УДК 519.4

# О проблеме изоморфизма для коммутативных полугрупп

**М. А. Тайцлин** (Новосибирск)

Мы приводим утверждения о строении конечно порожденных коммутативных полугрупп, которые позволяют нам найти необходимые и достаточные условия изоморфизма двух конечно определенных коммутативных полугрупп. Эта часть работы может представлять и самостоятельный интерес, но для нас основной результат — установление рекурсивной эквивалентности трех алгоритмических проблем: проблемы изоморфизма для коммутативных полугрупп, проблемы изоморфизма для регулярных коммутативных полугрупп и проблемы сопряженности конечных последовательностей элементов в группах $GL(l, Z)$.

## § 1. Конечно порожденные коммутативные полугруппы

Напомним, что нулем коммутативной полугруппы $A$ называют такой ее элемент $o$, что $o+x=x$ для всех $x \in A$.

В этой статье через $A$, $A_1$, $A_2$, $B$ обозначаются коммутативные полугруппы с нулем.

Напомним, что $a$ делит $b$ в $A$, если существует такой $c \in A$, что $a+c=b$. Мы скажем, что $a \lhd b$, если существует такое натуральное $n$, что $a$ делит $nb$, и скажем, что $a \lhd\rhd b$, если $a \lhd b$ и $b \lhd a$.

Отношение $\lhd\rhd$, понятно, является отношением эквивалентности. Классы эквивалентности по этому отношению являются подполугруппами и называются архимедовыми компонентами $A$ (см. [1], § 4.3). Ради краткости вместо «архимедова компонента» будем говорить «компонента».

Ясно, что отношение $\lhd$ индуцирует отношение на компонентах (другими словами, $\lhd$ не зависит от выбора представителей из компонент). Новое отношение будем обозначать через $\lhd^*$. Ясно, что $\lhd^*$ является верхней полуструктурой.

Если $A$ порождается множеством $X$, то обозначим для $a \in A$ через $X(a)$ множество тех $b \in X$, для которых $b \lhd a$. Ясно, что

$$a_1 \lhd\rhd a_2 \Leftrightarrow X(a_1)=X(a_2).$$

Мы скажем, что $Y$ замкнуто в $X$, если $Y=X(a)$ для некоторого $a \in A$. По предыдущему полуструктура компонент изоморфна полуструктуре замкнутых подмножеств $X$ (с отношением включения).

В случае, когда $X$ конечно, $Y$ замкнуто в $X$ тогда и только тогда, когда никакой элемент подполугруппы, порожденной $Y$ в $A$, не делится ни на какой элемент из $X-Y$.

Понятно, что любое замкнутое подмножество $X$ содержит те элементы $X$, которые делят нуль полугруппы $A$. Поэтому пересечение любых двух замкнутых подмножеств $X$ непусто.

При конечном $X$ пересечение любых двух замкнутых подмножеств $X$ снова замкнуто. Значит, в случае, когда полугруппа $A$ конечно порождена, множество компонент $S(A)$ конечно, и $\lhd^*$ является структурой.

Даже если $A$ конечно порождена, некоторые компоненты $A$ могут не быть конечно порожденными полугруппами. Например, в полугруппе, образованной парами натуральных чисел с операцией покоординатного сложения, компонента содержащая $(1, 1)$, не является конечно порожденной. Этим объясняется преимущество использования вместо компонент подполугрупп, порожденных замкнутыми подмножествами множества образующих.

Однако, если в компоненте $P$ конечно порожденной полугруппы $A$ имеются регулярные элементы, то подполугруппа $G(P)$, порожденная ими, является конечно порожденной (и, очевидно, является группой). Учитывая, что это тривиальное утверждение очень существенно используется в дальнейшем, приведем его доказательство.

Напомним, это элемент $x \in A$ называется р е г у л я р н ы м в $A$, если существует такой $y \in A$, что $x=2x+y$ в $A$. Пусть $a$ — регулярный элемент из $P$, конечное $X$ порождает $A$, $Y=X(a)$. Тогда имеется такой $a_1 \in A$, что $a=2a+a_1$ в $A$. Обозначим $a+a_1$ через $b$ и покажем, что $Z=\{y+b \mid y \in Y\}$ порождает $P$. Очевидно, все элементы из множества $Z$ лежат в $P$ и являются регулярными. Но элементы $G(P)$ — это в точности регулярные элементы $P$. Поэтому $Z \subseteq G(P)$. Если $g$ — произвольный элемент из $G(P)$, то $g=a+g_1$ для некоторого $g_1$. Вместе с тем $X(g)=Y$ и, значит, $g=\sum_{y \in Y} n(y)\,y$, где $n(y)$ — натуральные числа. Отсюда

$$g=a+g_1=a+\sum_{y \in Y} n(y)\,b+g_1=g+\sum_{y \in Y} n(y)\,b=\sum_{y \in Y} n(y)(y+b).$$

Множество $L(X)$ формальных линейных комбинаций элементов $X=\{x_1, \ldots, x_k\}$, т. е. выражений вида $n_1x_1+\ldots+n_kx_k$, где $n_1, \ldots, n_k$ — натуральные числа, вместе с операцией покоординатного сложения образует коммутативную полугруппу. Нулем в ней является комбинация с нулевыми коэффициентами, обозначаемая через $o$. Будем говорить, что одна комбинация меньше другой, если она делит вторую в $L(X)$, что комбинация минимальна в некотором множестве комбинаций, если в этом множестве нет отличной от нее и меньшей комбинации, и т. п. Если $X_1 \subseteq X$, мы считаем $L(X_1)$ подполугруппой $L(X)$.

Если $X \subseteq A$, то имеется единственный гомоморфизм $L(X)$ в $A$, продолжающий тождественное вложение $X$ в $A$. Этот гомоморфизм каждому элементу из $L(X)$ приписывает значение в $A$. При этом значения разных элементов $L(X)$ могут оказаться равными. Говоря, что $f$ и $g$ из $L(X)$ равны в $A$ (и записывая $f=g$ в $A$), мы понимаем под этим, что образы $f$ и $g$ равны при рассматриваемом гомоморфизме $L(X)$

в $A$. Аналогично мы понимаем, что $f$ делит $g$ в $A$, $f$ нерегулярен в $A$, и т. п. Нам удобно рассматривать $L(X)$ и при пустом $X$, понимая в этом случае под $L(X)$ одноэлементную полугруппу и приписывая ее элементу в качестве значения в $A$ нуль полугруппы $A$.

В дальнейшем типичной будет более общая ситуация, когда $Y$ не содержится в $B$, а имеется отображение $\psi$ множества $Y$ в $B$, которое не обязательно взаимно однозначно. Ясно, что это $\psi$ однозначно продолжается до гомоморфизма $L(Y)$ в $B$. Образ $y$ из $L(Y)$ при этом гомоморфизме мы называем значением $y$ в $B$. В наших рассмотрениях всякий раз будет понятно, какое $\psi$ имеется в виду.

Элемент $h$ из $A$ мы называем цейтинским элементом $A$, если для любых $x$, $u$, $v \in A$ из равенства $h+x+u=h+x+v$ в $A$ следует равенство $h+u=h+v$. Существование цейтинских элементов в конечной порожденной коммутативной полугруппе следует из теоремы Редеи о конечной определенности ([2], теорема 9.28) и теоремы Г. С. Цейтина ([3], лемма 5). Пусть $\psi$ отображает $X$ в $A$, $\psi X$ порождает $A$, $X$ содержит $k$ элементов и $X=\{x_1, \ldots, x_k\}$. Ясно, что среди цейтинских элементов $A$ существуют элементы вида

$$n\psi x_1+\ldots+n\psi x_k, \qquad (1)$$

где $n$ — натуральное число, большее 1. Дело в том, что элемент, делящийся на цейтинский, снова цейтинский. Среди цейтинских элементов выберем такой, который допускает запись вида (1) с наименьшим $n>1$. Этот элемент будем называть минимальным цейтинским элементом $A$ для $\psi$, а наименьшее $n>1$, для которого (1) есть цейтинский элемент, назовем цейтинским числом $A$ для $\psi$.

Если $c \in L(X)$, $Y \subseteq X \subseteq A$, через $L(Y)/E_c$ мы обозначаем факторполугруппу полугруппы $L(Y)$ по отношению конгруэнтности $E_c$ на $L(Y)$, задаваемому условием: $E_c(u, v) \Leftrightarrow c+u=c+v$ в $A$. Имеется естественное отображение $Y=\{y_1, \ldots, y_m\}$ в $L(Y)/E_c$, переводящее $y \in Y$ в классе $yE_c$ по $E_c$, содержащий $y$, и это отображение продолжается до гомоморфизма $L(Y)$ на $L(Y)/E_c$. В этой ситуации через $h(Y, c)$ мы обозначаем элемент вида $ny_1+\ldots+ny_m$ с наименьшим натуральным $n>1$, значение которого в $L(Y)/E_c$ является цейтинским элементом. По определению, полугруппа $L(Y)/E_{c+h(Y,c)}$ является полугруппой с сокращением. Через $G(Y, c)$ мы обозначаем максимальную подгруппу полугруппы $L(Y)/E_{c+h(Y,c)}$. Пусть $h(Y, c)=n(Y, c)y_1+\ldots+n(Y, c)y_m$.

Сейчас мы напомним (правда, в несколько измененном виде) определения ряда понятий, которые будут центральными в наших рассмотрениях и которые играли основную роль и в предыдущих работах автора по коммутативным полугруппам (см. [4]—[7]).

