

## КОНСТРУКТИВНЫЕ СПОСОБЫ ЗАДАНИЯ И ПОСТРОЕНИЯ КОНЕЧНЫХ ГРУПП

Предложены на основе эффективной нумерации перестановок способы задания и построения конечных групп. Показана тривиальная разрешимость проблем эквивалентности, тождества и сопряженности слов в конечной группе. Доказана разрешимость проблемы изоморфизма в конечных группах.

### Введение

Теория групп – один из важных разделов математики. Сформировавшись в работах Эвариста Галуа как абстрактная наука, теория групп вначале применялась собственно в математике, а затем открылись ее прикладные возможности в механике, квантовой физике, кристаллографии.

Группа определяется как множество элементов (конечное или бесконечное) с заданной на нем бинарной операцией и такое, что в нем выполняются аксиомы ассоциативности, о единичном и обратных элементах [1–3]. Получив бурное развитие в XIX–XX веках, теория групп, пожалуй, прошла пик своего развития [1]. В этой теории были поставлены и решены ряд крупных проблем. Так, была доказана неразрешимость проблемы тождества слов [4] и их сопряженности в группе [5], а также проблемы установления изоморфизма групп [6].

Одними из ключевых вопросов теории групп являются вопросы задания и построения конкретной группы или некоторого их класса. Группу можно задать [2] как множество элементов с одной бинарной операцией, удовлетворяющее указанным выше аксиомам, при помощи таблицы умножения (таблицы Кэли), образующих и определяющих соотношений и, наконец, графической схемы (сети).

Группа, заданная одним из указанных выше способов, может быть изоморфно представлена группой перестановок [1–3]. Собственно сама теория групп начиналась с подстановок, а сегодня они заняли свое «скромное положение в общей теории». Тем не менее существует принципиальная разница между заданием конечной группы группой подстановок и образующими и определяющими соотношениями. При задании конечной группы с помощью подстановок отпадает необходимость в задании определяющих соотношений, поскольку они появляются автоматически. В этом смысле перестановка является конструктивной образующей, в отличие от абстрактной (неконструктивной) образующей, задаваемой буквами различных алфавитов. Абстрактные образующие естественным образом появляются в рамках свободных групп [1]. При этом для задания конечной группы как фактор-группы свободной группы кроме абстрактных образующих необходимо задать определяющие соотношения. Именно здесь и начинаются проблемы конечных групп, так как для группы, заданной системой образующих и системой определяющих соотношений, нельзя установить: конечна ли эта группа или бесконечна, коммутативна она или нет и т. д. [1]. Для прак-

тического использования конечных групп, например в информатике, существенные ограничения накладывает проблема эквивалентности слов в группе. Неудивительно, что здесь господствуют конструкции, основанные на полиномах различных степеней, простых числах и пр.

Конечная группа, как группа с кручением, независимо от природы ее элементов и вида бинарной операции является по существу группой отображений. Правда, существующий традиционный способ формирования перестановок на основе транспозиций далек от совершенства, поскольку допускает неоднозначность их представления [2].

В монографии [1] отмечено, что конечной целью теории групп следует считать «задачу полного описания всех существующих в природе групп или хотя бы достаточно широких классов групп...». Однако до настоящего времени не удалось получить полного описания даже конечных групп, хотя и имеется ряд предложений [1] по путям их каталогизации: использование разрешимых и простых групп, описание групп данного порядка и др.

Нерешенность указанного вопроса применительно к конечным группам объясняется, на наш взгляд, следующими основными причинами. Во-первых, отсутствует стандартный способ описания конечных групп с использованием конструктивных образующих. Во-вторых, не разработан формальный способ построения всей совокупности элементов конечной группы на основе указанных образующих. И, наконец, не предложены достаточно конструктивные и эффективные критерии изоморфизма конечных групп и алгоритмы их вычисления. Хотя понятие изоморфизма групп вполне конкретно и для конечных групп должен существовать некоторый способ перебора соответствий, однако такая процедура не совсем очевидна. Так, говоря о трудностях решения проблемы изоморфизма двух групп заданных конечным числом образующих и соотношений, автор [1] отмечает, «что задание конечных групп таблицами Кэли приводит к аналогичной проблеме изоморфизма».

Ниже на основе специальной системы счисления производится эффективная нумерация перестановок и на множестве этих номеров определяется группа. Предлагается способ формального построения всех элементов группы с использованием двух номеров перестановок, задающих конечную группу. Показывается тривиальная разрешимость проблем эквивалентности, тождества, сопряженности слов в конечной группе, доказывается разрешимость проблемы изоморфизма конечных групп и предлагаются критерии их изоморфизма. Высказываются некоторые соображения по построению каталога конечных групп.



Пусть, например, необходимо построить код перестановки  $M_i = 5-1-3-2-4$ . Последовательно выполняя приведенные выше операции, имеем:

$$\begin{aligned} M_1 &= 1-2-3-4-5 & K_1 &= 0-0-0-0-0 \\ M_{i1} &= 5-1-2-3-4 & K_{i1} &= 4-0-0-0-0 \\ M_{i2} &= 5-1-2-3-4 & K_{i2} &= 4-0-0-0-0 \\ M_{i3} &= 5-1-3-4-2 & K_{i3} &= 4-0-1-0-0 \\ M_{i4} &= 5-1-3-2-4 & K_{i4} &= 4-0-1-1-0. \end{aligned}$$

В итоге перестановке  $M_i = 5-1-3-2-4$  соответствует код  $K_{i4} = 4-0-1-1-0$ . Совпадение кодов  $K_{i1}$  и  $K_{i2}$  объясняется отсутствием необходимости каких-либо сдвигов в перестановке  $M_{i1}$ .

