УДК 5919.41.46

© Голиков В.П.
Golikov V.

КОНСТРУКТИВНЫЙ СПОСОБ ПОСТРОЕНИЯ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП

CONSTRUCTIVE METHOD FOR BUILDING OF FINITE ABEL'S GROUPS

Аннотация. *Предложен способ построения конечных абелевых групп с использованием эффективных номеров перестановок.*

Annotation. *Method for building of finite Abel's groups used effective numbers of permutations were offered.*

Ключевые слова. *Теория групп, множество элементов, конструктивный способ, абелевы группы, арифметические операции.*

Key words. *The theory of groups, many elements, constructive way, Abelian groups, the arithmetic operations.*

Введение

В математике группа определяется как множество элементов (конечное или бесконечное) с заданной в нем бинарной операцией и такое, что в нем выполняются аксиомы ассоциативности, о единичном и обратных элементах [1...3].

Теория групп, начало которой положено работами Эвариста Галуа, вначале применялась в математике, а затем открылись её прикладные возможности в механике, квантовой физике, кристаллографии и информатике.

Группы делятся на конечные и бесконечные, коммутативные и некоммутативные группы. Коммутативные группы называют также абелевыми группами в честь норвежского математика Абеля, который в 1824 г. доказал, что общее алгебраическое уравнение с одним неизвестным степени выше четвертой не разрешимо в радикалах, т.е. не существует формулы, выражающей корни такого уравнения через коэффициенты с помощью арифметических операций и радикалов.

Конечная группа может быть задана при помощи таблицы умножения (таблицы Кэли), образующих и определяющих соотношений, а также с помощью графической схемы (сети). Группа, заданная одним из указанных выше способов, может быть изоморфно представлена группой подстановок [1...3]. При задании конечной группы с помощью подстановок отпадает необходимость в дополнительном задании определяющих соотношений, поскольку подстановки являются конструктивным образующими в отличие от абстрактных образующих, для которых в силу алгебраического подхода определяющие соотношения обязательны.

Конечная абелева группа может быть задана посредством прямого произведения циклических групп. При использовании только двух абстрактных образующих «a» и «b», каждая из которых задает циклические группы G_m и G_n, соответственно определяющие соотношения группы $G_{m\times n}=G_m \times G_n$ имеют следующий вид:

$$a^m = I; \quad (1)$$

$$b^n = I; \quad (2)$$

$$a \cdot b \cdot a^{-1} \cdot b^{-1} = I; \quad (3)$$

или $$a^m = b^n = a \cdot b \cdot a^{-1} \cdot b^{-1} = I, \quad (4)$$

где I – единица группы.

Соотношение (3) отражает свойство коммутативности группы

$$a \cdot b = b \cdot a. \quad (5)$$

Хотя формула (4) является общим определяющим соотношением для конечной абелевой группы, тем не менее иногда [2] выражение (3), входящее в формулу (4),

Голиков Василий Петрович – доктор технических наук, профессор, ведущий научный сотрудник 4 Центрального НИИ Министерства обороны РФ, тел. (495)543-76.

Golikov Vasiliy – doctor of science (Technical), professor, senior researcher of 4th Central Institute of Russian Federation Defence ministry, tel. (495)543-76.

путем алгебраических преобразований сводится к некоторой степени произведения $a \cdot b$, т.е. к виду $(a \cdot b)^l$. Для конечных абелевых групп такое преобразование не обязательно, поскольку вся совокупность элементов группы для двух и более образующих ($K_1, K_2, ..., K_\xi$) получается путем непосредственного перемножения совокупностей элементов циклических групп с использованием сочетаний по одному, по два и т.д. элементов в каждом произведении. При этом общее число элементов группы N_0 с учетом единицы группы вычисляется по формуле

$$N_0 = \prod_{i=1}^{\xi} K_i, \qquad (5а)$$

где П – знак произведения.

Справедливость формулы (5а) доказывается путем ввода переменной $K = K_i - 1$ и представлением формулы в виде

$$N_0 = (K+1) \cdot (K+1) \cdot ... \cdot (K+1). \qquad (5б)$$

После раскрытия формулы (5б) получается сумма слагаемых, в точности количественно повторяющая слагаемые всевозможных произведений элементов циклических групп.

В практических приложениях иногда требуется, чтобы элементы конечной абелевой группы были представлены в виде чисел. Наиболее просто эта задача может быть решена путем нумерации абстрактных элементов конечной абелевой группы и представления её в виде таблицы Кэли. Однако при таком подходе в общем случае может не выполняться свойство численной аддитивности элементов абелевых групп.