Записывая, что $Y \subset X$, мы понимаем под этим, что одновременно $Y \subseteq X$ и $Y \neq X$. Пусть конечное $X$ порождает $A$, а $h$ — элемент из $L(X)$. Для $Y \subset X$ через $\mathfrak{N}(h, Y, A)$ обозначим совокупность тех комбинаций $c$ из $L(X-Y)$, для которых $c+u$ не делится в $A$ на $h$ ни при каком $u \in L(Y)$, через $\mathfrak{M}(h, Y, A)$ обозначим множество максимальных комбинаций из $\mathfrak{N}(h, Y, A)$, а через $\mathfrak{M}_1(h, Y, A)$ — множество тех комбинаций из $L(X-Y)$, для которых существуют большие комбинации в $\mathfrak{M}(h, Y, A)$. Подробнее, «$e$ лежит в $\mathfrak{M}(h, Y, A)$» равносильно тому, что $e$ лежит в $\mathfrak{N}(h, Y, A)$, но $e+f$ не лежит в $\mathfrak{N}(h, Y, A)$ ни при какой $f$ из $X-Y$, а «$e$ лежит в $\mathfrak{M}_1(h, Y, A)$» равносильно тому, что существует $f$ из $L(X-Y)$, для которой $e+f$ лежит в $\mathfrak{M}(h, Y, A)$. В частности, $\mathfrak{M}(h, Y, A) \subseteq \mathfrak{M}_1(h, Y, A)$, и если $\mathfrak{M}(h, Y, A)$ пусто, то пусто и $\mathfrak{M}_1(h, Y, A)$.

Из теоремы Диксона ([2], стр. 163—164) следует, что множества $\mathfrak{M}(h, Y, A)$ и $\mathfrak{M}_1(h, Y, A)$ конечны.

Ясно, что если $\mathfrak{M}(h, Y, A)$ непусто, то $Y$ непусто и $Y$ замкнуто в $X$. Действительно, если $a \in \mathfrak{M}(h, Y, A)$, $b \in X-Y$ и $b$ делит в $A$ некоторый элемент из $L(Y)$, то $a+b \in \mathfrak{N}(h, Y, A)$, а это противоречит определению $\mathfrak{M}(h, Y, A)$.

Если $h_1$ делится в $A$ на $h_2$, а $h_2$ делится в $A$ на $h_1$, то $\mathfrak{N}(h_1, Y, A) = \mathfrak{N}(h_2, Y, A)$. Значит, в этом случае $\mathfrak{M}(h_1, Y, A) = \mathfrak{M}(h_2, Y, A)$ и $\mathfrak{M}_1(h_1, Y, A) = \mathfrak{M}_1(h_2, Y, A)$.

Лемма 1 (ср. [4], лемма 3; [7], лемма 14). *Пусть конечное множество $X$ порождает $A$ и $h \in L(X)$.*

а) *Для любого $x \in L(X)$ либо $x$ делит $h$ в $A$, либо существуют такое $Y \subset X$ и такие $u \in L(X-Y)$ и $v \in L(Y)$, что $x = u+v$ в $L(X)$, а $u \in \mathfrak{M}_1(h, Y, A)$.*

б) *Для любого $Y_1 \subset X$ и любого $x$ из $\mathfrak{N}(h, Y_1, A)$ существуют такое $Y \supseteq Y_1$ и такие $u_1$ и $u_2$, что $u_1 \in \mathfrak{M}_1(h, Y, A)$, $u_2 \in L(Y-Y_1)$ и $x = u_1+u_2$ в $L(X)$.*

в) *Если $Y \subset X$; $u_1 u_2 \in L(X-Y)$; $v_1 v_2 \in L(Y)$; $u_1+v_1 = u_2+v_2$ в $A$, то $u_1 \in \mathfrak{N}(h, Y, A) \Longleftrightarrow u_2 \in \mathfrak{N}(h, Y, A)$; $u_1 \in \mathfrak{M}(h, Y, A) \Longleftrightarrow u_2 \in \mathfrak{M}(h, Y, A)$; $u_1 \in \mathfrak{M}_1(h, Y, A) \Longleftrightarrow u_2 \in \mathfrak{M}_1(h, Y, A)$.*

г) *Если $u \in \mathfrak{M}_1(h, Y, A)$, то либо $u$ — нуль в $L(X-Y)$, либо $u$ нерегулярен в $A$.*

Доказательство. Утверждения в) и г) очевидны; а) есть частный случай б) (при пустом $Y_1$). Доказательство б) приведено в [4] (см. там доказательство леммы 3).

Пусть конечное $X$ порождает $A$. Строго убывающую последовательность $Y_0 = X, Y_1, \ldots, Y_m$ подмножеств $X$ (т. е. такую, что $Y_{i+1} \subset Y_i$) вместе с последовательностью $c_1, \ldots, c_m$, для которой $c_i \in L(Y_{i-1} - Y_i)$, $c_i E_{d_i} \in \mathfrak{M}_1(h_{i-1}, Y_i E_{d_i}, L(Y_{i-1})/E_{d_i})$, $(Y_{i-1} - Y_i) E_{d_i} \cap Y_i E_{d_i}$ пусто, где $d_i = \sum_{j=1}^{i-1} c_j$ для $i = 2, \ldots, m$; $d_1$ — нуль полугруппы $A$; $h_{i-1}$ — значение $h(Y_{i-1}, d_i)$ при таком гомоморфизме $L(Y_{i-1})$ на $L(Y_{i-1} E_{d_i})$, при котором $y \in Y_{i-1}$ переходит в $y E_{d_i}$, а $c_i E_{d_i}$ — образ $c_i$ при этом гомоморфизме, назовем **координатой полугруппы $A$ относительно $X$**. При $m = 0$ координата есть одночленная последовательность $(X)$. Ясно, что для любой координаты $(Y_0, \ldots, Y_m; c_1, \ldots, c_m)$ $Y_m$ замкнуто в $X$ и содержит множество $X^0$ элементов $X$, делящих нуль полугруппы $A$.

Лемма 2. *Пусть конечное $X$ порождает $A$. Для каждых $x \in L(X)$ и $Z \subset X$ существуют такая координата $(Y_0, \ldots, Y_m; c_1, \ldots, c_m)$ относительно $X$*

*и такой $u$, что $Y_m \supseteq Z$ и $x=c+u$ в $A$, где $c=\sum_{i=1}^{m} c_i$, $u \in L(Y_m)$ и для некоторого $u_1 \in L(Z)$ значение $u+u_1$ делится в $L(Y_m)/E_c$ на значение $h(Y_m, c)$.*

Доказательство. Лемму докажем индукцией по числу элементов $X$. Пусть $h=h(X, o)$. Если при некотором $u_1 \in L(Z)$ $x+u_1$ делится на $h$ в $A$, то в качестве координаты надо взять $(X)$, а в качестве $u$ — сам $x$. Если же $x+u_1$ не делится на $h$ ни при каком $u_1 \in L(Z)$, то, по лемме 1б), существуют такие $Y_1 \subset X$ и $c_1 \in \mathfrak{M}_1(h, Y_1, A)$, $v \in L(Y_1)$, что $x=c_1+v$ в $A$, а $Y_1 \supseteq Z$. Пусть $(Y_1, ..., Y_m; c_2, ..., c_m)$ — такая последовательность, что $(Y_1E_{c_1}, \ldots, Y_mE_{c_1}, c_2E_{c_1}, \ldots, c_mE_{c_1})$ является координатой $L(Y_1)/E_{c_1}$ относительно $Y_1E_{c_1}$; $Y_m \supseteq Z$, а значения $v$ и $c_2+ \ldots +c_m+u$ равны в $L(Y_1)/E_{c_1}$, где $u \in L(Y_m)$ и для некоторого $u_1 \in L(Z)$ значение $u+u_1$ делится на значение $h(Y_m, c)$ в $L(Y_m)/E_c$. Тогда $x=c_1+v=c+u$ в $A$, а $(X, Y_1, \ldots, Y_m; c_1, c_2, \ldots, c_m)$ — координата $A$.

Координатными парами полугруппы $A$ относительно порождающего $A$ конечного множества $X$ назовем пару $(X, o)$ и такие пары $(Y, c)$, где $Y \subset X$, а $c \in L(X-Y)$, для которых существует координата $(Y_0, ..., Y_m; c_1, ..., c_m)$, удовлетворяющая условиям: $Y_m=Y$, $c=c_1+ ... +c_m$ в $L(X)$. Через $T(A, X)$ обозначим множество всех координатных пар $A$ относительно $X$. Ясно, что множество $T(A, X)$ конечно.

На множестве $T(A, X)$ рассмотрим отношение $\leqslant$, считая, что $(Y, c) \leqslant (Z, b)$, если $Y \subseteq Z$, а $c=c_1+c_2$ в $L(X)$, где $c_2 \in L(Z-Y)$, $c_1 \in L(X-Z)$ и $c_1$ делит $b$ в $L(X)$.

Легко проверяется, что это отношение $\leqslant$ является частичным порядком, а пара $(X, o)$ является наибольшей в $T(A, X)$.

Заметим еще, что пара $(Z, o)$ является координатной для всякого замкнутого $Z \subseteq X$.