#### Способ задания конечной группы

Бинарную операцию, используемую для построения конечной группы на кодах перестановок одинакового ранга, зададим следующим образом: произведению кода  $K_i$  на код  $K_j$  соответствует код  $K_l$ , который получается циклическим сдвигом перестановки  $M_i$  кодом  $K_j$ .

В развернутом виде указанная операция записывается следующим образом:

$$K_i \cdot K_j = (K_i \rightarrow M_i) \cdot K_j = M_l \rightarrow K_l, \quad (2)$$

где « $\rightarrow$ » – знак бинарной операции; « $\rightarrow$ » – процедура перевода кода в перестановку и наоборот.

Поскольку ранг всех используемых далее кодов и перестановок не превосходит девяти, то для краткости записей  $M_i$  и  $K_j$  дефисы (« $\rightarrow$ ») далее опускаем. При этом запись перестановки от кода отличается тем, что последний всегда оканчивается нулем.

Вычислим, например, произведение кодов  $K_i = 0210$  и  $K_j = 3210$ . Имеем

$$K_l = (0210)(3210) = (0210 \rightarrow 1432)3210 = 2341 \rightarrow 1000.$$

Покажем, что множество кодов перестановок конечного ранга  $n$  с введенной выше бинарной операцией образует группу.

Действительно, в качестве единицы  $I$  группы выступает код  $K_1 = 00\dots 0$ . Для любого кода  $K_i$  существует единственный обратный элемент  $K_i^{-1}$  и такой, что

$$K_i \cdot K_i^{-1} = K_i^{-1} \cdot K_i = K_1.$$

Порядок формирования кода  $K_i^{-1}$  отличается от вычисления кода  $K_j$  по перестановке  $M_j$  лишь тем, что на первом этапе определения кода  $K_{i1}^{-1}$  значение  $M_{i1}^{-1}$  вычисляется не по перестановке  $M_1$ , а по перестановке  $M_i$ , соответствующей коду  $K_i$ . На каждом последующем этапе вычисления  $K_{il}^{-1}$  используется соответственно ранее сформулированная перестановка  $M_{i(l-1)}^{-1}$ .

При этом в процессе последовательного вычисления  $K_{il}^{-1}$  из исходной перестановки  $M_i$  строится перестановка  $M_1$ .

Пусть, например, необходимо вычислить обратный код  $K_i^{-1}$  к коду  $K_i = 23110$ . Данному коду соответствует перестановка  $M_i = 32541$ . Проводя вычисления, имеем

$$K_{i1}^{-1} = 40000 M_{i1}^{-1} = M_i \cdot K_{i1}^{-1} = 13254$$

$$K_{i2}^{-1} = 01000 M_{i2}^{-1} = M_{i1}^{-1} \cdot K_{i2}^{-1} = 12543$$

$$K_{i3}^{-1} = 00200 M_{i3}^{-1} = M_{i2}^{-1} \cdot K_{i3}^{-1} = 12354$$

$$K_{i4}^{-1} = 00010 M_{i4}^{-1} = M_{i3}^{-1} \cdot K_{i4}^{-1} = 12345.$$

Итак, имеем  $K_i^{-1} = 41210$ , которому соответствует перестановка  $M_i^{-1} = 52143$ . Нетрудно убедиться, что  $K_i \cdot K_i^{-1} = K_i^{-1} \cdot K_i = K_1 = 00000$ .

Бинарная операция, заданная (2), является ассоциативной, поскольку она однозначно отображает множество всех кодов перестановок в себя.

Таким образом, множество всех кодов перестановок с бинарной операцией (2) является группой, поскольку оно удовлетворяет всем аксиомам группы.

Коды перестановок при задании группы далее выступают в качестве ее образующих.

Под *порядком* кода  $K_i$  далее понимаем степень, в которую необходимо возвести этот код, чтобы получить код  $K_1$  (единицу группы). Единицу группы далее обозначаем нулями (кодом  $K_1$ ) или для краткости символом « $I$ ».

Имеет место следующая теорема.

**Теорема 2.** Два кода перестановок  $K_i$  и  $K_j$  одного и того же ранга  $n$  с бинарной операцией (2) задают конкретную конечную группу и для любой, некоторым образом заданной конечной группы, найдется хотя бы одна пара кодов перестановок, которыми она определяется.

Проведем вначале доказательство первой части теоремы. Действительно, любая конечная группа может быть задана двумя образующими, как подгруппа симметрической группы [1]. При задании двух кодов перестановок отпадает необходимость в задании определяющих соотношений группы, поскольку в силу конструктивности образующих все они получаются автоматически при перемножении различных степеней кодов  $K_i$  и  $K_j$  в соответствии с операцией (2). По этой причине все возможные произведения  $K_i$  и  $K_j$  можно формально рассматривать в качестве определяющих соотношений группы. Поскольку бинарная операция (2) удовлетворяет аксиомам группы, а для ранга « $n$ » число всех кодов конечно и не превосходит  $n!$ , то все произведения возможных степеней кодов  $K_i$  и  $K_j$  образуют конечную группу. При этом если оба кода  $K_i$  и  $K_j$  равны  $K_1$ , то группа будет представлена одним единичным элементом. Если хотя бы один из кодов будет равен  $K_1$ , то группа будет циклической.

Докажем вторую часть теоремы.

Всякая подгруппа симметрической группы может быть порождена двумя подстановками, записанными в виде классических транспозиций. Между процедурой транспозиции и процедурой образования перестановок с использованием операции (2) можно установить соответствие, дающее одну и ту же перестановку. Каждой перестановке соответствует один единственный код. Следовательно любая подгруппа симметрической группы может быть задана двумя кодами. Поскольку построенная некоторым образом группа конечна, то найдется симметрическая группа конечного порядка, в которой эта группа будет подгруппой.