Более корректно указанная задача может быть решена путем нумерации элементов конечной абелевой группы, заданной в виде подстановок (перестановок) в рамках симметрической группы. Способы специальной нумерации перестановок (из их числа n!) и задания группы на этих номерах (кодах перестановок) предложены нами в статье [4].

Хотя в указанной статье приводятся примеры построения как некоммутативных, так и коммутативных групп на основе номеров перестановок задача построения произвольных конечных абелевых групп в статье не ставилась и не решалась.

Ниже предлагается способ построения конечных абелевых групп на основе кодов перестановок, в максимальной степени отражающий свойство численной аддитивности элементов этих групп.

Основы способа построения конечной группы

В основу способа построения конечной абелевой группы положен способ, предложенный нами для построения произвольной конечной группы и изложенный в статье [4]. Указанный способ основан на эффективной нумерации (гёделизации) перестановок. Номер (код) перестановки записывается в виде специальной линейно возрастающей от разряда к разряду системе счисления. Первый (младший правый) разряд произвольного кода всегда равен нулю, второй – нулю или единице и т.д.

При этом для записи числа в каждом разряде кода используется десятичная система счисления. Перестановки и их коды формируются на основе вложенных друг в друга циклов, в отличие от традиционного способа построения подстановок, основанного на независимых циклах. Предложенный способ обеспечивает единственность (однозначность) построения перестановки по её коду, и наоборот.

Все перестановки строятся из натурального ряда чисел 1–2–3–...–n (первой перестановки M_1), которому соответствует код 0–0–0–...– 0 (код K_1). Построение произвольной перестановки по её коду из перестановки M_1 начинается с реализации вначале числа циклических сдвигов самого старшего разряда кода, затем очередного разряда и так вплоть до $n-1$-го, поскольку последний младший разряд всегда нулевой. В связи с тем, что в приводимых ниже построениях числа разрядов перестановок и кодов не превосходят числа «9», то разделительные знаки «–» далее опускаем.

Так, например, коду $K_j = 32210$ соответствует перестановка $M_j = 41532$.

Переход от перестановки M_j к коду K_j производится в обратном порядке. Вначале берется число первой позиции перестановки M_j, и это число отыскивается в перестановке M_1. Далее подсчитывается, на сколько позиций необходимо сдвинуть это число в M_1, чтобы оно оказалось в ней на первой (левой) позиции. Полученное количество позиций заносится вместо нуля в старший разряд K_1 и таким образом получается код $K_i^{(1)}$. После этого из перестановки M_1 по коду $K_i^{(1)}$ формируется перестановка $M_i^{(1)}$. Далее выбирается число второй позиции M_j, отыскивается теперь уже в $M_i^{(1)}$ и подсчитывается, как и ранее, на сколько позиций необходимо его сдвинуть, чтобы оно оказалось на второй позиции $M_i^{(1)}$. Подсчитанное количество позиций заносится во вторую позицию $K_i^{(1)}$. В результате получаем код $K_i^{(2)}$ и так далее, пока не будет сформирован весь код K_i.

Используя вышеприведенный алгоритм, нетрудно убедиться, что перестановке $M_i = 51324$ соответствует код $K_i = 40110$.

Конечная группа задается на кодах перестановок одинакового ранга, т.е. содержащих одно и то же число

разрядов при этом выравнивание этого числа в кодах осуществляется добавлением дополнительных нулей в старшие разряды соответствующего кода. Например, исходные коды перестановок ранга 3 и 4 – K_1 = 010 и K_2 = 2110 при выравнивании их рангов будут иметь следующий вид: K_1 = 0010, K_2 = 2110.

Бинарная операция, используемая для построения конечной группы, задается на кодах перестановок одинакового ранга по следующему правилу: произведению кода K_i на код K_j соответствует код K_l, который получается циклическим сдвигом перестановки M_i кодом K_j и переводом полученной перестановки в код K_l. В формализованном виде эта операция записывается следующим образом:

$$K_i \cdot K_j = (K_i \rightarrow M_i) \cdot K_j = M_l \rightarrow K_l, \qquad (6)$$

где «·» – знак бинарной операции;

«→» – процедура перевода кода в перестановку, и наоборот.

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

K_l = (0210) · (3210) = (0210 · 1432) · 3210 = 2341 · 1000.

Порядком, когда K_i далее называем степень, в которую необходимо возвести этот код, чтобы получить единицу группы, т.е. K_1 = 0 – 0 – 0 –...– 0.