Действительно, по лемме 2 существуют такая координата $(Y_0, ..., Y_m; c_1, ..., c_m)$ и такой $u \in L(Y_m)$, что в $A$ $o=c+u$, где $c=\sum_{i=1}^{m} c_i$, а $Y_m \supseteq Z$. Из замкнутости $Y_m$ следует, что $c=o$, а из замкнутости $Z$ следует, что $u \in L(Z)$. По лемме 2 можно еще предполагать, что для некоторого $u_1 \in L(Z)$ значение $u+u_1$ делится в $L(Y_m)/E_c$ на значение $h(Y_m, c)$. Так как $c=o$, то это равносильно тому, что $u+u_1$ делится на $h(Y_m, o)$ в $A$. Из замкнутости $Z$ и определения $h(Y_m, o)$ следует, что $Y_m=Z$.

В частности, является координатной пара $(X^0, o)$. Ясно, что эта пара является наименьшей в $T(A, X)$.

Если $c$ — нерегулярный элемент из $X$, то множество $X\{c\}$ тех элементов $y \in X$, для которых существует такой $v \in L(X)$, что $x+y+v=x$ в $A$, замкнуто в $X$ и либо пара $(X\{c\}, c)$ является координатной, либо $c$ равняется в $A$ линейной комбинации отличных от $c$ элементов $X$.

Первое из этих утверждений очевидно, а для доказательства второго надо использовать лемму 2. По этой лемме (при $Z=X\{c\}$) существует такая координата $(Y_0, ..., Y_m; c_1, ..., c_m)$, что $Y_m \supseteq X\{c\}$ и для $d=c_1+... ...+c_m$ и некоторого такого $u \in L(Y_m)$, что значение $u+u_1$ делится в

$L(Y_m)/E_d$ на значение $h(Y_m, d)$ для некоторого $u_1 \in L(X\{c\})$, $c=d+u$ в $A$. Если $c \in X\{c\}$, то $c$ делится в $A$ на $2c$ и $c$ регулярен. Если $c \in Y_m - X\{c\}$, то из замкнутости $Y_m$ следует, что $d=o$. Теперь $c+u_1$ делится на $2c$ в $A$. Но $u_1 \in L(X\{c\})$, и, значит, $c+u_1+u_2=c$ в $A$ для некоторого $u_2 \in L(X)$. Опять получается, что $c$ делится на $2c$ в $A$, что противоречит нерегулярности $c$. Итак, $c \in L(X-Y_m)$. Если $d$ делится на $c$ в $L(X)$, то $d=c$, $u \in L(X\{c\})$. Из определения $h(Y_m, c)$ следует, что тогда $Y_m=X\{c\}$. Если же $a$ не делится на $c$ в $L(X)$, то $c$ равняется в $A$ линейной комбинации отличных от $c$ элементов $X$.

С двумя координатными парами $(Y, c)$ и $(Z, b)$ свяжем множество $\mathfrak{K}(c, b, Y, Z, A)$ тех элементов $v$ из $L(Y)$, для которых существуют такой $u \in L(Z)$, что в $A$

$$c+h(Y, c)+v=b+h(Z, b)+u. \tag{2}$$

Через $\mathfrak{K}_1(c, b, Y, Z, A)$ обозначим множество минимальных элементов из $\mathfrak{K}(c, b, Y, Z, A)$, а для $v \in \mathfrak{K}(c, b, Y, Z, A)$ через $u_1(v)$ — такой из $u \in L(Z)$, для которого в $A$ выполняется (2).

Если $v_1, v_2 \in \mathfrak{K}(c, b, Y, Z, A)$ и $v_1=v_2+w$ в $L(Y)$, то $w \in L(Z)$.

Действительно, в $A$

$$c+h(Y, c)+v_1=c+h(Y, c)+v_2+w=$$
$$=b+h(Z, b)+u_1(v_2)+w=b+h(Z, b)+u_1(v_1).$$

Если $w=w_1+a_1$ в $L(X)$, $w_1 \in L(Z)$, $a_1 \in L(X-Z)$, $a_1 \neq 0$, а координата $(Y_0, Y_1, \ldots, Y_m; c_1, \ldots, c_m)$ такова, что $b=c_1+\ldots+c_m$ и $Y_m=Z$, то $a_1=a+a_2+$ $+a_3$, $a_2 \in L(Y_i-Y_{i+1})$, $a_3 \in L(Y_{i+1})$, $a \in Y_i-Y_{i+1}$ для некоторого $i$. Пусть $d=$ $=c_1+\ldots+c_i$. Тогда для некоторых $w_2$, $w_3$ из $L(Y_{i+1})$ значения $c_{i+1}+a+$ $+a_2+w_2$ и $c_{i+1}+w_3$ равны в $L(Y_i)/E_d$, а $c_{i+1}E_d \in \mathfrak{M}_1(h_i, Y_{i+1}E_d, L(Y_i)/E_d)$. Пусть $f \in L(Y_i-Y_{i+1})$, $fE_d \in \mathfrak{M}(h_i, Y_{i+1}E_d, L(Y_i)/E_d)$ и $c_{i+1}$ делит $f$ в $L(X)$. Тогда значения $f+a+a_2+w_2$ и $f+w_3$ равны в $L(Y_i)/E_d$, но $(f+a+a_2)E_d \notin$ $\notin \mathfrak{M}(h_i, Y_{i+1}E_d, L(Y_i)/E_d)$. Это противоречит лемме 1в).

Наконец, через $\mathfrak{A}(c, Y, A)$ обозначим множество тех $v \in L(Y)$, для которых существует такой $u \in L(Y)$, что в $A$

$$c+v=c+h(Y, c)+u, \tag{3}$$

и через $\mathfrak{A}_1(c, Y, A)$ — множество минимальных элементов из $\mathfrak{A}(c, Y, A)$, а для $v \in \mathfrak{A}(c, Y, A)$ через $u_2(v)$ — такой из $u \in L(Y)$, для которого в $A$ выполняется (3).

Пусть $\varphi$ — гомоморфизм $L(X)$ в $A$, $Y \subseteq X$, $c \in L(X)$. Скажем, что $Y$ $(\varphi, c)$-замкнуто в $X$, если $\varphi c+\varphi y$ не делится в $A$ на $\varphi c+\varphi x$ для всяких $y \in L(Y)$, $x \in X-Y$. Например, если $X$ порождает $A$, $\varphi$ тождественно на $X$, $(Y, c) \in T\ (A, X)$, то $Y$ является $(\varphi, c)$-замкнутым в $X$.

Лемма 3. *Пусть $\varphi$, $\psi$ — такие отображения конечного множества $X$ в $A$, для которых выполняются условия:*

1) *$\varphi x$ порождает $A$, и $\psi x$ порождает $A$;*

2) *для каждого такого $x \in X$, что $\varphi x$ нерегулярен, найдутся такие $u, v \in A$, что $\varphi x=\psi x+u$, $\psi x=\psi x+u+v$ в $A$;*

3) *для каждого такого $x \in X$, что $\varphi x$ регулярен, $\psi x$ тоже регулярен и* $(\varphi x) \lhd\rhd (\psi x)$ в $A$.

*Будем через* $\varphi$ *и* $\psi$ *обозначать также гомоморфизмы* $L(X)$ *в* $A$, *продолжающие* $\varphi$ *и* $\psi$ *соответственно. Тогда*:

а) *цейтинские числа* $A$ *для* $\varphi$ *и* $\psi$ *равны, а минимальные цейтинские элементы* $h_\varphi$ *и* $h_\psi$ *полугруппы* $A$ *для* $\varphi$ *и* $\psi$ *делятся в* $A$ *друг на друга*;

б) $Y$ $(\varphi, c)$*-замкнуто в* $X$ *тогда и только тогда, когда* $Y$ $(\psi, c)$*-замкнуто в* $X$ (*для каждых* $Y \subseteq X$ *и* $c \in L(X)$);

в) $(\varphi Y, \varphi c) \in T(A, \varphi X) \Longleftrightarrow (\psi Y, \psi c) \in T(A, \psi X)$ *для каждого* $c \in L(X-Y)$ *и каждого* $(\varphi, c)$*-замкнутого* $Y \subseteq X$;

г) $\varphi u \in \mathfrak{K}(\varphi c, \varphi b, \varphi Y, \varphi Z, A) \Longleftrightarrow \psi u \in \mathfrak{K}(\psi c, \psi b, \psi Y, \psi Z, A)$ *для каждых таких* $c \in L(X-Y)$, $b \in L(X-Z)$, $(\varphi, c)$*-замкнутого* $Y \subseteq X$, $(\varphi, b)$*-замкнутого* $Z \subseteq X$, *что* $(\varphi Y, \varphi c) \in T(A, \varphi X)$, $(\varphi Z, \varphi b) \in T(A, \varphi X)$, *и каждого* $u \in L(Y)$;

д) $\varphi u \in \mathfrak{A}(\varphi c, \varphi Y, A) \Longleftrightarrow \psi u \in \mathfrak{A}(\psi c, \psi Y, A)$ *для каждых таких* $c \in L(X-Y)$, $(\varphi, c)$*-замкнутого* $Y \subseteq X$, *что* $(\varphi Y, \varphi c) \in T(A, \varphi X)$, *и каждого* $u \in L(Y)$;

е) *полугруппы* $L(\varphi Y)/E_{\varphi c}$ *и* $L(\psi Y)/E_{\psi c}$, $L(\varphi Y)/E_{\varphi c + h(\varphi Y, \varphi c)}$ *и* $L(\psi Y)/E_{\psi c + h(\psi Y, \psi c)}$ *и группы* $G(\varphi Y, \varphi c)$ *и* $G(\psi Y, \psi c)$ *изоморфны* (*для каждых* $c \in L(X-Y)$ *и* $(\varphi, c)$*-замкнутого* $Y \subseteq X$);

ж) *значение* $\varphi x$ *в* $L(\varphi Y)/E_{\varphi c + h(\varphi Y, \varphi c)}$ *тогда и только тогда лежит в* $G(\varphi Y, \varphi c)$, *когда значение* $\psi x$ *в* $L(\psi Y)/E_{\psi c + h(\psi Y, \psi c)}$ *лежит в* $G(\psi Y, \psi c)$ (*для каждых* $c \in L(X-Y)$, $(\varphi, c)$*-замкнутого* $Y \subseteq X$ *и* $x \in Y$).