Теорема доказана полностью.

Совершенно очевидно, что в формулировке теоремы 1 фразу «два кода перестановки» можно заменить словами «два целых положительных числа».

Заметим также, что требование совпадения рангов кодов в формулировке теоремы является принципиальным. Нельзя, например, перемножать коды 010 и 1000, а допустимо умножить 0010 на 1000. Это вызвано необходимостью использования для перестановок одного и того же исходного набора натуральных чисел. Данное требование можно исключить, если циклические сдвиги рассматривать в некоторой неограниченной последовательности натуральных чисел. Однако при письме слева–направо возникают неудобства, связанные с необходимостью осуществлять сдвиг справа–налево, либо писать числа справа–налево. В первом случае, например, коду 1000 будет соответствовать перестановка вида 4-1-2-3-5-6..., а во втором – ...6-5-3-2-1-4. Далее используются описанные ранее конструкции. При этом в паре кодов можно опустить лишние левые нули, например, вместо кодов 0100 и 0200 использовать коды 100 и 200, поскольку результат перемножения от этого не изменится.

Вполне естественно, что одна и та же группа может быть задана различной парой кодов и, как увидим далее, даже в рамках одной и той же симметрической группы.

Приведем примеры задания конечных групп с помощью кодов. Любая симметрическая группа может быть задана парой кодов 000...010 и 100...00, группа кварternионов – кодами 10041000 и 42542210, а группа икосаэдра – 10000 и 01210. Легко проверить, что приведенное задание указанных групп соответствует следующему заданию этих же групп в абстрактных образующих:

$$a^n = b^2 = (ab)^{(n-1)} = I, \quad (3)$$

$$a^4 = b^4 = (ab)^4 = I, \quad (4)$$

$$r^5 = f^2 = (rf)^3 = I. \quad (5)$$

#### Способ построения конечной группы

Пусть некоторая конечная группа, заданная двумя абстрактными образующими  $f$  и  $r$ , представлена в виде таблицы умножения. При этом считаем, что внутренние элементы таблицы записаны не в окончательном после использования определяющих соотношений группы виде, а только в виде произведений элементов верхней строки и левого столбца. В этом случае используются лишь соотношения вида

$$f^\alpha = I, r^\beta = I. \quad (6)$$

Указанную таблицу умножения группы далее называем *первообразной таблицей группы*. Первообразная таблица кроме элементов верхней строки содержит конечные слова, составленные из различных степеней образующих  $f$  и  $r$ .

Сделаем заготовку для трех верхних строк первообразной таблицы умножения группы в виде прямоугольной табл. 1.

Таблица 1

Заготовка для трех строк первообразной таблицы группы

$I$	$f$	$r$	...	...	...	...	...	...
$f$	...	...	...	...	...	...	...	...
$r$	...	...	...	...	...	...	...	...

В левом верхнем углу табл. 1 стоит единица, во второй и третьей позиции первой строки и первого столбца записаны образующие группы.

Далее путем умножения первой образующей  $f$  на элементы верхней строки начинаем заполнять вторую строку табл. 1. Элементы, полученные после умножения с использованием соотношений (6) и отсутствующие в верхней строке табл. 1, последовательно вносятся в эту строку. При этом в процессе заполнения второй строки таблицы образующая  $f$  умножается также и на вновь появившиеся в верхней строке элементы до тех пор, пока процесс образования новых элементов прекратится. Этот момент обязательно наступит, так как используются соотношения (6), и в этом случае верхняя строка по числу заполненных клеток сравняется со второй строкой.

После этого аналогичным образом заполняется строка образующей  $r$  и также вновь полученные и отсутствующие в верхней строке элементы вносятся в нее. После того как процесс образования новых элементов прекратится, возвращаемся к строке с образующей  $f$ , и т. д. вплоть до выполнения некоторого ограничительного условия.

Приведенная операция по заполнению указанных трех строк первообразной таблицы далее называется *развертыванием* образующих. Заполнение одной из строк для  $f$  или  $r$  табл. 1 называем *шагом развертывания*.

Докажем следующую лемму.

**Лемма 1.** Совокупность всех элементов первообразной таблицы умножения конечной группы, заданной двумя образующими, может быть получена за конечное число шагов развертывания.

Действительно, поскольку в качестве множимого поочередно выступают образующие  $f$  и  $r$  (в первой степени) и используются соотношения (6), то за достаточно большое число шагов развертывания можно сформировать слово любой заданной структуры первообразной таблицы. Естественно, что в процессе развертывания будут получены и другие лишние слова.

Построим для примера таблицу развертывания образующих группы диэдра  $D_3$ . Для нее

$$f^2 = I, r^3 = I. \quad (7)$$

Первообразная таблицы  $D_3$ , построенная в [2], включает восемнадцать элементов:  $I, r, r^2, f, fr, fr^2, rf, rfr, rfr^2, r^2f, r^2fr, r^2fr^2, frf, frfr, frfr^2, fr^2f, fr^2fr, fr^2fr^2$ .

Таблица развертывания образующих группы  $D_3$  представлена табл. 2.