Другая дополнительная информация о данном способе построения конечных групп содержится в статье [4].

Способ построения конечных абелевых групп

Способ построения конечных абелевых групп, реализуемый в виде формулы (конструкции), разрабатывается ниже в два этапа. На первом этапе предлагается и подробно описывается способ построения конечных абелевых групп с использованием только двух циклических образующих. На втором этапе рассматривается более общий случай.

Первый этап, в свою очередь, включает два подэтапа. На первом подэтапе предлагается способ построения исходных данных формул для конечных абелевых групп, степени образующих которых одинаковы, т.е. формул для групп типа

$$G_{m\times m} = C_m^{(1)} \times C_m^{(2)}, \qquad (7)$$

где $C_m^{(1)}$ и $C_m^{(2)}$ левая и правая образующие циклических групп m-го порядка, а на втором подэтапе – с использованием формул типа

$$G_{m\times(m+n)} = C_m^{(1)} \times C_{m+n}^{(2)}, \qquad (7a)$$

где n = 1, 2, ...

Необходимость в идентификации образующих $C^{(1)}$ и $C^{(2)}$ связана, как увидим ниже, с различием способов их построения.

Прежде чем построить конструктивную формулу для группы $G_{m\times m}$, сформулируем в виде предложений ряд утверждений.

Предложение 1. Код K_i перестановки, содержащий единицу в l-м разряде (l = 2, 3, ..., K) при счете справа налево, а во всех остальных разрядах, независимо от их количества – нули имеет порядок, равный l.

Справедливость данного предложения вытекает из способа построения кодов перестановки и бинарной операции умножения кодов.

Например, порядок K_i = 010 равен двум, т.е. 010^2 = = 000, так как (010 → 132) · 010 = 123 → К1 = 000.

Порядок кода K_i = 100 равен трем, кода K_i= =001000 – четырем и т.д.

Указанный в *Предложении* 1 код K_i далее называем моноединичным кодом и обозначаем в виде $K_{il}(l)$, где i – номер кода, l – номер разряда, в котором стоит единица.

Первая исходная перестановка M_1 далее называется четной, если она содержит четное число разрядов (чисел). Например, перестановки M_1 = 1·2, M_1 = 1·2·3·4 и т.д. являются четными исходными перестановками.

Пусть задана первая четная перестановка M_1 = 1 – –2 – 3 – ... – K (K = 4, 6, ...), соответствующая коду K_1 (единице группы). Выясним, какой код соответствует перестановке M_l, полученной из перестановки M_1, в которой произведен один циклический сдвиг относительно числа самого старшего разряда (единицы) в совокупности её только ξ старших разрядов, при условии, что ξ = К/2. Другими словами, необходимо установить код для перестановки, имеющий, например, вид M_i = 23415678, в которой циклический сдвиг на одно число произведен в перестановке M_1 в первых четырех старших разрядах (ξ = 8/2 = 4).

Перестановку M_l, полученную из четной перестановки M_1 = 1 – 2 – ... – K и имеющей один циклический сдвиг в совокупности ξ = К/2 старших разрядов далее обозначим через M_i(К/2).

Предложение 2. Перестановке M_i(К/2) соответствует код K_i = 100 ... ξ ... 00 ... 0, где число ξ кода размещается в точности на ξ = К/2-й позиции при счете слева направо.

Действительно, при умножении четной перестановки M_1 на код K_i = 100 ... 0 число «1» перестановки вследствие циклического сдвига перемещается на последнюю её позицию, т.е. получается перестановка типа M_j = 234...K_1. Для того, чтобы переместить эту единицу на ξ-ю позицию, равную К/2, необходимо перестановку M_j умножить на код K_ξ = 00 ... 0ξ00... 0. Например, для M_1 =123456 перестановка M_i(6/2) имеет вид M_i = 131756.

Этой перестановке, как нетрудно убедиться, соответствует код $K_i = 103000$.

Минимальная по числу разрядов перестановка типа $M_i(K/2)$ имеет вид $M_i(4/2) = 2134$, которой соответствует код $K_i = 1200$. Код перестановки $M_i(K/2)$ далее обозначается через $K_i(K/2)$.

Предложение 3. Порядок кода $K_i(K/2)$ перестановки $M_i(K/2)$ в точности равен числу $K/2$.

Другими словами, при возведении кода $K_i(K/2)$ в степень через $K/2$ шагов получается код $K_1 = 000...0$ (единица группы).