Д о к а з а т е л ь с т в о. а) Если $\varphi x$ регулярен, то из $(\varphi x) \lhd \rhd (\psi x)$ следует, что в $A$

$$\varphi x = n\varphi x + u = \psi x + u_1,$$

где $n$ — подходящее натуральное число, а $u_1, u_2 \in A$. В этом случае $\psi x$ тоже регулярен, и аналогичное равенство показывает, что $\psi x$ делится в $A$ на $\varphi x$. Если $\varphi x$ нерегулярен, то $\varphi x$ делится в $A$ на $\psi x$, а $\psi x$ делится в $A$ на $\varphi x$ по определению. Значит, $\sum\limits_{x \in X} m\varphi x$ и $\sum\limits_{x \in X} m\psi x$ при каждом натуральном $m$ делятся в $A$ друг на друга и одновременно являются или не являются цейтинскими.

б) Пусть $x \in X-Y$, $y \in L(Y)$, а $\varphi c + \varphi y$ делится в $A$ на $\varphi c + \varphi x$. Тогда, в силу а), $\psi c + \psi y$ делится в $A$ на $\psi c + \psi x$. Если теперь допустить, что $Y$ является $(\psi, c)$-замкнутым, то получим, что $Y$ является также $(\varphi, c)$-замкнутым. Меняя местами $\varphi$ и $\psi$, закончим доказательство б).

Ясно, что лемма 3 верна при пустом $X$. Утверждения в) и д) — ж) мы доказываем индукцией по числу элементов $X$. Для проведения индукции нужно предварительно установить несколько фактов.

П е р в ы й ф а к т. *Для любых* $u \in L(X)$ *и* $(\varphi, o)$*-замкнутого* $Y \subset X$

$$\varphi u \in \mathfrak{M}(h_\varphi, \varphi Y, A) \Longleftrightarrow \psi u \in \mathfrak{M}(h_\psi, \psi Y, A).$$

Действительно, если имеет место левая часть и для $u_1 \in L(Y)$, $u_2 \in L(X)$ в $A$ $\psi u + \psi u_1 = h_\psi + \psi u_2$, то

$$\varphi u + \varphi u_1 = \psi u + \psi u_1 + u_3 = h_\psi + \psi u_2 + u_3 = h_\varphi + \psi u_2 + u_3 + u_4,$$

где $u_3$, $u_4 \in A$, а это противоречит выбору $u$. Значит, $\psi u + \psi u_1$ не делится в $A$ на $h_\psi$ ни для какого $u_1 \in L(Y)$. Из того, что $\varphi u \in L(\varphi X - \varphi Y)$, и из

$(\varphi, o)$-замкнутости $Y$ следует, что $u \in L(X-Y)$. Поэтому $\psi u \in \mathfrak{N}(h_\psi, \psi Y, A)$. Вместе с тем для любого $x \in X - Y$ и подходящего $w_1 \in L(Y)$

$$\psi u + \psi x + \psi w_1 = \varphi u + \varphi x + \varphi w_1 + u_1 = h_\varphi + w + u_1 = h_\psi + w + u_1 + u_2,$$

где $w$, $u_1$, $u_2 \in A$. Значит, $\psi u \in \mathfrak{M}(h_\psi, \psi Y, A)$. Обратная импликация проверяется так же.

Второй факт. *Для любого $(\varphi, o)$-замкнутого $Y \subset X$ $\varphi Y$ и $\psi Y$ порождают в $A$ одну и ту же подполугруппу.*

Действительно, если $a$ лежит в подполугруппе, порожденной $\varphi Y$, $a = \psi z$ в $A$, где $z \in L(X)$, а $x \in X - Y$ встречается в $z$ с ненулевым коэффициентом, то в $A$ для подходящего $u \in L(Y)$

$$\psi u = \varphi u + u_1 = a + u_1 = \psi x + u_2 + u_1,$$

где $u_1$, $u_2 \in A$, а это противоречит $(\psi, o)$-замкнутости $Y$.

Третий факт. *Для любого $(\varphi, o)$-замкнутого $Y \subseteq X$ и любого $c \in L(X)$ полугруппы $L(\varphi Y)/E_{\varphi c}$ и $L(\psi Y)/E_{\psi c} = L(\psi Y)/E_{\varphi c}$ изоморфны.*

Рассматривая теперь для $(\varphi, o)$-замкнутого $Y \subseteq X$ и $c \in L(X)$ отображения $\varphi_1$ и $\psi_1 Y$ в $L(\varphi Y)/E_{\varphi c}$, где $\varphi_1(y) = (\varphi y)/E_{\varphi c}$, $\psi_1(y) = (\varphi z) E_{\varphi c}$, $z \in L(Y)$, $\varphi z = \psi y$ в $A$ для $y \in Y$, найдем, что эти $\varphi_1$ и $\psi_1$ удовлетворяют условиям 1) — 3) леммы 3 с заменой $X$ на $Y$, $\varphi$ на $\varphi_1$ и $\psi$ на $\psi_1$.

в) Фактически требуется установить только первый факт, что уже сделано.

д) Аналогично следует из а).

е), ж). Следуют из третьего факта и доказательства утверждения а).

г) Пусть $\varphi v \in \mathfrak{K}(\varphi c, \varphi b, \varphi Y, \varphi z, A)$. Тогда в $A$

$$\varphi c + h(\varphi Y, \varphi c) + \varphi v = \varphi b + h(\varphi Z, \varphi b) + \varphi u_1,$$

где $u_1 \in L(Z)$. Ясно, что в $A$

$$\psi c + h(\psi Y, \psi c) + \psi v = \varphi c + h(\varphi Y, \varphi c) + \varphi v + \varphi w,$$

$$\varphi c + h(\varphi Y, \varphi c) + \varphi v + \varphi w + \varphi w_1 = \varphi c + h(\varphi Y, \varphi c) + \varphi v,$$

где $w$, $w_1 \in L(Y)$. Если бы $\varphi w$ делилось в $A$ на $\varphi x$, где $x \in X - Z$, то в $A$ при подходящих $u_2 \in L(Z)$, $u_3 \in L(X)$

$$\varphi b + \varphi u_2 = \varphi b + \varphi x + \varphi u_3,$$

что противоречит $(\varphi, b)$-замкнутости $Z$. Значит, $w \in L(Z)$. Окончательно в $A$ имеем

$$\psi c + h(\psi Y, \psi c) + \psi v = \varphi b + h(\varphi Z, \varphi b) + \varphi u_1 + \varphi w = \psi b + h(\psi Z, \psi b) + \psi u_4,$$

где $u_4 \in L(Z)$. Значит, $\psi v \in \mathfrak{K}(\varphi c, \varphi b, \varphi Y, \varphi Z, A)$. Обратная импликация проверяется так же. Лемма доказана.

Элементы $z_1, \ldots, z_l$ группы $G$ называются независимыми в $G$, если для любых целых $n_1, \ldots, n_l$ из равенства $n_1 z_1 + \ldots + n_l z_l$ нулю в $G$ следует, что $n_1 = \ldots = n_l = 0$.

Скажем, что конечное $X$ канонически порождает $A$, если $X$ порождает $A$ и выполняются следующие условия:

а) для каждой компоненты $P$ полугруппы $A$, если $P$ содержит регулярные элементы, то $X$ содержит множество $X(P)$, состоящее из всех элементов конечного порядка из $G(P)$, элементов $z^1(P),\ldots,z^{l(P)}P$ из $G(P)$ и таких независимых в $G(P)$ элементов $y^1(P),\ldots,y^{l(P)}(P)$, что каждый элемент из $G(P)$ равен в $G(P)$ сумме элемента конечного порядка и целочисленной линейной комбинации элементов $y^1(P),\ldots, y^{l(P)}(P)$ (другими словами, элементы конечного порядка из $G(P)$ и элементы $y^1(P), \ldots, y^{l(P)}(P)$ порождают $G(P)$ как группу), а $y^i(P)+z^i(P)$ есть нуль в $G(P)$ для $i=1, \ldots, l(P)$;

б) для каждого нерегулярного $x \in X$ множество $X-\{x\}$ не порождает $A$;

в) $X$ есть объединение множества нерегулярных элементов из $X$ и множеств $X(P)$ для всех таких компонент $P$ полугруппы $A$, которые содержат регулярные элементы.