Таблица 2

Таблица развертывания образующих группы  $D_3$

$I$	$f$	$r$	$fr$	$rf$	$r^2$	$rfr$	$r^2f$	$r^2fr$	$frf$	$fr^2$	$frfr$
$f$	$I$	$fr$	$r$	$frf$	$fr^2$	$frfr$	$fr^2f$	$fr^2fr$	$rf$	$r^2$	$rfr$
$r$	$rf$	$r^2$	$rfr$	$r^2f$	$I$	$r^2fr$	$f$	$fr$	$rfrf$	$rfr^2$	$rfrfr$
$fr^2f$	$fr^2fr$	...	$rfr^2$	...	$r^2fr^2$	...	$frfr^2$	...	$fr^2fr^2$	...	$fr^2fr^2$
$r^2f$	$r^2fr$	...	$frfr^2$	...	$fr^2fr^2$	...	$rfr^2$	...	$r^2fr^2$	...	$r^2fr^2$
$rfr^2f$	$rfr^2fr$	...	$r^2fr^2$	...	$rfr^2fr^2$	...	$rfrfr^2$	...	$fr^2$	...	$fr^2$

С целью уменьшения размеров табл. 2 развертывание ее образующих проведено лишь до того момента, когда указанные выше восемнадцать элементов появились лишь в верхней строке таблицы.

Докажем следующую теорему.

**Теорема 3.** Все элементы конечной группы, заданной двумя кодами перестановок, могут быть получены с использованием бинарной операции (2) за конечное число шагов развертывания.

Доказательство. Поскольку коды заданы, то однозначно заданы образующие соотношения вида (6), которые получаются путем возведения кодов в степень. В соответствии с теоремой 2 пара кодов задает конечную группу, а значит, для нее существует первообразная таблица группы. По вышеприведенной лемме 1, применяя операцию развертывания кодов (образующих), можно за конечное число шагов получить все элементы первообразной таблицы. Если в процессе развертывания образующих сразу применять бинарную операцию (2) по всем получающимся кодам, а не только к соотношениям (6), то сразу получим в окончательном виде три первых строки таблицы Кэли, каждая из которых содержит полный набор элементов группы.

Теорема доказана.

Далее употребляем понятные по смыслу словосочетания *развертывание группы* и *таблица развертывания группы*. Для примера проведем развертывание группы  $D_3$ . Эта группа задается двумя кодами: 010 и 100. Таблица развертывания этой группы представлена табл. 3.

Таблица 3

Таблица развертывания группы  $D_3$

000	010	100	210	110	200
010	000	210	100	200	110
100	110	200	010	210	000

Анализ таблицы показывает, что действительно во всех трех строках таблицы присутствует полный набор элементов группы  $D_3$ .

Заметим, что все вышеприведенные построения с равным успехом можно было применить к трем первым столбцам таблицы умножения группы. Отметим также, что несмотря на «конструктивность» способов задания и формирования конечных групп, построенные группы, тем не менее, сохраняют все свойства абстрактных групп.

#### Разрешимость основных проблем теории групп в конечных группах

Неразрешимость указанных во введении проблем доказана посредством построения групп с использованием конечного числа абстрактных образующих и определяющих соотношений, для которых соответствующие проблемы неразрешимы. При этом используется результат Поста, в котором утверждается, что существует система «продукций», для которых нет алгоритма, позволяющего для любых двух слов указать, равны они в этой системе продукций или нет.

Для конечных групп, заданных кодами перестановок, основные проблемы теории групп (такие как проблемы эквивалентности, тождества и сопряженности слов в группе) тривиально разрешимы. Их разрешимость сформулируем в виде следствий из соотношения (2) и теорем 2 и 3.

Слова  $W_1$  и  $W_2$  группы  $W$  называются эквивалентными (равными), если будучи различными по написанию они представляют один и тот же элемент.

Проблема эквивалентности слов заключается в отыскании алгоритма, который за конечное число шагов устанавливает эквивалентны или нет любые два слова группы. При такой формулировке проблемы никаких ограничений на сам алгоритм не накладывается.

**Следствие 1.** Проблема эквивалентности слов в конечной группе разрешима.

Действительно, последовательно применяя операцию (2) к словам составленным из кодов (образующих) в конце концов получим ответ на поставленный вопрос.

Проблема тождества слов является частным случаем проблемы эквивалентности и формулируется следующим образом [1]: нужно найти алгоритм, который позволил бы для любой группы, заданной конечным числом образующих и соотношений, в конечное число шагов ответить на вопрос, равно ли единице некоторое данное слово в этих образующих, или же доказать, что такой алгоритм не может существовать.

Сама проблема возникла, видимо, из того, что проблему эквивалентности слов предлагалось решать путем преобразования слова  $W_2$  в  $W_1$  вычеркиванием в первом из них слова, равного  $I$ .

**Следствие 2.** Проблема тождества слов в конечной группе разрешима.

Алгоритм решения проблемы остается тем же, что и при установлении эквивалентности слов.

В связи со следствием 1 проблему сопряженности слов можно свести к проблеме сопряженности элементов группы.

Элементы  $a$  и  $b$  группы  $G$  называются *сопряженными* в этой группе, если в  $G$  можно найти хотя бы один такой элемент  $g$ , что

$$b = g^j a g. \quad (8)$$

Умножая обе части выражения (8) слева на  $g$ , получим:

$$gb = ag. \quad (9)$$

Проблема сопряженности элементов группы, следовательно, сводится к ответу на вопрос: найдется ли для двух элементов  $a$  и  $b$  такой элемент  $g$ , чтобы выполнялось равенство (9)?

**Следствие 3.** Проблема сопряженности слов в конечной группе разрешима.

Действительно, если конечная группа задана двумя кодами, то сформировав путем развертывания ее элементы и подставляя в (9) вместо элемента  $g$  все другие элементы кроме самих элементов  $a$  и  $b$ , за конечное число шагов получим ответ на поставленный вопрос.

