathrm{GHom}(A, B).$$

Можно, таким образом, констатировать, что группы G-гомоморфизмов определяют бифунктор из категории групп в категорию групп, контравариантный по первому аргументу и ковариантный по второму. (Заметим также, что может рассматриваться новая категория: с объектами — группами и морфизмами — G-гомоморфизмами.)

В коммутативном случае изучение групп гомоморфизмов является важной и активно разрабатываемой проблемой (см., напр., монографию [2] и имеющиеся там ссылки). Далее мы предпринимаем попытку разобраться со строением групп G-гомоморфизмов, хотя бы в простейшем случае, когда группа A является бесконечной циклической, а группа B — конечной, небольшого порядка.

2. $\mathbb{Z}$-словарь над группой. Зафиксируем первую группу $A = \mathbb{Z}$ и рассмотрим ковариантный функтор, сопоставляющий группе B группу G-гомоморфизмов

$$V_{\mathbb{Z}}(B) = \mathrm{GHom}(\mathbb{Z}, B), \tag{4}$$

которую будем называть *$\mathbb{Z}$-словарной группой* или *$\mathbb{Z}$-словарем* над группой B.

В этом случае, во-первых, благодаря коммутативности группы $A = \mathbb{Z}$ теряется различие между *гомо-* и *антигомо*морфизмами, а, во-вторых, каждый гомоморфизм $f : \mathbb{Z} \to B$ однозначно определяется своим значением $b = f(1)$ (которое может быть произвольным элементом группы B).

В результате мы приходим к следующему описанию группы (4). Рассмотрим свободный моноид, порожденный B, который состоит из всевозможных слов вида

$$w = [b_1, b_2, ..., b_s];\ b_i \in B;\ i = 1, ..., s;\ s = 0, 1, 2, ... \tag{5}$$

(включая пустое слово $w = [\,]$).

Поскольку буквы являются элементами группы (и их можно перемножать), то для всякого слова (5) определяется его *значение*

$$\mathrm{val} : W(B) \longrightarrow B; \mathrm{val}([b_1, b_2, ..., b_s]) = b_1 \cdot b_2 \cdot ... \cdot b_s. \tag{6}$$

Значением пустого слова считается 1. Отображение (6) является гомоморфизмом моноида в группу.

Далее, для слов вида (5) определятся *литеральные* (побуквенные) степени:

$$w^{[k]} = [b_1^k, b_2^k, ..., b_s^k]; k \in \mathbb{Z}. \tag{7}$$

Для пустого слова пустыми считаются все литеральные степени. Возведение в литеральную степень является эндоморфизмом моноида $W(B)$ в себя.

Два слова, (5) и $w' = [b'_1, b'_2, ..., b'_t]$ ($b'_j \in B$; $i = 1, ..., t$; $t = 0, 1, 2, ...$) будем называть $\mathbb{Z}$-*эквивалентными* (и использовать обозначение: $w \sim w'$), если совпадают значения всех литеральных степеней этих слов:

$$\mathrm{val}(w^{[k]}) = \mathrm{val}((w')^{[k]}) \tag{8}$$

для любого $k \in \mathbb{Z}$.

Другими словами, $w \sim w'$ равносильно выполнению для любого $k \in \mathbb{Z}$ равенства $b_1^k \cdot b_2^k \cdot \ldots \cdot b_s^k = (b'_1)^k \cdot (b'_2)^k \cdot \ldots \cdot (b'_t)^k$.

Слова, эквивалентные пустому, будем называть *тривиальными*. Отношение $\sim$ является конгруэнцией на $W(B)$, фактормоноид $W(B)/\sim$ является группой и

$$V_{\mathbb{Z}}(B) \cong W(B)/\sim . \tag{9}$$

Класс эквивалентности слова (5) будем (с использованием полужирных квадратных скобок) обозначать

$$\mathbf{w} = [b_1, b_2, ..., b_s]. \tag{10}$$

Единицей в группе (9) служит класс пустого слова $[\,]$. Однобуквенные слова $[b]$ попарно не эквивалентны, слово $[1]$ тривиально. Двухбуквенное слово тривиально тогда и только тогда, когда буквы взаимно обратны; трехбуквенное — когда буквы попарно коммутируют и их произведение равно 1.

Слово будем называть *редуцированным*, если оно не эквивалентно никакому слову меньшей длины. В каждом классе эквивалентности имеется редуцированное слово, но, вообще говоря, — не единственное.