Если $A$ конечно порождена, то $A$ порождается некоторым конечным $X_1$, для которого выполняется б). Для каждой компоненты $P$ выберем в качестве $X(P)$ такое множество, которое состоит из элементов конечного порядка из $G(P)$, элементов $z^1(P),\ldots, z^{l(P)}(P)$ из $G(P)$ и независимых в $G(P)$ элементов $y^1(P),\ldots, y^{l(P)}(P)$, и при этом $X(P)$ порождает $G(P)$, а $z^i(P)+y^i(P)$ — нуль в $G(P)$ для $i=1,\ldots, l(P)$. Пусть $X$ есть объединение нерегулярных элементов из $X_1$ и $X(P)$ для таких компонент $P$, которые содержат регулярные элементы. Это $X$ канонически порождает $A$.

Прежде всего заметим, что $X$ порождает $A$. Если $x$ — регулярный элемент из $A$, то $x$ лежит в некоторой компоненте $P$ и, значит, равен в $A$ подходящей линейной комбинации элементов $X(P)$. Если $x$ — нерегулярный элемент из $A$, то $x$ равен в $A$ линейной комбинации некоторых элементов из $X_1$, среди которых все регулярные, по предыдущему, лежат в подполугруппе, порожденной $X$, а нерегулярные лежат в $X$.

Если $x$ — нерегулярный элемент из $X$, лежащий в компоненте $P$, и $x$ равняется в $A$ линейной комбинации отличных от $x$ элементов $X$, то все регулярные элементы, встречающиеся в этой комбинации с ненулевыми коэффициентами, лежат в отличных от $P$ компонентах $Q \lhd^* P$, а потому равняются в $A$ линейным комбинациям отличных от $x$ элементов $X_1$. Получается, что б) не выполняется для $X_1$, а это невозможно. Значит, $X$ удовлетворяет условию б). Условиям а) и в) $X$ удовлетворяет по построению.

## § 2. Условия изоморфизма

При изоморфизме $A_1$ на $A_2$ сохраняются отношения $\lhd$ и $\lhd\rhd$, и, значит, этот изоморфизм индуцирует изоморфизм $\langle S(A_1);\ \lhd^*\rangle$ на $\langle S(A_2);\ \lhd^*\rangle$ В частности, при изоморфизме компоненты отображаются на компоненты.

В этом параграфе мы будем для $i=1$, 2 предполагать, что конечное $X_i$ канонически порождает $A_i$.

При изоморфизме $A_1$ на $A_2$ нерегулярный $x \in X_1$ переходит в нерегулярный элемент $A_2$. Этот изоморфизм индуцирует изоморфизм структуры замкнутых подмножеств $X_1$ на структуру замкнутых подмножеств $X_2$. Если при индуцированном изоморфизме $X_1(x)$ переходит в замкнутое $Y \subseteq X_2$, то подполугруппа, порожденная $X_1(x)$, отображается на подполугруппу, порожденную $Y$.

Элементы этой подполугруппы являются линейными комбинациями элементов $Y$, т. е. имеют вид

$$n_1 y_1 + \ldots + n_k y_k, \tag{4}$$

где $n_1, \ldots, n_k$ — натуральные числа, а $y_1, \ldots, y_k \in Y$.

Образ $x$ есть элемент вида (4), где $n_i \neq 0$ для всех $i$ и среди $y_1, \ldots, y_k$ встречается нерегулярный $y_i$ с $X_2(y_i) = Y$.

Действительно, в противном случае пусть $w_i$ — прообраз $y_i$. Будем также считать, что $n_i \neq 0$ для всех $i$. Тогда $w_i$ либо регулярен, либо $X_1(w_i) \neq X_1(x)$, $x = n_1 w_1 + \ldots + n_k w_k$. Если регулярный $w_i$ делится на $x$, то $w_i = 2w_i + w' = 2x + w''$ и $x = 2x + w'''$ при подходящих $w'$, $w''$, $w'''$, а это противоречит нерегулярности $x$. Значит, ни один $w_i$ не делится на $x$, и каждый $w_i$ является линейной комбинацией $X_1(x) - \{x\}$. Это противоречит условию б).

Если $y_i$ — нерегулярный и $X_2(y_i) = Y$, то $n_i = 1$.

Действительно, если $n_i > 1$, то образ $x$ имеет вид $y_i + y_i + v$. Пусть $z$ — прообраз $y_i$, а $u$ — прообраз $v$. Тогда $z$ и $u$ — линейные комбинации элементов $X_1(x)$. Если $z = x + z_1$, то $x = 2x + 2z_1 + u$, а это противоречит нерегулярности $x$. Если же $z$ есть линейная комбинация элементов $X_1(x) - \{x\}$, то $u = x + u_1$ (ибо иначе $X_1(x) - \{x\}$ порождает $A$, а это противоречит условию б)), $x = x + 2z + u_1$ и $X_1(z) \neq X_1(x)$ (иначе $x$ регулярен). Поэтому $X_2(y_i) \neq Y$, что противоречит выбору $y_i$.

Итак, образ $x$ имеет вид $y + v$, где $y \in Y$, $X_2(y) = Y$, $y$ нерегулярен, а $v$ — линейная комбинация элементов $Y$. По предыдущему, $v$ не делится на $y$. Пусть $u$ — прообраз $v$, $z$ — прообраз $y$. Тогда $u$ не делится на $x$ (иначе $v$ делится на $y$), значит, $z = x + z_1$. Теперь $x = x + z_1 + u$, $x + z_1 = x + 2z_1 + u$, $y = y + v + v_1$, где $v_1$ — образ $2z_1 + u$. Отсюда, в частности, следует, что $X_2(v) \neq Y$.

Итак, нами доказана

Лемма 4. *С изоморфизмом $\varphi$ $A_1$ на $A_2$ связываются такие изоморфизм $\hat{\varphi}$ структуры замкнутых подмножеств $X_1$ на структуру замкнутых подмножеств $X_2$ и отображение $\varphi^*$ множества нерегулярных элементов из $X_1$ в множество нерегулярных элементов из $X_2$, что для каждого $y \in A_1$*

$$X_2(\varphi(y)) = \hat{\varphi}(X_1(y)).$$

*При этом для каждого нерегулярного $x \in X_1$*

$$X_2(\varphi(x)) = X_2(\varphi^*(x))$$

*и существуют такие* $v(x),\ w(x) \in A_2$, *что в* $A_2$

$$\varphi(x) = \varphi^*(x) + v(x), \quad \varphi^*(x) + v(x) + w(x) = \varphi^*(x),$$

*а* $X_2(v(x))$ — *собственное подмножество* $X_2(\varphi(x))$.

Лемма 5. $\varphi^*$ *есть взаимно однозначное отображение множества нерегулярных элементов из* $X_1$ *на множество нерегулярных элементов из* $X_2$.

Доказательство. Если $y$ — нерегулярный элемент из $X_2$ и $\hat{\varphi}(Y) = X_2(y)$, то образ $y$ при изоморфизме, обратном к $\varphi$, имеет вид $x+u$, где $x$ — нерегулярный элемент из $X_1$, $X_1(x) = Y$ и существует такой $u_1 \in A_1$, что $x+u+u_1 = x$. Теперь $\varphi(x) = \varphi^*(x) + v(x) = y + \varphi(u_1)$. Если $\varphi(u_1) = \varphi^*(x) + v_2$, то $x = x + 2u + 2u_1$,

$$\varphi(x) = \varphi(x+2u) + 2\varphi(u_1) = 2\varphi^*(x) + v_3 = 2\varphi^*(x) + 2w(x) + 2v(x) + v_3,$$
$$x = 2x + u_2,$$

а это противоречит нерегулярности $x$. Значит, $\varphi(u_1)$ не делится на $\varphi^*(x)$. Если $y \neq \varphi^*(x)$, то $\varphi^*(x) = y + \varphi(u_1) + w(x)$, и правая часть является линейной комбинацией отличных от $\varphi^*(x)$ элементов $X_2$, а это противоречит условию б). Итак, $\varphi^*$ есть отображение на. Одновременно фактически доказана и взаимная однозначность $\varphi^*$. Лемма доказана.

Ясно, что $\varphi G(P) = G(\varphi P)$ для каждой компоненты $P$ полугруппы $A$. Потому множества $X_1(P)$ и $X_2(\varphi P)$ содержат по одинаковому числу элементов. Для нерегулярных $x \in X_1$ уже определено $\varphi^*(x)$, а для регулярных $x \in X_1$ определим $\varphi^*(x)$ так, чтобы $\varphi^*$ отображало $X_1(P)$ на $X_2(\varphi P)$ для каждой компоненты $P$ полугруппы $A_1$, в которой есть регулярные элементы. Тогда $\varphi^*$ является взаимно однозначным отображением $X_1$ на $X_2$. Через $\varphi^*$ мы будем также обозначать гомоморфизм $L(X_1)$ на $L(X_2)$, продолжающий это отображение.