Действительно, в перестановке $M_i(K/2)$, построенной по коду Ki(K/2), первая половина чисел до $K/2$ включительно отличается от этих же чисел первой четной перестановки M_1 лишь тем, что она имеет один циклический сдвиг по старшему разряду. Вторая же половина чисел (после разряда $K/2$) в перестановке $M_i(K/2)$ не изменяется и в точности совпадает с числами перестановки M_1.

При возведении кода $K_i(K/2)$ в квадрат в первой половине чисел перестановки $M_i(K/2)$ осуществляется второй циклический сдвиг относительно старшего разряда, а вторая половина чисел, как и ранее, остается без изменения и так далее, пока на $K/2$ циклическом сдвиге первая половина чисел в перестановке $M_i(K/2)$ не превратится в упорядоченную последовательность $1 - 2 - -3 - \ldots - K/2$. Если учесть, что вторая половина чисел перестановки M_i(K/2) остается без изменения, то после $K/2$-го циклического сдвига перестановка $M_i(K/2)$ станет тождественно равной перестановке M_1. Перестановке же M_1 соответствует код $K_1 = 00 \ldots 00$, т.е. единица группы, полученная после возведения исходного кода $K_i(K/2)$ в степень $K/2$.

Продемонстрируем возведение в степень, например, кода $K_i(6/2) = 103000$. Действительно, коду $K_i(6/2)$ соответствует четная перестановка $M_i(6/2) = 231456$. Умножая её на код $K_i(6/2)$, получим перестановку 312456. Умножая её ещё раз на указанный код, получим перестановку $M_1 = 123456$, которой соответствует код K_1, т.е. единица группы.

Заметим, что при построении моноединичного кода $K_{i1}(l)$ счет разрядов ведется справа налево (от младшего разряда к старшему), а при построении кода $K_i(K/2)$ слева направо (от старшего разряда к младшему). Поэтому при одинаковом ранге кодов, равным, например, K, запись $K/2$ для разных типов кодов $K_{i1}(K/2)$ и $K_i(K/2)$ обозначают числа разных хотя и рядом стоящих разрядов. Например, при $K = 4$ для моноединичного кода $K_{i1}(K/2)$ единица стоит во втором при счете справа налево разряде, т.е. $K_{i1}(4/2) = 0010$. Код же $K_i(K/2)$ в этом случае равен $K_i(K/2) = 1200$, т.е. число 2 кода, равное 4/2, стоит во втором при счете слева направо разряде.

Имеет место следующая теорема.

Теорема 1. Моноединичный код $K_i(K/2)$ четной перестановки M_i и код $K_j(K/2)$ четной перестановки M_j одного и того же ранга порождают конечную абелеву группу типа $G_{m\times m}$ с образующими

$$K_{i1}^{K/2}(K/2) = K_j^{K/2}(K/2) = \left(K_{i1}^{K/2}(K/2)\cdot K_j^{K/2}(K/2)\right)^{K/2}. \quad (8)$$

В *Теореме* 1 утверждается, что, например, код $K_{i1}(6/2) = 000100$ и код $K_j(6/2) = 103000$ порождают конечную абелеву группу.

Доказательство теоремы разобьем на два этапа. На первом этапе докажем коммутативность произведения кодов K_i и K_j, а на втором – докажем, что степень (порядок) произведения этих кодов равна степени каждого кода в отдельности.

Докажем коммутативность произведения кодов, т.е., что

$$K_{i1}(K/2)\cdot K_j(K/2) = K_j(K/2)\cdot K_{i1}(K/2). \quad (9)$$

Действительно, при формировании результирующей перестановки M_i из перестановки M_1 по произведению кодов $K_{i1}(K/2)\cdot K_j(K/2)$ в соответствии с принятым порядком её формирования (циклические сдвиги от старшего разряда к младшему) вначале после реализации операций кода $K_{i1}(K/2)$ получает циклический сдвиг на один разряд вторая половина чисел перестановки M_1. Затем после реализации операций второго кода $K_j(K/2)$ получим, что аналогичный циклический сдвиг на один разряд произойдет в первой половине чисел перестановки M_1.

Рассмотрим теперь произведение кодов $K_j(K/2)\cdot K_{i1}(K/2)$. Поскольку в первом коде числа, отличные от нуля, располагаются в первой половине кода K_1, а во втором – во второй его половине, то из указанного выше произведения кодов можно по правилу сложения обычных чисел образовать в предложенной системе счисления результирующий код K_{ij1}

$$K_{ij1} = K_j(K/2) + K_{i1}(K/2). \quad (10)$$

Код K_{ij1} будет отличаться от кода $K_j(K/2)$ лишь тем, что в начале второй половины его чисел вместо нуля будет стоять единица.

