УДК 512.24

А. П. Горюшкин

ОБ АЛГОРИТМЕ ДЛЯ ВЫЧИСЛЕНИЯ ИНДЕКСА ПОДГРУППЫ В ГРУППЕ, РАЗЛОЖИМОЙ В ПРЯМОЕ ПРОИЗВЕДЕНИЕ

Устанавливается, что в некоторой бесконечной серии групп, разложимых в прямое произведение, не существует алгоритма для вычисления индекса конечно порожденной подгруппы.

Ключевые слова: группа, подгруппа, прямое произведение, порождающее множество, алгоритмическая проблема, разрешимость, проблема вхождения, проблема равенства, проблема индекса.

Теория групп изобилует проблемами, не имеющими алгоритмического решения. В последние десятилетия такого рода проблемам нашлось практическое применение в криптографии в качестве основы криптостойкости протокола. Для криптографических приложений представляют интерес как классические проблемы Дэна (проблема слов, проблема сопряжённости и проблема изоморфизма), так и алгоритмические проблемы в теории групп, тесно связанные с классическими. Такими являются проблема вхождения и проблема индекса.

Проблема слов (проблема равенства) для конечно определённой группы G состоит в отыскании или доказательстве невозможности алгоритма, который для любого элемента w узнавал бы, равен этот элемент единице в G или нет.

Проблема вхождения для конечно определённой группы G состоит в отыскании или доказательстве невозможности алгоритма, который по любому конечному множеству элементов h_i (i = 1, 2, …, m) и элементу w узнавал бы, принадлежит или нет элемент w подгруппе H = гр(h_1, h_2, … , h_m), порождённой элементами h_i. Из алгоритмической разрешимости проблемы вхождения следует разрешимость проблемы слов. Поэтому проблему вхождения называют обобщённой проблемой равенства.

Проблема индекса для конечно определённой группы G состоит в отыскании алгоритма, который по любому конечному множеству элементов h_i (i = 1, 2, …, m) группы G узнавал бы, конечный или бесконечный индекс в G имеет подгруппа H = гр(h_1, h_2, … , h_m), порождённая этим

Горюшкин Александр Петрович — кандидат физико-математических наук, доцент, профессор кафедры математики и физики (Камчатский государственный университет имени Витуса Беринга, Петропавловск-Камчатский); e-mail: as2021@mail.ru.

множеством.

В конечно порождённой группе содержится лишь конечное число подгрупп для каждого данного конечного индекса. Поэтому если в группе G разрешимы проблема вхождения и проблема индекса, то, получив информацию, что индекс подгруппы H в G конечен, простым перебором подгрупп конечного индекса можно в конечное число шагов этот индекс вычислить точно (детальное описание такого алгоритма см., например, в [1], глава I, § 8, стр. 47—49).

Отметим, что если группа G является конечным расширением группы с неразрешимой проблемой индекса, то и в G проблема индекса также будет неразрешима. То же самое относится и к проблеме вхождения.

Для бесконечной циклической группы обе эти задачи сводятся к отысканию наибольшего общего делителя конечного числа целых чисел и проверки делимости двух чисел. Точнее, если H – подгруппа бесконечной циклической группы $F_1 = \langle a \rangle$ и $H = \text{гр}(a^{m_1}, a^{m_2}, \ldots, a^{m_k})$ и $w = a^n$, где $m_1, m_2, \ldots, m_k, n \in \mathbf{Z}$, то $w \in H$ тогда и только тогда, когда n делится на число $s = \text{НОД}(m_1, m_2, \ldots, m_k)$. Заметим, что в этом случае индекс $[F_1 : H]$ равен числу s. Таким образом, для группы F_1 алгоритм, решающий проблему вхождения в подгруппу H, одновременно даёт ответ и об индексе этой подгруппы в группе F_1.

Свободный порождающий элемент для подгруппы H в этом примере можно найти с помощью преобразования исходного порождающего множества.

В любой группе порождающее множество подгруппы можно изменить с помощью преобразований (аналогичных элементарным преобразованиям порождающего множества подпространства векторного пространства):

(1) замена элемента x на x^{-1};

(2) замена элемента x на элемент $x\,y$, где $x \neq y$;

(3) удаление единичного элемента.

Если в результате таких преобразований появится единичный элемент, то его из порождающего множества можно удалить.