Если $\mathbb{Z}$-словари групп B и B' представлены в виде (9), то гомоморфизм словарных групп

$$\psi_* : V_{\mathbb{Z}}(B) \longrightarrow V_{\mathbb{Z}}(B'),$$

отвечающий гомоморфизму $\psi : B \to B'$, может быть задан формулой

$$\psi_*([b_1, b_2, ..., b_s]) = [\psi(b_1), \psi(b_2), ..., \psi(b_s)]. \tag{11}$$

Нетрудно доказать, что $\mathbb{Z}$-словарь для прямого произведения двух (и любого конечного числа) групп изоморфен произведению $\mathbb{Z}$-словарей для групп-сомножителей.

3. $\mathbb{Z}$-словарь для группы конечного периода и для конечной группы. Пусть группа B является группой конечного периода d.

Тогда, как легко видеть, словарная группа также будет иметь период d. Значения литеральных степеней любого слова (5) будут повторяться с периодом, делящим d.

Историей слова (5) мы будем называть список значений литеральных степеней, начиная с первой и кончая степенью $d-1$:

$$\mathrm{hist}(w) = [\mathrm{val}(w), \mathrm{val}(w^{[2]}), ..., \mathrm{val}(w^{[d-1]})]. \tag{12}$$

В случае группы B конечного периода получается, что два слова из $W(B)$ эквивалентны тогда и только тогда, когда их истории совпадают:

$$[w \sim w'] \Leftrightarrow [\mathrm{hist}(w) = \mathrm{hist}(w')]. \tag{13}$$

Если же B является конечной группой порядка n, то оказывается, что количество попарно различных возможных историй для слов из $W(B)$ не превосходит n^{d-1}, и, следовательно, $\mathbb{Z}$-словарная группа $V_{\mathbb{Z}}(B)$ также является конечной и ее порядок не превосходит указанного числа.

В случае конечной группы B как-либо занумеруем ее элементы (начиная с единичного); затем занумеруем лексикографически слова из моноида $W(B)$. В каждом классе эквивалентных слов можно выбрать слово с наименьшим лексикографическим номером. Это слово автоматически будет редуцированным. Будем называть его *минимальным редуцированным* словом (mr-*словом*). С помощью mr-слов получают однозначное представление элементы словарной группы. (Необходимо заметить также, что всякое подслово mr-слова является mr-словом.)

4. Пакет процедур Cayley. Если данная группа B невелика (настолько, что может быть описана своей таблицей умножения — таблицей Кэли), то можно попытаться найти для нее все mr-слова и построить таблицу Кэли для $\mathbb{Z}$-словаря $V_{\mathbb{Z}}(B)$. С целью накопления "экспериментального материала"о словарных группах автором был разработан пакет компьютерных программ (процедур) **Cayley**, реализующий высказанную выше идею. Пакет позволяет:

— тестировать квадратную матрицу на возможность ее соответствия какой-либо конечной группе;

— изучать простейшие свойства групп, задаваемых таблицами Кэли, вычислять период группы и периоды ее элементов, находить центр и коммутант;

— проверять подмножество в группе на предмет того, является ли оно подгруппой (нормальной подгруппой);

— вычислять групповую оболочку подмножества и, в частности, определять, является ли это подмножество порождающим;

— задавать фактор-группу данной группы по ее нормальной подгруппе;

— задавать декартово произведение двух групп.

Имеется также возможность находить в заданной группе порождающие системы элементов, удовлетворяющие тем или иным (заранее предписанным) определяющим соотношениям, либо делать вывод об отсутствии таких систем. Это позволяет в некоторых случаях "опознать" группу путем просмотра таблиц групп малого порядка и подбора в этом списке группы, изоморфной данной.

Задача формирования списка mr-слов оказывается весьма трудоемкой как в плане значительных временных затрат, так и в плане высоких требований к объему оперативной памяти. Опробованы два алгоритма перебора mr-слов.

Первый алгоритм после определения всех mr-слов некоторой длины l осуществляет приписывание к ним справа очередной буквы (следя за тем, чтобы она не коммутировала с последней буквой исходного слова). Каждое из вновь полученных слов длины $l+1$ сопоставляется со всеми ранее найденными словами (в том числе и с уже найденными словами длины $l+1$) на предмет обнаружения эквивалентности. Если таковая не обнаруживается, то слово вносится в реестр mr-слов. Останов производится, если не найдется ни одного mr-слова длины $l+1$. Ясно, что этот алгоритм "экстремален в плане времени".