Если далее из перестановки M_1 с использованием кода K_{ij1} сформировать результирующую перестановку M_r, то вполне очевидно, что в итоге получим ту же перестановку, что в выше рассмотренном случае, в которой первая и вторая половина чисел в M_1 получили по одному циклическому сдвигу, а следовательно, одной и той же результирующий перестановке M_i в обоих случаях будет соответствовать один и тот же код.

Коммутативность произведения кодов (9) доказана.

Для доказательства того, что порядок кодов $K_j(K/2) \cdot K_{i1}(K/2)$ равен $K/2$ воспользуемся выражением (10). Код K_{ij1} по своей структуре состоит из двух независимых частей, составленных исходными кодами $K_j(K/2)$ и $K_{i1}(K/2)$. Каждый из них имеет порядок $K/2$. Поэтому, последовательно возводя код K_{ij1} в степень, получим, что при степени $K/2$ этот код будет равен коду K_1, т.е. единице группы. Теорема доказана полностью.

Продемонстрируем справедливость *Теоремы* 1 на примере двух кодов: $K_{i1}(6/2) = 000100$ и $K_j(6/2) = 103000$.

$$K_{i1}(6/2)\cdot Kj(6/2)\rightarrow 123564\cdot 103000\rightarrow 2315641\rightarrow 103100. \quad (11)$$

$$Kj(6/2)\cdot Ki1(6/2) = 103000\cdot 000100 = 103100. \quad (12)$$

То есть, действительно, исходные коды коммутативны и как нетрудно проверить порядок кодов 000100, 103000 и 103100 равен трем.

Для задания конечной абелевой группы $G_{m\times m}$ достаточно задать две образующие в виде двух кодов перестановок, имеющих следующий вид:

$$\begin{aligned}
&G_{2\times 2}: && 0010^2 - 1200^2.\\
&G_{3\times 3}: && 000100^3 - 103000^3.\\
&G_{4\times 4}: && 00001000^4 - 10040000^4.\\
&G_{5\times 5}: && 0000010000^5 - 1000500000^5. \quad (13)\\
&\ldots && \ldots\\
&G_{m\times m}: && (\overbrace{00\ldots01}^{m}\overbrace{00\ldots0}^{m})^m - (\overbrace{10\ldots0m}^{m}\overbrace{00\ldots0}^{m})^m.
\end{aligned}$$

Далее приведем способ построения из групп типа $G_{m\times m}$ конечных абелевых групп типа $G_{m\times(m+n)}$. В силу перестановочности образующих абелевых групп предложенные ниже способы позволят сформировать любую конечную абелеву группу, порождаемую двумя образующими. Введем два новых понятия: расширение и выравнивание кода перестановки. Первая из них относится к коду $K_j(K/2)$, а вторая – $K_{i1}(K/2)$.

Будем говорить, что код $K_j(K/2)$ расширен на n разрядов, если в него дополнительно введено n нулей сразу за первым старшим разрядом кода, т.е. 1-й. Расширенный на n разрядов код перестановки $K_j(K/2)$ далее обозначается в виде $K_j(K/2, n)$. Например, исходный код $K_j(4/2) = 1200$ после расширения на два разряда ($n = 2$) будет иметь вид $K_j(4/2, 2) = 100200$.

Отметим, что перестановка, соответствующая расширенному коду, может быть как четной, так и нечетной, при этом в процессе расширения кода совокупность его младших нулевых разрядов не изменяется.

Выравнивание вода $K_{i1}(K/2)$ с кодом $K_i(K/2,n)$ сводится к введению в код $K_{i1}(K/2)$ n дополнительных нулей перед его старшим разрядом. По существу, данная процедура сводится к выравниванию рангов двух образующих группу кодов, и поэтому новые обозначения здесь не вводятся. Например, исходный код $K_{i1}(4/2) = 0010$ после выравнивания с кодом $K_i(4/2, 2) = 100200$ имеет вид $K_{i1} = 000010$.

Имеет место следующая теорема.

Теорема 2. Моноединичный код $K_{i1}(K/2)$ четной перестановки M_i и расширенный код $K_j(K/2, n)$ четной перестановки M_j порождают конечную абелеву группу типа $G_{m\times(m+n)}$ с образующими $K_{i1}^{K/2}(K/2)$ и $K_j^{K/2+n}(K/2,n)$.