Бесконечная циклическая группа $\langle a \rangle = F_1$ — это свободная группа ранга один. Однако для свободной группы F_r любого ранга r и проблема вхождения, и проблема индекса имеют алгоритмическое решение. Пусть $H = \text{гр}(h_1, h_2, \ldots, h_m)$ — конечно порождённая подгруппа свободной группы F_n. С помощью преобразований порождающего множества в конечное число шагов можно получить свободные порождающие для подгруппы H и, таким образом, найти ранг H. Такой способ получения свободных порождающих подгруппы свободной принято называть *методом Я. Нильсена* (см., например, [2], глава 1, п. 2, стр. 16—21).

О. Шрейер, оперируя не только порождающими элементами подгруппы, но и представителями смежных классов, установил связь между

индексом подгруппы свободной группы, рангом этой подгруппы и рангом исходной свободной группы (см. [2], стр. глава 1, п. 3, стр. 33—34). Если подгруппа H ранга k имеет конечный индекс в свободной нециклической группе ранга r, то этот индекс равен

$$\frac{k-1}{r-1}.$$

С помощью формулы Шрейера проблема индекса подгруппы свободной группы сводится к вычислению ранга подгруппы, который можно найти с помощью метода Нильсена.

Таким образом, проблема индекса для свободной группы алгоритмически разрешима. С помощью метода Нильсена в конечное число шагов можно выяснить, входит или не входит элемент свободной группы в данную конечную порождённую подгруппу, т. е. проблема вхождения для свободных групп тоже алгоритмически разрешима.

Каждый элемент из прямого произведения $A \times B$ имеет представление в виде произведения ab, где $a \in A$ и $b \in B$. Элемент ab равен единице тогда и только тогда, когда a и b — оба единичные. Это значит, что если в группах A, B алгоритмически разрешима проблема равенства, то эта проблема разрешима и в прямом произведении $A \times B$. Иначе говоря, разрешимость проблемы равенства *наследуется* прямым произведением. Разрешимость проблемы индекса в такой конструкции может и не наследоваться.

Будем называть группу G *почти свободной*, если она содержит в качестве подгруппы конечного индекса свободную *нециклическую* группу F. Если конечно определённая группа G почти свободна, то её свободная подгруппа F имеет конечный ранг; кроме того, можно считать, что F — нормальна в G.

В почти свободной группе разрешима и проблема индекса, и проблема вхождения.

Теорема. В прямом произведении двух изоморфных почти свободных групп проблема индекса алгоритмически неразрешима.

Доказательство. Пусть группы A и B — две изоморфные почти свободные группы. Группа A содержит в качестве нормальной подгруппы конечного индекса свободную подгруппу A_1 ранга m; и элементы a_1, a_2, …, a_m являются свободными порождающими для A_1. Аналогично в группе B содержится нормальная подгруппа B_1, причём B_1 свободная ранга m и $b_1, _2, \ldots, b_m$ — её свободные порождающие. Кроме того, $[A : A_1] = [B : B_1]$.

Если группа $G = A \times B$ является прямым произведением групп A и B, то её подгруппа G_1, порождённая подгруппами A_1 и B_1, образует прямое произведение:

$$G_1 = A_1 \times B_1.$$

Индекс G_1 в G равен $[A : A_1] \cdot [B : B_1]$, и поэтому он конечен.

Рассмотрим теперь произвольную конечно определённую группу R, заданную представлением

$$R = <r_1, r_2, \ldots, r_k; w_1(r_i), \ldots, w_n(r_i)>,$$

где $r_1, r_2, \ldots, r_k$ - порождающие элементы, а $w_1(r_i), \ldots, w_n(r_i)$ — определяющие соотношения. Напомним, что определяющее соотношение — это слова в алфавите $r_1, r_2, \ldots, r_k, r_1^{-1}, r_2^{-1}, \ldots, r_k^{-1}$.

В группе A_1 выберем подгруппу P такого индекса s, чтобы выполнялось неравенство

$$s \geq \frac{k-1}{m-1}.$$

Тогда по формуле О. Шрейера ранг подгруппы P равен $s(m – 1) + 1$, и это число не меньше k. Если ранг подгруппы P окажется строго больше k, то представление группы R дополним ещё $s – k$ порождающими элементами и приравняем эти элементы к единице. Без ограничения общности можно считать, что это уже сделано, т. е. $s = k$.

Пусть элементы $p_1, p_2, \ldots, p_k$ свободно порождают подгруппу P.