Второй алгоритм вместе с уже найденными словами хранит их истории, что очень убыстряет тестирование слова на "новизну"(т. е. на min-редуцированность). Но этот алгоритм "экстремален в плане пространства"(безжалостно расходует оперативную память).

Тем не менее кое-что удается просчитать.

5. Примеры описания $\mathbb{Z}$-словарных групп.

Пример 1. Группа $\mathbf{S_3}$ — симметрическая группа степени 3. Выберем следующую нумерацию элементов: 1, 2 = '$(1,2,3)$', 3 = '$(1,3,2)$', 4 = '$(1,2)$', 5 ='$(2,3)$', 6 = '$(1,3)$'. Вычисления с помощью пакета **Cayley** дают следующие результаты: группа $V_{\mathbb{Z}}(\mathbf{S_3})$ имеет порядок 54; ее элементы могут быть представлены mr-словами, среди которых: 1 пустое, 5 однобуквенных, 14 двухбуквенных, 22 трехбуквенных, 12 четырехбуквенных; словарная группа содержит: 9 элементов порядка 2, 26 — порядка 3, 18 — порядка 6 (одно из таких слов: $[2,4]$); имеет нетривиальный центр, состоящий из пустого слова и слов $[2,4,2,4]$, $[3,4,3,4]$.

Пример 2. Группа $\mathbb{H}_8$ — группа кватернионов. Нумерация: 1, 2 = '-1', 3 = 'i', 4 = '$-i$', 5 = 'j', 6 = '$-j$', 7 = 'k', 8 = '$-k$'. Группа $V_{\mathbb{Z}}(\mathbb{H}_8)$ имеет порядок 16. Гипотеза о том, что словарная группа изоморфна прямому произведению исходной группы на циклическую группу порядка 2 (т. е. $V_{\mathbb{Z}}(\mathbb{H}_8) \cong \mathbb{H}_8 \times \mathbf{C_2}$) подтверждается тем, что могут быть найдены элементы (например: $a = [2]$, $b = [1]$, $c = [1,2,3]$), порождающие словарную группу и удовлетворяющие соотношениям $a^2 = b^2 = (ab)^2$; $c^2 = 1$; $ac = ca$; $bc = cb$, которые однозначно определяют (см. [1]) группу $\mathbb{H}_8 \times \mathbf{C_2}$.

Пример 3. Группа $\mathbf{D_4}$ — диэдральная группа. Результат аналогичен предыдущему: $V_{\mathbb{Z}}(\mathbf{D_4}) \cong \mathbf{D_4} \times \mathbf{C_2}$.

Пример 4. Группа $\mathbf{UT_3(3)}$ — группа верхних унитреугольных матриц над полем $\mathbb{F}_3$, порядок которой равен 27 (а все неединичные элементы имеют порядок 3). Словарная группа имеет порядок 81 и подтверждается (с помощью подбора подходящих порождающих элементов), что она изоморфна прямому произведению исходной группы на циклическую группу $\mathbf{C_3}$.

Пример 5. Группа $\mathbf{A_4}$ — знакопеременная группа степени 4. Словарная группа имеет порядок 3072; ее элементы могут быть представлены mr-словами с длинами от 0 до 6.

Пример 6. Группа $\mathbf{S_4}$ — симметрическая группа степени 4. Вычисления довести до конца не удалось. Словарная группа содержит не менее 100 000 элементов.

Заметим, что словарный функтор можно итерировать. В простых случаях, когда однократное его применение сводится к прямому умножению на циклическую группу, повторное применение (в силу мультипликативности функтора) сведется к повторению такого умножения. Попытка найти "второй словарь"для группы $\mathbf{S_3}$ дала группу из 4374 элементов.

Библиографический список

1. *Коксеттер Г. С. М., Мозер У. О. Дж.* Порождающие элементы и определяющие соотношения дискретных групп. М.: Наука, 1980. 240 с.
2. *Фукс Л.* Бесконечные абелевы группы. М.: Мир, 1974. Т. 1. 336 с.
3. *Frölich A.* Non-abelian homological algebra. I : Derived functors and satellites // Proc. London Math. Soc. 1961. Vol. 11. № 42. P. 239—275.