Группа считается *простой*, если она не имеет собственных нормальных подгрупп. Проблема установления простоты подгруппы сводится к отысканию алгоритма, который за конечное число шагов дает ответ на вопрос: является ли хотя бы одна из подгрупп группы нормальным делителем?

**Следствие 4.** Если для группы  $G$  известны все ее подгруппы, то проблема установления простоты конечной группы разрешима.

Для ответа на вопрос о простоте группы достаточно для каждой из подгрупп группы, используя бинарную операцию (2), сформировать ее левые и правые смежные классы. Если ни для одной из подгрупп эти классы не совпадают, то группа является простой.

Прямым вычислением решаются и другие частные задачи. Например, для того чтобы вычислить левый или правый неизвестный множитель в уравнениях типа

$$xa = b, ax = b$$

достаточно представить их в виде

$$x = ba^{-1}, x = a^{-1}b$$

и далее в соответствии с вышеизложенным алгоритмом необходимо вычислить обратный элемент  $a^{-1}$  и произвести вычисления.

Проблема изоморфизма двух групп сводится также к отысканию алгоритма, который за конечное число шагов позволяет установить: изоморфны эти группы или нет? Для конечных групп эта проблема разрешима.

**Теорема 4.** Проблема изоморфизма двух конечных групп разрешима.

Приведем алгоритм, который за конечное число шагов позволяет установить: изоморфны или нет две группы, заданные таблицами Кэли с помощью абстрактных образующих?

Две группы  $G$  и  $G'$ , имеющие одинаковое число элементов с заданными в них бинарными операциями  $f$  и  $f'$  далее считаются изоморфными, если существует однозначное отображение элементов группы  $G$  на элементы группы  $G'$ , и такое, что для любых элементов группы  $G$   $a, b, c, d$  выполняются равенства  $f(ab) = c, f(ba) = d$ , то для поставленных им в соответствие четырех элементов  $a', b', c'$  и  $d'$  группы  $G'$  имеют место равенства  $f'(a'b') = c'$  и  $f'(b'a') = d'$ . При этом если  $c = d$ , то и  $c' = d'$ .

Пусть для групп  $G$  и  $G'$  порядка  $n$  заданы таблицы Кэли. Если единица  $I$  группы первой строки занимает не самую левую позицию, то путем преобразования таблицы переместим ее в это положение.

Пронумеруем элементы верхней строки и первого столбца таблицы группы  $G$  натуральными числами  $1, 2, \dots, n$ . Используя далее таблицу умножения группы  $G$ , построим для нее латинский квадрат стандартного (редуцированного) вида [10] и обозначим его через  $L_0$ . Все позиции этого квадрата будут заполнены числами из промежутка  $1, 2, \dots, n$ . Для установления изоморфизма групп  $G$  и  $G'$  далее начинаем формировать все возможные латинские квадраты  $L_i$  стандартного вида для группы  $G$  и сравнивать их с квадратом  $L_0$ . Максимально возможное число таких квадратов равно  $(n - 1)!$ . Все они формируются на основе упорядоченного набора элементов верхней строки таблицы группы  $G$ , который принимается за исходную начальную перестановку. Формирование всей совокупности перестановок осуществляется с помощью возрастающей последовательности кодов перестановок вида  $000\dots 00, 000\dots 010, 00\dots 100, \dots, (n - 1)(n - 2)\dots 210$  и ничем не отличается от вышеизложенного. Каждый перестановке будет соответствовать свой латинский квадрат группы  $G$ . Очевидно, что группы  $G$  и  $G'$  будут изоморфны лишь в том случае, если найдется латинский квадрат  $L_j$ , тождественно равный (т. е. являющийся копией) квадрату  $L_0$ . В противном случае группы будут не изоморфными.

Другими словами, достаточным критерием изоморфизма двух групп  $G$  и  $G'$  одинакового порядка является наличие такого соответствия между элемента-

ми группы, стандартные латинские квадраты которых являются тождественно равными. Существование алгоритма формирования латинских квадратов, который был описан выше, доказывает справедливость теоремы 4.

Принципиальной в приведенном алгоритме является процедура формирования перестановок, хотя сам критерий изоморфизма – тождественность латинских квадратов – является вполне естественным.

Рассмотрим пример установления изоморфизма двух групп, заданных для простоты кодами перестановок, приведенных в табл. 4 вместе с порядковыми номерами, которые им присвоены. Нижние индексы кодов далее используются для формирования перестановок из элементов.

Таблица 4

*Элементы группы G*

000 <sub>1</sub>	110 <sub>2</sub>	200 <sub>3</sub>	100 <sub>4</sub>	210 <sub>5</sub>	010 <sub>6</sub>
1	2	3	4	5	6

Таблица 5

*Элементы группы G'*

0000	0110	1200	2100	1010	2210
1	2	3	4	5	6

Элементы группы  $G'$  представлены в табл. 5. Используя бинарную операцию (2), построим таблицы Кэли для данных групп и затем в соответствии с присвоенными им в табл. 4 и 5 номерам построим по таблицам Кэли стандартные латинские квадраты. Исходные латинские квадраты  $L$  и  $L'$  для групп  $G$  и  $G'$  представлены табл. 6 и 7 соответственно.

Таблица 6

*Латинский квадрат  $L_1$  группы G*

1	2	3	4	5	6
2	1	5	6	3	4
3	6	4	1	2	5
4	6	4	1	2	5
5	4	6	2	1	3
6	3	2	5	4	1

Таблица 7

*Латинский квадрат  $L'_1$  группы G'*

1	2	3	4	5	6
2	1	4	3	6	5
3	5	1	6	2	4
4	6	2	5	1	3
5	3	6	1	4	2
6	4	5	2	3	1

Из сравнения латинских квадратов  $L_1$  и  $L'_1$  видно, что они различны. Это означает, что если элементы группы  $G$  отобразить на элементы группы  $G'$  в соответствии с табл. 6 и 7, то изоморфизм не выполняется. Например, произведение элемента 2 на элемент 3 в группе  $G$  дает 5, а в группе  $G' - 4$ .