Лемма 6. *Пусть* $\varphi$ — *изоморфизм* $A_1$ *на* $A_2$. *Тогда*

$$n(Y, c) = n(\hat{\varphi}Y, \varphi^* c), \tag{5}$$

$$T(A_2, X_2) = \{(\hat{\varphi}Y, \varphi^* c) \mid (Y, c) \in T(A_1, X_1)\}, \tag{6}$$

$$\mathfrak{K}(\varphi^* c, \varphi^* b, \hat{\varphi}Y, \hat{\varphi}Z, A_2) = \varphi^* \mathfrak{K}(c, b, Y, Z, A_1), \tag{7}$$

$$\mathfrak{A}(\varphi^* c, \hat{\varphi}Y, A_2) = \varphi^* \mathfrak{A}(c, Y, A_1) \tag{8}$$

*для любых* $(Y, c)$, $(Z, b) \in T(A_1, X_1)$;

$$\hat{\varphi}(X_1(x)) = X_2(\varphi^*(x)) \text{ для каждого } x \in X_1; \tag{9}$$

*полугруппы* $L(Y)/E_c$ *и* $L(\hat{\varphi}Y)/E_{\varphi^* c}$ *одновременно являются или не являются группами,* (10)

*полугруппы* $L(Y)/E_{c+h(Y,c)}$ *и* $L(\hat{\varphi}Y)/E_{\varphi^* c + h(\hat{\varphi}Y, \varphi^* c)}$ *изоморфны,* (11)

*группы* $G(Y, c)$ *и* $G(\hat{\varphi}Y, \varphi^* c)$ *изоморфны,* (12)

*значение* $x$ *в* $L(Y)/E_{c+h(Y,c)}$ *лежит в* $G(Y, c)$ *тогда и только тогда, когда значение* $\varphi^* x$ *лежит в* $G(\hat{\varphi}Y, \varphi^* c)$, (13)

$\varphi^*$ *индуцирует изоморфизм факторполугрупп*

$$(L(Y)/E_{c+h(Y,c)})/G(Y,c) \text{ и } (L(\hat{\varphi}Y)/E_{\varphi^*c+h(\hat{\varphi}Y,\varphi^*c)})/G(\hat{\varphi}Y,\varphi^*c) \tag{14}$$

*для каждых* $(Y, c) \in T(A_1, X_1)$ *и* $x \in L(Y)$.

Доказательство. Пусть $\psi(x) = \varphi^*(x)$ для $x \in X_1$, $X = X_1$ и $A = A_1$. Из леммы 4 следует, что выполнены условия 1) — 3) леммы 3 (с заменой $\varphi$ на ограничение $\varphi$ на $X$). Значит, имеют место утверждения а) — ж) леммы 3. Так как $\varphi$ — изоморфизм $A_1$ на $A_2$, то можно в а) — ж) заменить $\varphi$ на тождественное отображение $X_1$ в $A_1$ и $A_2$ на $A_1$ в соответствующих местах. Например,

$$(\varphi Y, \varphi c) \in T(A_2, \varphi X) \Longleftrightarrow (Y, c) \in T(A_1, X_1)$$

и потому в) можно переписать так:

$$(Y, c) \in T(A_1, X_1) \Longleftrightarrow (\psi Y, \psi c) \in T(A_2, \psi X).$$

При этом $\psi X$ есть $X_2$. Остается заменить $\psi Y$ на $\hat{\varphi}Y$ и $\psi c$ на $\varphi^* c$. Лемма доказана.

Ясно, что отображение $\hat{\varphi}$ индуцирует отображение множества компонент $A_1$ на множество компонент $A_2$, которое мы также обозначаем через $\hat{\varphi}$. Если $\varphi$ — изоморфизм, то

$$\text{группы } G(P) \text{ и } G(\hat{\varphi}P) \text{ изоморфны} \tag{15}$$

для каждой компоненты $P$ полугруппы $A_1$.

Независимо от $\varphi$ можно рассматривать такие пары отображений $(\hat{\varphi}, \varphi^*)$, что $\hat{\varphi}$ является изоморфизмом структуры замкнутых подмножеств $X_1$ на структуру замкнутых подмножеств $X_2$, а $\varphi^*$ взаимно однозначно отображает $X_1$ на $X_2$, переводя регулярные элементы в регулярные, а нерегулярные — в нерегулярные. Такую пару $(\hat{\varphi}, \varphi^*)$ мы будем называть хорошей, если выполнены условия (5) — (15). Из леммы 6 следует, что в случае, когда $A_1$ и $A_2$ изоморфны, хорошие пары существуют.

Напомним, что для $X$, порождающего $A$, и $x \in X$ через $X\{x\}$ мы обозначаем множество тех $y \in X$, для которых существуют такие $u \in A$, что $x+y+u=x$ в $A$. Для любого $x \in X$ $X\{x\}$ замкнуто в $X$.

Используя работы автора [4] и [5], можно построить алгоритмы, которые для $i = 1, 2$ по конечным множествам образующих и определяющих соотношений для $A_i$ строят конечное $X_i$, канонически порождающее $A_i$, вычисляют цейтинское число $A_i$ для $X_i$; $X_i\{x\}$ для всех $x \in X_i$; все замкнутые подмножества $X_i$; $T(A_i, X_i)$; $\mathfrak{K}_1(c, b, Y, Z, A_i)$, $\mathfrak{A}_1(c, Y, A_i)$, $h(Y, c)$ для всех $(Y, c), (Z, b) \in T(A_i, X_i)$; конечные множества определяющих соотношений для $L(Y)/E_c$, $L(Y)/E_{c+h(Y,c)}$, $G(Y, c)$, $G(P)$, а также $u_1(v)$, $u_2(w)$ для всех $(Y, c), (Z, b) \in T(A_i, X_i)$, $w \in \mathfrak{A}_1(c, Y, A_i)$,

$v \in \mathfrak{K}_1(c, b, Y, Z, A_i)$ и всех компонент $P$ полугруппы $A_i$. С помощью этих алгоритмов находятся все хорошие пары.

Лемма 7. *Пусть* $(\hat{\varphi}, \varphi^*)$ — *хорошая пара, а* $\psi$ — *такой гомоморфизм* $L(X_1)$ *в* $L(X_2)$, *что*

1) $\psi x = \varphi^* x + v(x)$ *для каждого нерегулярного* $x \in X_1$, *где* $v(x) \in \in L(X_2\{\varphi^* x\})$;

2) $\psi x \in L(X_2(\hat{\varphi}P))$ *и каждый элемент из* $X_2(\hat{\varphi}P)$ *равен в* $A_2$ *элементу вида* $\psi y$, *где* $y \in L(X_1(P))$, *для каждой компоненты* $P$ *полугруппы* $A_1$ *и каждого* $x \in X_1(P)$;

3) $\psi$ *индуцирует изоморфизм* $L(Y)/E_{c+h(Y,c)}$ *на* $L(\hat{\varphi}Y)/E_{\varphi^*c+h(\hat{\varphi}Y,\varphi^*c)}$ *для каждой* $(Y, c) \in T(A_1, X_1)$;

4) $\varphi(c+v)$ *и* $\psi(c+h(Y, c)+u_2(v))$ *равны в* $A_2$ *для каждых* $(Y, c) \in T(A_1, X_1)$ *и* $v \in \mathfrak{A}_1(c, Y, A_1)$;

5) $\psi(b + h(Z, b) + w)$ *и* $\psi(c + h(Y, c) + u_1(w))$ *равны в* $A_2$ *для каждых* $(Y, c), (Z, b) \in T(A_1, X_1)$ *и* $w \in \mathfrak{K}_1(b, c, Z, Y, A_1)$.

*Тогда* $\psi$ *индуцирует изоморфизм* $A_1$ *на* $A_2$.

*Наоборот, если* $\psi$ *удовлетворяет* 1) *и* 2) *и индуцирует изоморфизм* $A_1$ *на* $A_2$, *то* 3) — 5) *выполнены.*

Доказательство. Надо проверить сначала, что $\psi$ отображает $A_1$ на $A_2$. Доказываем для произвольного $y \in A_2$, что для некоторого $x \in L(X_1)$ в $A_2$ равны $y$ и $\psi(x)$. Это следует из 2) для регулярного $x$. Если уже доказано, что каждый элемент каждой такой отличной от $Q$ компоненты $Q_1$, что $Q_1 \lhd^* Q$, имеет прообраз, а $y$ — нерегулярный элемент из $Q \cap X_2$, то $y$ равен в $A_2$ $\varphi^*(x)$ для некоторого нерегулярного $x \in X_1$ и в $A_2$

$$y = y + v(x) + w = \psi(x) + w,$$

где $w \in L(X_2\{y\})$. Так как значение $w$ в $A_2$ лежит в отличной от $Q$ компоненте $Q_1 \lhd^* Q$, то существует такой $u \in L(X_1)$, что $w$ равен $\psi(u)$ в $A_2$. Отсюда $y$ и $\psi(x + u)$ равны в $A_2$.