Докажем вначале, что порядок (степень) расширенного кода $K_j(K/2, n)$ равен $K/2 + n$.

Доказательство. Поскольку расширенный код перестановки образуется из перестановки $K_j(K/2)$ и имеет вид

$$K_j(K/2, n) = \overbrace{100\ldots0K/2}^{K/2}\overbrace{0\ldots0}^{K/2}, \quad (14)$$

то по аналогии с кодом $K_j(K/2)$ (в котором в соответствии с *Предложением* 3 совокупность чисел $K/2$ старших разрядов кода принимает вид упорядоченной последовательности перестановки M_1 после $K/2$ циклических сдвигов) здесь такая же ситуация наступает после $K/2+n$ циклических сдвигов совокупности чисел $K/2+n$ старших разрядов.

Например, порядок расширенного кода

$$K_j(4/2, 1)=10200 \quad (15)$$

равен трем, так как

$$K_1\cdot K_j\rightarrow M_1\cdot K_j\rightarrow 12345\cdot 10200\rightarrow 23145\cdot 10200\rightarrow$$
$$\rightarrow 31245\cdot 10200\rightarrow 12345 = M_1. \quad (16)$$

Докажем далее коммутативность исходных кодов, порождаемых конечную абелеву группу вида $G_{m\times(m+n)}$, т.е.

$$K_{i1}(K/2)\cdot K_j(K/2, n) = K_j(K/2, n)\cdot K_{i1}(K/2). \quad (17)$$

Рассмотрим вначале, какую перестановку образует произведение кодов

$$K_{ij} = K_{i1}(K/2)\cdot K_j(K/2, n). \quad (18)$$

Моноединичный код $K_{i1}(K/2)$ в силу построения составлен из нулей, за исключением разряда $K/2$ при счете справа налево, в котором стоит единица. Поэтому перестановка M_{i1}, полученная из перестановки M_1 и соответствующая коду $K_{i1}(K/2)$, имеет один циклический сдвиг чисел младших разрядов, начинающихся числом разряда $K/2$. Числа других разрядов перестановки M_1 не изменяются.

При умножении перестановки M_{i1} на код $K_j(K/2, n)$ только упорядоченная совокупность чисел $K/2+n$, старших разрядов этой перестановки получает один циклический сдвиг, а остальные числа $K/2$ младших разрядов остаются без изменения.

Полученная таким образом перестановка M_{i1j} и будет соответствовать коду K_{i1j}.

Рассмотрим далее какая перестановка соответствует произведению кодов

$$K_{ilj} = K_j(K/2, n)\cdot K_{il}(K/2). \quad (19)$$

В силу того, что единичный значащий разряд кода $K_{il}(K/2)$, в котором стоит единица, находится в поле младших разрядов кода $K_j(K/2, n)$, составленных из одних нулей, то результирующий код K_{ilj} может быть получен численным суммированием исходных кодов по аналогии с выражением (10), т.е.

$$K_{ilj} = K_j(K/2, n)+K_{il}(K/2). \quad (20)$$

Вполне очевидно, что если первую перестановку M_1 умножить на код K_{ilj}, то в итоге получим перестановку M_{jil}, которая будет в точности равна перестановке M_{ilj}, а следовательно, и коды K_{ilj} и K_{jil} будут также тождественно равны.

Коммутативность произведения кодов и *теорема* 2 в целом доказана.

Последовательность пар образующих кодов конечных абелевых групп, например, типа $G_{3\times(3+n)}$ имеет следующий вид:

$$\begin{aligned}
&G_{3\times4}: \quad 0000100^3 - 1003000^4;\\
&G_{3\times5}: \quad 00000100^3 - 10003000^5;\\
&G_{3\times6}: \quad 000000100^3 - 100003000^6;\\
&\ldots \qquad \ldots\\
&G_{3\times n}: \quad \overbrace{00\ldots0}^{n}100^3 - \overbrace{100\ldots0}^{n}3000^n.
\end{aligned} \quad (21)$$

Для разработки способа построения конечной абелевой группы на основе m циклических образующих сделаем ряд определений.

Далее различаем однопорядковые и разнопорядковые совокупности кодов перестановок. Первые из этих совокупностей содержат коды одинакового порядка m (m = 2, 3, 4, ...), а вторые – хотя бы одну пару кодов различного порядка, например, m_1 и m_2.