Для дальнейшей проверки групп  $G$  и  $G'$  на предмет их изоморфизма будем в табл. 4 группы  $G$  производить перестановки ее элементов, формировать латинские квадраты и сравнивать их с квадратом  $L_1$ . Допустим, что сформирован код 040000, которому соответствует перестановка 162345. Этой перестановке соответствует отображение элементов группы  $G$  на числа 1–6, имеющие вид табл. 8.

Таблица 8  
Таблица расположения элементов группы  $G$  для кода 040000

000 <sub>1</sub>	010 <sub>6</sub>	110 <sub>2</sub>	200 <sub>3</sub>	100 <sub>4</sub>	210 <sub>5</sub>
1	2	3	4	5	6

Если теперь для соответствия элементов, заданного табл. 8, построить латинский квадрат, то он в точности будет повторять латинский квадрат  $L_1$ , приведенный в табл. 7. Следовательно группы  $G$  и  $G'$  изоморфны. Конечно, это была умышленная заготовка изоморфного представления ранее построенной (хотя и в другом представлении) группы диэдра  $D_3$  (табл. 3) группой  $G$ , таблица развертывания которой представлена табл. 9.

Таблица 9

Таблица развертывания группы  $G'$

0000	0110	1200	2100	1010	2210
0110	0000	2100	1200	2210	1010
1200	1010	0000	2210	0110	2100

Практическое использование критерия изоморфизма в виде тождественности латинских квадратов групп требует большого объема вычислений. Возникает вопрос: могут ли быть более простые критерии? Ответ на этот вопрос утвердительный.

Пусть некоторая конечная группа представлена своей таблицей развертывания. По аналогии с латинским квадратом будем говорить для нее о трехстрочечном стандартном латинском прямоугольнике. Под расширением латинского прямоугольника группы далее понимаем строки латинского квадрата, построенного из той же группы, что и прямоугольник. Докажем следующую лемму.

**Лемма 2.** Группы  $G$  и  $G'$ , имеющие тождественно равные стандартные латинские прямоугольники, имеют тождественно равные расширения.

**Доказательство.** Тождественность латинских прямоугольников групп означает, что в процессе развертывания их таблиц каждый шаг развертывания группы  $G'$  в точности повторяет шаг развертывания группы  $G$ . Дополнив первые столбцы латинских прямоугольников групп симметрично первой строке и проведя перемножения элементов, получим таблицы Кэли для групп. Переведем далее таблицы Кэли в латинские квадраты. Необходимо доказать, что для дополнительно построенных произведений элементов групп  $a_i \cdot a_j$  (где  $i = \overline{4, n}, j = \overline{1, n}$ ,  $n$  – порядок группы) будет соблюдаться тождественность номеров элементов в латинских квадратах групп. Действительно, в силу доказанной выше леммы 1 при построении таблицы развертывания группы, когда используются только образующие соотношения (6), все произведения элементов типа  $a_i \cdot a_j$  для  $i \geq 4$  в явном виде присутствуют в этой таблице. Если же используются другие определяющие соотношения группы, то указанные произведения присутствуют в таблице развертывания группы в неявном виде. Если бы произведения указанных элементов для  $i \geq 4$  порождали различные структуры шагов развертывания в группах  $G$  и  $G'$ , то латинские прямоугольники этих групп были бы различны. По условию же они тождественно равны друг другу, а значит, и расширения их латин-

ских прямоугольников будут тождественно равны друг другу.

Лемма доказана.

Имеет место следующая теорема.

**Теорема 5.** Конечные группы  $G$  и  $G'$ , для которых найдется хотя бы одна пара тождественно равных стандартных латинских прямоугольников, являются изоморфными.

Действительно, в силу леммы 2 тождественно равные латинские прямоугольники имеют тождественно равные продолжения, а следовательно, группы  $G$  и  $G'$  в силу критерия тождественности латинских квадратов изоморфны.

Если учесть, что из двух образующих можно составить всего две перестановки, то при использовании в качестве критерия изоморфизма групп латинских прямоугольников необходимо построить  $2 \cdot C_{n-1}^2 = (n-1) \cdot (n-2)$  таких прямоугольников.

Однако оказывается, что это количество может быть уменьшено. Для этого рассмотрим еще один критерий изоморфизма конечных групп.

При задании конечных групп двумя абстрактными образующими, например  $a$  и  $b$ , часто используют соотношение свободных групп типа

$$(ab)^\gamma = I. \quad (10)$$

При этом сама группа в этом случае задается определяющими соотношениями вида

$$a^\alpha = b^\beta = (ab)^\gamma = I. \quad (11)$$

Поскольку при задании конечной группы кодами перестановок достаточно задать две образующие  $a$  и  $b$ , а все остальные элементы соотношения (11) ( $ab$ ,  $\alpha$ ,  $\beta$ ,  $\gamma$ ) получаются автоматически, то можно использовать очередной критерий изоморфизма двух конечных групп: тождественность «тройки степеней  $\alpha$ – $\beta$ – $\gamma$ ».

Однако здесь возникает вопрос о единственности задания и однозначности представления конкретной конечной группы. На самом деле такое задание конечных групп с помощью соотношений типа (11) не только не единственно, но может быть и неоднозначным.