Осталось проверить, что для $x, y \in L(X_1)$

$$x = y \text{ в } A_1 \Longleftrightarrow \psi x = \psi y \text{ в } A_2.$$

Используя лемму 2, найдем такие пары $(Y, c)$, $(Z, b)$ из $T(A_1, X_1)$, что $x = c + u_1$, $y = b + u_2$ в $L(X_1)$, $u_1 \in L(Y)$, $u_2 \in L(Z)$, значение $u_1$ делится на значение $h(Y, c)$ в $L(Y)/E_c$, значение $u_2$ делится на значение $h(Z, b)$ в $L(Z)/E_b$. При этом пусть $u_1 = w_1 + w_1'$, $u_2 = w_2 + w_2'$, $w_1 \in \mathfrak{A}_1(c, Y, A_1)$, $w_2 \in \mathfrak{A}_1(b, Z, A_1)$. Тогда, по 4), в $A_2$

$$\psi(c + u_1) = \psi(c + h(Y, c) + u_2(w_1) + w_1'),$$

$$\psi(b + u_2) = \psi(b + h(Z, b) + u_2(w_2) + w_2').$$

Из 1) и 2) легко следует, что в $L(X_2)$

$\psi(c+h(Y, c)+u_2(w_1)+w_1') = \varphi^* c + h(\hat{\varphi} Y, \varphi^* c) + \varphi^*(u_2(w_1)) + \varphi^* w_1' + z_1$, где $z_1 \in L(\hat{\varphi} Y)$, а образ $z_1$ в $L(\hat{\varphi} Y)/E_{\varphi^* c + h(\hat{\varphi} Y, \varphi^* c)}$ лежит в $G(\hat{\varphi} Y, \varphi^* c)$,

$\psi(b+h(Z, b)+u_2(w_2)+w_2') = \varphi^* b + h(\hat{\varphi} Z, \varphi^* b) + \varphi^*(u_2(w_2)) + \varphi^* w_2' + z_2$, где $z_2 \in L(\hat{\varphi} Z)$, а образ $z_2$ в $L(\hat{\varphi} Z)/E_{\varphi^* b + h(\hat{\varphi} Z, \varphi^* b)}$ лежит в $G(\hat{\varphi} Z, \varphi^* b)$. Если $\psi x = \psi y$ в $A_2$, то $\varphi^*(u_2(w_2)) + \varphi^* w_2' + z_2 \in \mathfrak{K}(\varphi^* b, \varphi^* c, \hat{\varphi} Z, \hat{\varphi} Y, A_2)$. Из выбора $z_2$ следует, что $\varphi^*(u_2(w_2)) + \varphi^* w_2' \in \mathfrak{K}(\varphi^* b, \varphi^* c, \hat{\varphi} Z, \hat{\varphi} Y, A_2)$. Из (7) следует, что $u_2(w_2) + w_2' \in \mathfrak{K}(b, c, Z, Y, A_1)$. Если же $x = y$ в $A_1$, то $u_2(w_2) + w_2' \in \in \mathfrak{K}(b, c, Z, Y, A_1)$ по определению. Таким образом, если $x = y$ или $\psi x = \psi y$, то существуют такие $z_3$ и $z_4$, что $u_2(w_2) + w_2' = z_3 + z_4$ в $L(X_1)$, $z_3 \ni \in \mathfrak{K}_1(b, c, Z, Y, A_1)$, $z_4 \in L(Y)$. По 5), в $A_2$ имеем $\psi(y) = \psi(c + h(Y, c) + u_1(z_3) + z_4)$, а по определению $y = c + h(Y, c) + u_1(z_3) + z_4$, $x = c + h(Y, c) + u_2(w_1) + w_1'$ в $A_1$. В результате

$$x = y \text{ в } A_1 \Leftrightarrow u_1(z_3) + z_4 = u_2(w_1) + w_1' \text{ в } L(Y)/E_{c+h(Y, c)};$$

$$\psi x = \psi y \text{ в } A_2 \Leftrightarrow \psi(u_1(z_3) + z_4) = \psi(u_2(w_1) + w_1') \text{ в } L(\hat{\varphi} Y)/E_{\psi(c+h(Y, c))} \Leftrightarrow$$

$$\Leftrightarrow \psi(u_1(z_3) + z_4) = \psi(u_2(w_1) + w_1') \text{ в } L(\hat{\varphi} Y)/E_{\varphi^* c + h(\hat{\varphi} Y, \varphi^* c)}.$$

Для завершения доказательства леммы остается сослаться на 3).

## § 3. Запись условий изоморфизма в терминах разрешимости одной из систем матричных уравнений

Символом $1_i$ мы обозначаем единичную квадратную матрицу порядка $i$. Символом 0 мы обозначаем матрицу, все элементы которой — нули.

С каждой хорошей парой $(\hat{\varphi}, \varphi^*)$ мы эффективно свяжем сейчас совокупность $\Sigma(\hat{\varphi}, \varphi^*)$ квадратных матриц заранее заданных порядков с неизвестными элементами, совокупность $Ю(\hat{\varphi}, \varphi^*)$ матричных уравнений видов

$$\alpha\theta_1 = \theta_2\beta, \quad \theta_1 = \begin{pmatrix} 1_i & 0 \\ \varkappa & \theta_2 \end{pmatrix}, \quad \theta_1 = \begin{pmatrix} 1_i & 0 \\ 0 & \theta_2 \end{pmatrix}$$

и несколько совокупностей сравнений $Я_j(\hat{\varphi}, \varphi^*)$ видов $\theta_1 \equiv \alpha \pmod m$, где $m$ — натуральное число, $\theta_1$ и $\theta_2$ — из $\Sigma(\hat{\varphi}, \varphi^*)$, а $\alpha$ и $\beta$ — заданные прямоугольные целочисленные матрицы.

Основной результат параграфа

Теорема 1. *Полугруппы $A_1$ и $A_2$ тогда и только тогда изоморфны, когда найдется такая хорошая пара $(\hat{\varphi}, \varphi^*)$ и для каждой матрицы $\theta$ из $\Sigma(\hat{\varphi}, \varphi^*)$ найдется такая квадратная целочисленная с определителем $\pm 1$ матрица $\theta^0$ одинакового с $\theta$ порядка, что набор $\{\theta^0 | \theta \in \Sigma(\hat{\varphi}, \varphi^*)\}$ является решением совокупности уравнений $Ю(\hat{\varphi}, \varphi^*)$ и одной из совокупностей сравнений $Я_j(\hat{\varphi}, \varphi^*)$.*

Оставшаяся часть параграфа посвящена построению $\Sigma(\hat{\varphi}, \varphi^*)$ и $Ю(\hat{\varphi}, \varphi^*)$, $Я_j(\hat{\varphi}, \varphi^*)$ и доказательству теоремы 1.

Будем для $i = 1, 2$ и для $(Y, c) \in T(A_i, X_i)$ предполагать, что группа $G(Y, c)$ порождается элементами $y^1(Y, c), \dots, y^{l(Y, c)}(Y, c)$ и элементами конечного порядка из $G(Y, c)$, а элементы $y^1(Y, c), \dots, y^{l(Y, c)}(Y, c)$ независимы в $G(Y, c)$. Ясно, что $l(Y, c) = l(\hat{\varphi}Y, \varphi^*c)$ для $(Y, c) \in T(A_1, X_1)$. Пусть $\theta(P)$ — это квадратная матрица с неизвестными элементами порядка $l(P)$, а $\theta(Y, c)$ — квадратная матрица с неизвестными элементами порядка $l(Y, c)$.

Если $G$ — группа, $v \in G$, $n$ — отрицательное целое число, то под $nv$ мы понимаем, как обычно, такой элемент $u \in G$, что $u + (-n)v$ — нуль группы $G$.

Пусть $\psi$ — такой изоморфизм $A_1$ на $A_2$, что $\hat{\psi} = \hat{\varphi}$, а $\psi^* = \varphi^*$ для фиксированной на дальнейшее хорошей пары $(\hat{\varphi}, \varphi^*)$. Тогда, по лемме 4, для нерегулярного $x \in X_1$ в $A_2$

$$\psi x = \varphi^*(x) + \sum_{j=1}^{l(X_1\{x\}, x)} \lambda_j^0(x) y^j(\hat{\varphi}(X_1\{x\}), \varphi^* x) + u(x), \tag{16}$$

где $\lambda_j^0(x)$ — целые числа, а $u(x)$ — такой элемент из $L(\hat{\varphi}(X_1\{x\}))$, значение которого в $L(\hat{\varphi}(X_1\{x\}))/E_{\varphi^* x}$ имеет конечный порядок. В то же время для компоненты $P$ полугруппы $A_1$ в $A_2$

$$\psi y^i(P) = \sum_{j=1}^{l(P)} \theta_{ji}^0(P) \cdot y^j(\hat{\varphi}P) + u(y^i(P)), \tag{17}$$

где $\theta_{ji}^0(P)$ — целые числа, а $u(y^i(P))$ — элемент конечного порядка в $G(\hat{\varphi}P)$ из $X_2(\hat{\varphi}P)$. Изоморфизм $\psi$ для каждой $(Y, c) \in T(A_1, X_1)$ индуцирует изоморфизм $\psi(Y, c)$ группы $G(Y, c)$ на группу $G(\hat{\varphi}Y, \varphi^*c)$. При этом

$$\psi(Y, c)(y^i(Y, c)) = \sum_{j=1}^{l(Y,c)} \theta_{ji}^0(Y, c) \cdot y^j(\hat{\varphi}Y, \varphi^*c) + u(y^i(Y, c)) \tag{18}$$

в $G(\hat{\varphi}Y, \varphi^*c)$, где $\theta_{ji}^0(Y, c)$ — целые числа, а $u(y^i(Y, c))$ — элемент конечного порядка в $G(\hat{\varphi}Y, \varphi^*c)$.

Ясно, что $\det \theta^0(P) = \pm 1$ для каждой компоненты $P$ полугруппы $A_1$ и $\det \theta^0(Y, c) = \pm 1$ для каждой $(Y, c) \in T(A_1, X_1)$. Изоморфизмы $\psi(Y, c)$ должны быть согласованы с $\psi$. Должны также выполняться условия 3) — 5) леммы 7. Как показано в лемме 7, это необходимо и достаточно для того, чтобы $\psi$ был изоморфизмом $A_1$ на $A_2$.