Аналогичным образом в группе B_1 выберем подгруппу Q ранга k, индекса s в B и со свободными порождающими $q_1, q_2, \ldots, q_k$.

Рассмотрим теперь два нормальных делителя, один в группе P, а другой — в Q. В группе P нормальный делитель N_1, порождённый элементами $w_1(r_i), \ldots, w_n(r_i)$, а в группе Q нормальный делитель N_2, порождённый элементами $w_1(q_i), \ldots, w_n(q_i)$. Точнее,

$$N_1 = <w_1(r_i), \ldots, w_n(r_i)>^P;$$

$$N_2 = <w_1(q_i), \ldots, w_n(q_i)>^Q.$$

В группе G_1 возьмем две подгруппы:

$$H_1 = \text{гр}(w_1(q_i), \ldots, w_n(q_i), p_1q_1, \ldots, p_kq_k);$$

$$H_2 = \text{гр}(w_1(p_i), \ldots, w_n(p_i), p_1q_1, \ldots, p_kq_k).$$

Элементы r_i, q_i лежат в различных прямых сомножителях группы G_1, поэтому они перестановочны:

$$r_i\, q_i = q_i\, r_i.$$

Это значит, что для любого слова φ выполняется равенство

$$\varphi(p_iq_i) = \varphi(p_i)\, \varphi(q_i).$$

Сопряжение элемента $w_j(p_i)$ с помощью элемента из H_1 равно соответствующему сопряжению с помощью элемента из подгруппы A. Отсюда следует, что подгруппа H_1 содержит N_1. Аналогично H_2 включает N_2.

Кроме того, и сами подгруппы H_1 и H_2 совпадают. Пусть $H = H_1 = H_2$, тогда:

$$H \cap P = N_1;$$

$$H \cap Q = N_2.$$

Если подгруппа H имеет конечный индекс в прямом произведении $A \times B$, то индекс H в подгруппе $A_1 \times B_1$ тоже конечен, а значит, конечны индексы N_1 и N_2 в подгруппах P и Q соответственно. Это означает, что группа R — конечна. Наоборот, если R конечна, то индексы N_1 и N_2 в подгруппах P и Q конечны, но P и Q подгруппы конечного индекса в прямых множителях, и, следовательно, индекс $[G_1 : H]$ и соответственно $[G : H]$ конечен.

Иначе говоря, проблема индекса в группе G эквивалентна проблеме конечности в классе всех конечно определённых групп.

Проблема конечности алгоритмически неразрешима (см., например, С. Адян [3]), а это значит, что и проблема индекса для конечно определенной группы тоже алгоритмически неразрешима.

Утверждение доказано.

Заметим, что в доказательстве используется лишь изоморфизм свободных подгрупп A_1 и B_1, т. е. группы A и B в этой серии групп с неразрешимой проблемой индекса можно было взять и не изоморфными; достаточно лишь конечности индексов $[A : A_1]$ и $[B : B_1]$.

Алгоритмическая неразрешимость проблемы означает, что машинного решения такой задачи не существует. Например, никакая техника никогда не сможет по единой программе отвечать на вопрос, конечен или бесконечен индекс произвольно выбранной конечно порождённой подгруппы в группе $F_2 \times F_2$, заданной представлением

$$< a, b, c, d; aca^{-1}c^{-1}, ada^{-1}d^{-1}, bcb^{-1}c^{-1}, bdb^{-1}d^{-1} >.$$

Отметим, что в некоторых случаях вычисление индекса конечно порождённой подгруппы в конечно определённой группе можно доверить технике. Правда, результат можно получить, как правило, лишь в случае конечного (и сравнительно небольшого) индекса подгруппы. Например, при использовании математического пакета символьных вычислений Maple 18 индекс подгруппы должен не превышать 128 000.

Машинные вычисления такого рода, связанные с решением конкретных задач в теории групп, представлены в работах [4]—[7].

Для прямого произведения двух свободных групп второго ранга неразрешима и проблема вхождения (С. Михайлова, [8]). Доказательство этого утверждения в [8], проведённое лишь для одной группы $F_2 \times F_2$, легко переносится и на более общий случай прямого произведения двух почти свободных групп.

Таким образом, возникает бесконечная серия конечно определённых групп, для которых проблема вхождения и проблема индекса оказались эквивалентными (обе неразрешимы).