То, что такое задание группы не единственно легко подтверждается многочисленными примерами с использованием кодов перестановок. Так, например, симметрическую группу  $S_4$  можно задать двумя различными тройками соотношений типа (11):

$$0010^2 = 1000^4 = 1110^3 = I, \quad (12)$$

$$2110^4 = 2100^3 = 3200^4 = I. \quad (13)$$

Эквивалентность заданий группы  $S_4$  соотношениями (12) и (13) нетрудно проверить, построив таблицы развертывания групп.

Примечательно здесь то, что различные пары образующих порождают одно и то же множество элементов группы. Поэтому в отличие от задачи установления изоморфизма групп здесь возникает задача отыскания различных пар кодов перестановок группы, которые их инвариантно задают. Интерес представляет конечно решение, отличное от прямого перебора пар кодов с последующим построением таблицы развертывания группы.

Неоднозначность представления конечной группы соотношениями типа (11) продемонстрируем на следующем примере.

Для группы, являющейся прямым произведением циклических групп  $C_2 \times C_4$ , и с учетом условия коммутативности группы ( $ab = ba$ ) в [2] приведены следующие определяющие соотношения этой группы:

$$a^2 = b^4 = ab a^{-1} b^{-1} = I. \quad (14)$$

Если учесть, что  $a^{-1} = a$ ,  $b^{-1} = b^3$ ,  $b^{-2} = b^2$ , то последнее выражение несложно привести к виду:

$$a^2 = b^4 = (ab)^4 = I. \quad (15)$$

Для тройки степеней «2-4-4» зададим в кодах перестановок следующие две группы

$$000010^2 = 100200^4 = 100210^4 = I, \quad (16)$$

$$20402000^2 = 76541210^4 = 56143210^4 = I. \quad (17)$$

Как нетрудно проверить с помощью таблицы разветвления группы соотношению (16) действительно соответствует коммутативная группа  $C_2 \times C_4$ , содержащая 8 элементов. Соотношение же (17) задает циклическую группу четвертого порядка, являющуюся подгруппой группы кватернионов. В качестве образующей « $a$ » здесь выступает элемент  $K_i = 76541210$ . Аналогичные циклические группы с тройками «2-4-4» получаются в рамках симметрической группы  $S_4$  с образующими  $K_i = 1100$  и  $K_j = 2010$ .

Эти примеры говорят о том, что применять критерий изоморфизма тождественности «тройки степеней» можно только к двум однотипным группам, т. е. группам, являющимся одновременно циклическими, не циклическими, но коммутативными либо, наконец, некоммутативными. К какому типу относится каждая из групп легко определить прямым вычислением, используя два образующих кода перестановок группы.

При использовании последнего критерия изоморфизма групп порядок следования степеней  $\alpha$ ,  $\beta$  и  $\gamma$  в соотношении (11) является принципиальным. Однако следует заметить, что некоторые пары кодов, выступающие в качестве образующих группы, обладают свойством перестановочности степеней. Так, например, группа икосаэдра может иметь следующие определяющие соотношения

$$1000^5 = 01210^2 = 11210^3 = I, \quad (18)$$

$$01210^2 = 11210^3 = 21110^5 = I, \quad (19)$$

$$11210^3 = 01210^2 = 10000^5 = I. \quad (20)$$

Из этих соотношений видно, что тройка степеней «5-2-3» может быть сведена к тройке степеней «2-3-5» и «3-2-5».

Однако, например, для группы  $S_4$ , заданной соотношением (12), при перестановке образующих получим

$$1110^3 = 1000^4 = 3200^4 = I. \quad (21)$$

В итоге вместо тройки степеней «2-4-3» в соотношении (12) получили тройку «3-4-4» в соотношении (21), т. е. степени тройки оказались не перестановочными.

В связи с этим при применении критерия изоморфизма групп по тройке степеней в случае их несовпадения необходимо проверять на возможность их перестановочности или образования новых степеней. Этот критерий необходимо применять одним из первых, и только после этого переходить к критерию тождественности латинских прямоугольников. При этом в случае совпадения числа элементов в анализируемых группах нет необходимости строить все  $(n-1)(n-2)$  латинских прямоугольников. В этом случае для установления изоморфизма двух групп достаточно взять в

качестве исходных два образующих кода одной группы и найти среди элементов другой группы два таких кода перестановок, которые бы обеспечивали совпадение троек степеней обеих групп. Если такая пара кодов во второй группе отыщется, и при проверке окажется, что группы являются однотипными, то группы изоморфны, в противном случае – не изоморфны.

### Некоторые соображения по построению каталога конечных групп

Вышеприведенные построения не составляют принципиальных трудностей для создания каталога конечных групп в некотором разумном объеме. Этот каталог, на наш взгляд, целесообразно строить по принципу вложенных друг в друга симметрических групп, начиная с группы  $S_1$ . Поскольку для каждой из последующих симметрических групп все предыдущие являются ее подгруппами, то все построения каталога можно осуществить в рамках максимально возможной симметрической группы  $S_n$ . Наиболее простым, хотя и весьма трудоемким здесь является способ построения всех подгрупп на основе сочетаний всевозможных пар кодов перестановки группы  $S_n$ . Далее путем применения критериев изоморфизма в виде троек степеней и латинских прямоугольников можно построить все подгруппы группы  $S_n$ . В каталог целесообразно поместить левые тройки соотношений (11), разделенные дефисом, количество элементов группы, данные о ее коммутативности, простоте и др. При этом вносимые в каталог группы целесообразно выражать в кодах минимально возможного ранга.

Продемонстрируем схему заполнения каталога конечных групп на примере симметрической группы  $S_4$ . Коды перестановок ранга «4», их порядок и сами перестановки приведены в табл. 10.