Считаем, что каждый код перестановки содержит основную и второстепенную части. Второстепенная часть включает всю упорядоченную совокупность нулевых старших разрядов кода вплоть (исключительно) до первого не равного нулю разряда кода при просмотре слева направо. Эта часть появляется в процессе выравнивания кодов. Основную часть кода образуют все разряды кода, начиная с первого ненулевого разряда кода при просмотре слева направо. Основная часть кода, в свою очередь, содержит *значащую* и *нулевую* (кроме моноединичного кода) часть.

Значащая часть основной части кода заключена между самым левым и самым правым нулевым разрядом кода включительно.

Например, в коде K_i = 00010200 первые три левых нуля 000 образуют вспомогательную часть кода, остальные числа разрядов 10200 – основную часть. При этом числа 102 разрядов являются значащей частью, а два последних нуля 00 – нулевой частью основной части кода.

Считаем, что основная часть моноединичного кода всецело является значащей частью, т.е. она вовсе не содержит нулевой части. Например, в коде K_{il} = 00100 числа 100 разрядов всецело являются значащей частью кода.

Сформулируем правило формирования совокупности специальных однопорядковых кодов перестановок. Обозначим через m – порядок кодов последовательности (m = 2, 3, ..., M), а через n (n = 0, 1, 2, ..., N) – порядковый номер кода в последовательности однопорядковых кодов. Пусть далее основная часть K'_{min} кода образуется с использованием следующей формулы:

$$K'_{mn} = (10^{m-2} - m(n-1))\overbrace{00\ldots0}^{m(n-1)}, \quad (22)$$

где 10^{m-2} – обычное число, вычисляемое в десятичной системе счисления, разряды которого в общем случае разделены знаком «–», разделительный знак «–»(используется по необходимости) в значащей части кода;

$m(n$-1) – десятичное число в значащей части кода (здесь «–» знак вычитания) и одновременно число нулей в нулевой части.

Например, основная часть кодов для m = 2, 3 и n = =1, 4 имеет следующий вид:

$$K'_{2,1} = 10; \quad K'_{2,2} = 1200; \quad K'_{2,3} = 140000;$$

$$K'_{2,4} = 16000000; \quad (23)$$

$$K'_{3,1} = 100; \quad K'_{3,2} = 103000;$$

$$K'_{3,3} = 106000000; \quad K'_{3,4} = 109000000000. \quad (24)$$

Для того, чтобы перейти от главной части кодов, заданных кодами перестановок K, необходимо перевести выравнивание их рангов по самому последнему коду в каждой последовательности, т.е. $K_{2,4}$ и $K_{3,4}$. В итоге получим следующую последовательность кодов перестановок

$$\begin{aligned}
&K_{2,i}: 00000010^2 - 00001200^2 -\\
&-00140000^2 - 16000000^2;\\
&K_{3,i}: 0000000010^3 - 000000103000^3 -\\
&-000106000000^3 - 109000000000^3,
\end{aligned} \quad (25)$$

где степень означает порядок кодов.

Имеет место следующее предложение.

Предложение 4. Конечная одноранговая последовательность кодов, основная часть которых вычисляется с использованием формулы (22), образует совокупность циклических образующих, любой набор которых порождает конечную однопорядковую абелеву группу.

Справедливость коммутативности любых двух кодов перестановок в последовательности типа (25) следует из самого способа их построения и доказывается по аналогии с доказательством *Теоремы* 1. Из попарной ком-

мутативности и одноранговости кодов в последовательности вытекает справедливость *предложения* 4 в целом.

Для формулирования аналогичного утверждения применительно к разнопорядковым кодам последовательности сделаем специальное определение. Будем говорить, что код K_i не имеет пересечения по основной части с кодом K_j, если число разрядов нулевой части кода K_j не меньше числа разрядов всей основной части кода K_i. Последовательность однопорядковых кодов, для которой сформулировано *предложение* 4, образует последовательность кодов, не имеющих пересечений по основной части.

Данная задача наиболее просто решается путем построения вначале всех абстрактных элементов группы из абстрактных циклических образующих, а затем всех кодов перестановок.

Построим в виде кодов всю совокупность элементов конечной абелевой группы, заданной тремя образующими, порядок которых равен 2, 2 и 3.

Результаты построения всех элементов группы приведены в таблице. При этом в первой верхней строке приведены абстрактные элементы группы, во второй их коды перестановок, в третьей сами перестановки и, наконец, в четвертой – коды перестановок, переведенные в обычные десятичные числа N_i.