С другой стороны, в почти свободной группе обе проблемы: и проблема вхождения, и проблема индекса — алгоритмически разрешимы. Возможно, что эта связь между двумя алгоритмическими проблемами выполняется для всех конечно определённых групп.

Иначе говоря, возникает естественный **вопрос**: верно ли, что в классе конечно определённых групп проблема вхождения алгоритмически эквивалентна проблеме индекса?

Список литературы

1. Горюшкин А. П. Амальгамированные свободные произведения групп. Владивосток: Издательский дом Дальневост. федерал. ун-та, 2012. 158 с.
2. Линдон Р., Шупп П. Комбинаторная теория групп. М.: Мир, 1980. 448 с.
3. Адян С. И. Алгоритмическая неразрешимость проблем распознавания некоторых свойств групп // Докл. АН СССР. 1955. Т. 103. № 4. С. 533—535.
4. Горюшкин А. П. Особенности машинного исследования дискретных групп // Вестник КРАУНЦ, Сер. физ.-мат. науки. 2013. № 1 (6). С. 43—55.
5. Горюшкин А. П. Машинное решение задач дискретной математики // Вестник КРАУНЦ, Сер. физ.-мат. науки. 2011. № 2 (3). С. 58—68.
6. Горюшкин А. П. О группах с представлением < a, b; an = 1, ab = b3a3 > // Вестник КРАУНЦ, Серия. Физико-математические науки. 2010. № 1. С. 8—11.
7. Горюшкин А.П., Горюшкин В. А. Элементы абстрактной и компьютерной алгебры: учебное пособие. 2-е изд., испр. и доп. Петропавловск-Камчатский: КамГУ им. Витуса Беринга, 2011. 518 с.
8. Михайлова С. А. Проблема вхождения для прямых произведений групп // Математический сборник. 1966. Т. 70. № 2. С. 241—251.

* * *

Goryushkin Alexander P.

ON ALGORITHM FOR CALCULATION OF INDEX OF A SUBGROUP IN A DIRECT PRODUCT OF THE DECOMPOSABLE GROUP

(Vitus Bering Kamchatka State University, Petropavlovsk Kamchatskiy)

In this paper the author proves that for a certain infinite series of direct product of the decomposable groups there is not any algorithm for calculation of index finitely generated subgroups.

Keywords: group, subgroup, direct product, set of generators, algorithmic problem, decidability, occurrence problem, equality problem, index problem.

References

1. Goryushkin A. P. *Amalgamirovannye svobodnye proizvedeniya grupp* (Amalgamated free products of groups), Vladivostok, DFU Publ., 2012. 158 p.
2. Lindon R. C., Schupp P. E. *Combinatornaya teoriya grupp* (Combinatorial group theory), Moscow, 1980. 448 p.
3. Adyan S. I. Algotitmicheskaya nerazreshimost problem razpoznavaniya nekotorych svoystv grupp (Algorithmic undecidability of problems of recognition some properties of groups), *Doklady AN SSSR*, 1955, vol. 103, no. 4, pp. 533—535.

4. Goryushkin A. P. Osobennosti mashinnogo issledovaniya diskretbych grupp (Features of machine study of discrete groups), *Vestnik KRAUNC, Series. Fiziko-matematicheskie nauki*, 2013, no. 1(6), pp. 43—55.
5. Goryushkin A. P. Mashinnoe reshenie zadach diskretnoy matematiki (Machine solutions of discrete mathematics problems), *Vestnik KRAUNC, Series. Fiziko-matematicheskie nauki*, 2011, no. 2(3), pp. 58—68.
6. Goryushkin A. P. O gruppach s predstavleniem < a, b; an = 1, ab = b3a3 > (On groups with representation < a, b; an = 1, ab = b3a3 >), *Vestnik KRAUNC, Series. Fiziko-matematicheskie nauki*, 2010, no. 1, pp. 8—11.
7. Goryushkin A. P., Goryushkin V. A. *Elementy abstractnoy i comp'yuternoy algebry* (Elements of abstract and computer algebra), Petropavlovsk-Kamchatskiy, KamGU im. Vitusa Beringa Publ., 2011. 518 p.
8. Mihaylova S. A. Problema vchogdeniya dlya pryamych proizvedehiy grupp (The occurrence problem for direct products of groups), *Matematicheskiy sbornik*, 1966, vol. 70, no. 2, pp. 241—251.

* * *