Таблица 10

Перестановки и их коды ранга «4»

$i$	Код перестановки и ее порядок	Перестановка	$i$	Код перестановки и ее порядок	Перестановка
1	0000 <sup>1</sup>	1234	13	2000 <sup>2</sup>	3412
2	0010 <sup>2</sup>	1243	14	2010 <sup>4</sup>	3421
3	0100 <sup>3</sup>	1342	15	2100 <sup>3</sup>	3124
4	0110 <sup>2</sup>	1324	16	2110 <sup>4</sup>	3142
5	0200 <sup>3</sup>	1423	17	2200 <sup>3</sup>	3241
6	0210 <sup>2</sup>	1432	18	2210 <sup>2</sup>	3214
7	1000 <sup>4</sup>	2341	19	3000 <sup>4</sup>	4123
8	1010 <sup>3</sup>	2314	20	3010 <sup>3</sup>	4132
9	1100 <sup>4</sup>	2413	21	3100 <sup>2</sup>	4231
10	1110 <sup>3</sup>	2431	22	3110 <sup>3</sup>	4213
11	1200 <sup>2</sup>	2134	23	3200 <sup>4</sup>	4312
12	1210 <sup>2</sup>	2143	24	3210 <sup>2</sup>	4321

Возможное начало достаточно скромного по информации каталога конечных групп может выглядеть таким, каким оно показано в табл. 11.

В табл. 11 под символом  $S_n$  обозначено множество тех элементов группы, которые не формируются в предыдущих группах. Буквы  $i$ ,  $n$ ,  $a$  обозначают соответственно циклическая, некоммутативная и абелева группы. Циклические группы представлены двумя образующими для того чтобы было видно отличие их троек степеней от других групп, хотя это и не обяза-

тельно. Группы №№1, 2, 3 и 5 табл. 11 являются симметрическими группами  $S_1, S_2, S_3$  и  $S_4$ , а №4 и №6 – знакопеременными группами  $A_2$  и  $A_4$  соответственно, хотя некоторые из них имеют специальные названия [2]. Группа №7 является некоммутативной группой восьмого порядка. В отличие от группы кватернионов она в качестве подгруппы содержит четверную группу (№9). Группа №8 – циклическая группа четвертого порядка. Реально создаваемый каталог должен быть, конечно, намного информативней и кроме других характеристик групп может содержать информацию о первооткрывателях отдельных групп.

Таблица 11

*Возможное начало каталога конечных групп*

№ пп.	Определяющие соотношения группы	Кол-во элементов в группе	Тип группы
1	$S_1$		
	$I-I-I$	1	ц
	$S_2$		
2	$10^2 - I - 10^2$	2	ц
	$S_3$		
3	$010^2 - 100^3 - 210^2$	3!	н
4	$100^3 - 200^3 - I$	3	ц
	$S_4$		
5	$0010^2 - 1000^4 - 1110^3$	4!	н
6	$0100^3 - 1210^2 - 2100^3$	4!/2	н
7	$0010^2 - 2000^2 - 3200^4$	8	н
8	$1000^4 - 3000^4 - I$	4	ц
9	$0010^2 - 1200^2 - 1210^2$	4	а
...	...	...	...

Создаваемый каталог конечных групп может выступать в качестве базового. Пользователи же конечных групп вправе создавать собственные каталоги, в которых группы базового каталога могут быть изоморфно представлены кодами перестановок более высокого ранга. Например, вместо четверной группы №9 в табл. 11 можно использовать изоморфную ей группу с определяющими соотношениями

$$000010^2 = 140000^2 = 140010^2 = I. \quad (22)$$

Переход к кодам перестановок более высокого ранга повышает, в некотором смысле, информационную избыточность элементов группы. Использование

же абстрактных образующих для задания конечных групп обедняет группу как числовую конструкцию. Поэтому имеет право на существование задача разработки способа, позволяющего строить изоморфные группы кодами различных (больших или меньших) рангов. Если учесть, что код перестановки есть своеобразная запись некоторого целого положительного числа, то в более общем виде указанная задача формулируется следующим образом: найти способ, позволяющий из пар целых положительных чисел формировать классы попарно изоморфных друг другу конечных групп. Могут быть и частные, более узкие постановки этой задачи.

Таким образом, задание конечной группы кодами перестановок делает ее достаточно определенной числовой конструкцией, все основные проблемы которой разрешаются прямым вычислением.

### Литература

1. Курош А.Г. Теория групп. – М.: Наука, 1967.
2. Гроссман Н., Магнус В. Группы и их графы. – М.: Мир, 1971.
3. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. – М.: Наука, 1977.
4. Новиков П.С. Об алгоритмической неразрешимости проблемы тождества слов в теории групп // Тр. матем. института АН СССР. – 1955. – Т. 44.
5. Новиков П.С. Неразрешимость проблемы сопряженности в теории групп // Изв. АН СССР. Сер. Матем. – 1954. – Т. 18.
6. Адян С.И. Неразрешимость некоторых алгоритмических проблем теории групп. // Тр. моск. матем. о-ва. – 1957. – Т. 6.
7. Машины Тьюринга и рекурсивные функции / Г.-Д. Эббинхаус, К. Якобс, Ф.-К. Манн и др. – М.: Мир, 1972.
8. Клини С.К. Введение в математику. – М.: ИЛ, 1957.
9. Голиков В.П. Рациональный алгоритм вычисления значений функции распределения простых чисел // Двойные технологии. – 2003. – №4.
10. Математическая энциклопедия. – М.: Советская энциклопедия, 1982. – Т. 3.