Результаты построения конечной абелевой группы

$G_{a\times b\times c}$	a	b	c	c^2	ab	ac
K_i	0000010	0001200	1040000	2400000	0001210	1040010
M_i	1234576	1235467	2315467	3124567	1235476	2315476
N_i	1	8	816	1920	9	745
$G_{a\times b\times c}$	ac^2	bc	bc^2	abc	abc^2	I
K_i	2400010	1041200	2401200	1041210	2401210	0000000
M_i	3124576	2315467	3125467	2315476	3125476	1234567
N_i	1921	824	1928	825	1929	0

Построение конечных абелевых групп из разнопорядковых кодов в общем случае осуществляется с использованием процедуры расширения кодов, и вопрос об их пересечении здесь является определяющим.

Пусть требуется построить конечную абелеву группу из l циклических групп, имеющих различные и возрастающие (неубывающие) порядки $l_1, l_2, ..., l$.

Предложение 5. Конечная абелева группа, образуемая возрастающими (неубывающими) циклическими группами порядка $l_1, l_2, ..., l$, может быть построена из одноранговых разнопорядковых кодов $K_1, K_2, ..., K_\xi$, с использованием процедуры расширения кодов в рамках однопорядковой последовательности для кода K_1 и обеспечением условия отсутствия пересечения всех формируемых кодов по их основной части.

Справедливость *Предложения* 5 следует из *теоремы* 2 при увеличении числа исходных кодов более двух и соблюдения условия отсутствия пересечения кодов по их основной части.

Пусть, например, необходимо построить конечную абелеву группу из трех циклических образующих, порядок которых равен 2, 3 и 4. Воспользовавшись условиями, сформулированными в *Предложении* 5, получаем, что коды образующих имеют следующий вид:

$K_1^2 = 0000000010^2$; $K_2^3 = 0000010200^3$; $K_3^4 = 1006000000^4$.

Возникает вопрос: каким образом построить все элементы конечной абелевой группы, заданной кодами образующих?

Анализ таблицы показывает, что для элементов группы, составленных из двух и трех образующих, выполняется условие арифметической аддитивности относительно исходных элементов как в системе счисления кодов перестановок, так и в десятичной системе счисления. Для степеней каждой отдельной образующей это условие не выполняется в силу цикличности образования перестановок этих элементов.

В заключение приведем вариант решения поставленной в статье [4] задачи об отыскании способа построения конечной группы кодами более высокого ранга изоморфной группы с кодами минимального ранга, отличной от решений, сформулированных в *Предложениях* 4 и 5.

Будем говорить, что перестановка M_i, содержащая m разрядов, расширена справа на n разрядов (M_i, n), если в ней справа приписана совокупность упорядоченных чисел $m+1, m+2, ..., m+n$. Например, перестановка $M_i = 312$, расширенная на три разряда ($n=3$) , имеет следующий вид $M_{i,3} = 312456$.

Пусть группа G задана двумя кодами минимального ранга K_i и K_j, которым соответствуют перестановки M_i и M_j. Имеет место следующее предложение.

Предложение 6. Группа G, заданная кодами минимального ранга K_i и K_j, которым соответствуют перестановки M_i и M_j, изоморфна группе G', построенной с использованием кодов $K_{i,n}$ и $K_{j,n}$, которым соответствуют

расширенные справа перестановки $M_{i,n}$ и $M_{j,n}$.

Справедливость *Предложения* 6 вытекает из того, что порядок кодов $K_{i,n}$ и $K_{j,n}$ и их различных произведений в точности соответствует порядку кодов K_i и K_j и их различных произведений.

Условия, сформулированные в *Предложении* 6, являются достаточными, но не необходимыми. Это следует из того, что одна и та же группа может задаваться различной парой кодов и поэтому даже при изоморфизме двух групп, заданных кодами различных рангов, условие *предложения* 6 может не выполняться. Так, например, коды образующих диэдра (приведенные в статье [4]) 010-100 и 0110-1200 обеспечивают изоморфизм групп, но не подпадают под *Предложение* 6. Однако коды 010-210 и 0110-2210 для тех же групп обеспечивают выполнение условий *Предложения* 6, так как указанным парам кодов соответствуют пары перестановок 132-321 и 1324 и 3214.

Предложение 6 справедливо как для абелевых, так и некоммутативных групп, причем не только для двух, но и для m образующих.

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. Голиков В.П. Конструктивные способы задания и построения конечных групп. «Двойные технологии», №1, 2004.

Материал поступил в редакцию 26. 02. 2010 г.