Итак, с хорошей парой $(\hat{\varphi}, \varphi^*)$ связываются целочисленные квадратные с определителем $\pm 1$ матрицы $\theta^0(P)$, $\theta^0(Y, c)$, целочисленные векторы $\lambda^0(x)$ и дополнительное отображение, которое взаимно однозначно отображает элементы конечного порядка из $G(P)$ на элементы конечного порядка из $G(\hat{\varphi P})$, элементы конечного порядка из $G(Y, c)$ на элементы конечного порядка из $G(\hat{\varphi Y}, \varphi^* c)$, а каждому $y^i(P)$ ставит в соответствие элемент конечного порядка из $G(\hat{\varphi P})$ и каждому $y^i(Y, c)$ — элемент конечного порядка из $G(\hat{\varphi Y}, \varphi^* c)$ и, кроме того, каждому нерегулярному $x$ из $X_1$ — элемент конечного порядка из $L(X_2\{\varphi^* x\})/E_{\varphi^* x}$. Всего существует конечное число дополнительных отображений, и каждое из них при заданных $\lambda^0(x)$, $\theta^0(P)$, $\theta^0(Y, c)$ определяет свое $\psi$.

Если $y$ — регулярный элемент из $Y$ и $y$ лежит в компоненте $P$, то $X_1(P) \subseteq Y$. Пусть в $G(Y, c)$

$$y^i(P) = \sum_{j=1}^{l(Y,c)} \alpha_{ji}(P, Y, c) \cdot y^j(Y, c) + v(y^i(P)),$$

где $v(y^i(P))$ — элемент конечного порядка, а в $G(\hat{\varphi Y}, \varphi^* c)$

$$y^i(\hat{\varphi P}) = \sum_{j=1}^{l(Y,c)} \beta_{ji}(P, Y, c) \cdot y^j(\hat{\varphi Y}, \varphi^* c) + v(y^i(\hat{\varphi P})),$$

где $v(y^i(\hat{\varphi P}))$ — опять элемент конечного порядка. Тогда в $G(\hat{\varphi Y}, \varphi^* c)$

$$\psi(Y, c)(y^i(P)) = \sum_{j=1}^{l(Y,c)} \alpha_{ji}(P, Y, c) \sum_{k=1}^{l(Y,c)} \theta^0_{kj}(Y, c) \cdot y^k(\hat{\varphi Y}, \varphi^* c) + u_1,$$

где элемент $u_1$ имеет конечный порядок, а, с другой стороны,

$$\psi(Y, c)(y^i(P)) = \sum_{j=1}^{l(P)} \theta^0_{ji}(P) \sum_{k=1}^{l(Y,c)} \beta_{kj}(P, Y, c) \cdot y^k(\hat{\varphi Y}, \varphi^* c) + u_2,$$

где $u_2$ — элемент конечного порядка. Значит, матрицы $\theta^0(P)$ и $\theta^0(Y, c)$ должны удовлетворять уравнению

$$\beta(P, Y, c) \cdot \theta(P) = \theta(Y, c) \cdot \alpha(P, Y, c), \tag{19}$$

где $\alpha(P, Y, c)$, $\beta(P, Y, c)$ — определенные выше прямоугольные целочисленные матрицы. Понятно, что это уравнение не зависит от дополнительного отображения. При заданном дополнительном отображении вычисляются также $u_1$ и $u_2$, которые должны совпадать. Если $m$ — общее кратное порядков элементов конечного порядка групп $G(P)$, $G(Y, c)$, то выполнимость равенства $u_1 = u_2$ зависит только от вычетов по модулю $m$, к которым принадлежат элементы матриц $\theta^0(P)$, $\theta^0(Y, c)$. Значит, для справедливости равенства $u_1 = u_2$ матрицы $\theta^0(P)$, $\theta^0(Y, c)$, кроме уравнения (19), должны еще удовлетворять одной из конечного числа систем сравнений. Это же замечание относится и к разбираемым далее условиям, и мы его больше уже не повторяем.

Если $y$ — нерегулярный элемент из $Y$, то $(X_1\{y\}, y)$ является координатной парой, меньшей $(Y, c)$, и можно предполагать, что для нее условия согласованности уже изучены. Пусть

$$y^i(X_2\{\varphi^* y\}, \varphi^* y) = \sum_{j=1}^{l(Y,c)} \beta_{ji}(y, Y, c) \cdot y^j(\hat{\varphi} Y, \varphi^* c) + v_1, \tag{20}$$

$$\varphi^* y = \sum_{j=1}^{l(Y,c)} \gamma_j(y, Y, c) \cdot y^j(\hat{\varphi} Y, \varphi^* c) + v_2$$

в $G(\hat{\varphi} Y, \varphi^* c)$, где $v_1, v_2$ — элементы конечного порядка, а в $G(Y, c)$

$$y = \sum_{j=1}^{l(Y,c)} \delta_j(y, Y, c) \cdot y^j(Y, c) + v_3,$$

где $v_3$ — элемент конечного порядка. Учитывая (16) и (18), имеем

$$\psi(Y, c)(y) = \sum_{j=1}^{l(Y,c)} \delta_j(y, Y, c) \sum_{k=1}^{l(Y,c)} \theta^0_{kj}(Y, c) \cdot y^k(\hat{\varphi} Y, \varphi^* c) + u_1,$$

$$\psi(Y, c)(y) = \sum_{k=1}^{l(Y,c)} \Big(\gamma_k(y, Y, c) + \sum_{j=1}^{l(X_1\{y\}, y)} \lambda^0_j(y) \cdot \beta_{kj}(y, Y, c)\Big) \cdot y^k(\hat{\varphi} Y, \varphi^* c) + u_2$$

где $u_1, u_2$ — элементы конечного порядка.

Получается, что $\lambda^0(y), \theta^0(Y, c)$ удовлетворяют уравнению

$$\beta(y, Y, c) \cdot \lambda(y) + \gamma(y, Y, c) = \theta(Y, c) \cdot \delta(y, Y, c), \tag{21}$$

где $\beta(y, Y, c)$ — определенная выше целочисленная прямоугольная матрица, $\gamma(y, Y, c)$ и $\delta(y, Y, c)$ — столбцы целых чисел, а $\lambda(y)$ — столбец с неизвестными элементами. Это уравнение можно переписать в более удобной форме, предполагая, что в $G(Y, c)$

$$y^i(X_1\{y\}, y) = \sum_{j=1}^{l(Y,c)} \alpha_{ji}(y, Y, c) \cdot y^j(Y, c) + v_4, \tag{22}$$

где $v_4$ — элемент конечного порядка.

$\lambda^0(y)$ и $\theta^0(Y, c)$ тогда и только тогда удовлетворяют уравнению (21), когда существует такой столбец целых чисел $\lambda^0_1(y)$, что $\lambda^0(y)$, $\lambda^0_1(y)$ и $\theta^0(Y, c)$, $\theta^0(X_1\{y\}, y)$ удовлетворяют уравнениям

$$\begin{gathered}\begin{pmatrix} 1 & 0 \\ \lambda_1(y) & \theta(Y, c) \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & \alpha(y, Y, c) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \beta(y, Y, c) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda(y) & \theta(X_1\{y\}, y) \end{pmatrix}, \\ \begin{pmatrix} 1 & 0 \\ \gamma(y, Y, c) & 1_{l(Y,c)} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ \lambda_1(y) & \theta(Y, c) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \theta(Y, c) \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ \delta(y, Y, c) & 1_{l(Y,c)} \end{pmatrix},\end{gathered} \tag{23}$$

где $\lambda_1(y)$ — столбец с неизвестными элементами, имеющий $l(Y, c)$ элементов, а $\alpha(y, Y, c)$ — прямоугольная целочисленная матрица, определяемая равенствами (22).

Система (23) равносильна уравнению (21) вместе с

$$\theta(Y, c)\cdot\alpha(y, Y, c)=\beta(y, Y, c)\cdot\theta(X_1\{y\}, y). \tag{24}$$

То, что $\theta^0(Y, c)$ и $\theta^0(X_1\{y\}, y)$ должны удовлетворять уравнению (24), доказывается так же, как то, что $\theta^0(Y, c)$ и $\theta^0(P)$ удовлетворяют уравнению (19).

Из обозрения стр. 384—386 статьи [6] видно, что условие 3) сводится к уравнению

$$\sum_{y\in Y_{\text{нер}}}\beta(y, Y, c)\cdot\lambda(y)\cdot\varepsilon(y, Y, c)+\theta(Y, c)\eta(Y, c)=\tau(Y, c), \tag{25}$$

где $Y_{\text{нер}}$ — множество нерегулярных элементов из $Y$, а $\varepsilon(y, Y, c)$, $\eta(Y, c)$, $\tau(Y, c)$ — целочисленные прямоугольные матрицы, $\beta(y, Y, c)$ — ранее определенная целочисленная матрица. Надо при этом учитывать, что имеют место (12)—(14).

Совсем просто понять, что условия 4) и 5) все вместе для фиксированной $(Y, c)$ и любых $(Z, b)\in T(A_1, X_1)$, $v\in\mathfrak{A}_1(c, Y, A_1)$, $w\in\mathfrak{K}_1(b, c, Z, Y, A_1)$ водятся к уравнению

$$\sum_{y\in Y_{\text{нер}}[c]}\beta(y, Y, c)\cdot\lambda(y)\cdot\varepsilon_1(y, Y, c)+\theta(Y, c)\cdot\eta_1(Y, c)=\tau_1(Y, c), \tag{26}$$

где $\varepsilon_1(y, Y, c)$ — строка целых чисел, $\eta_1(Y, c)$ и $\tau_1(Y, c)$ — целочисленные прямоугольные матрицы, а $Y_{\text{нер}}[c]$ — множество таких нерегулярных элементов $y$ из $X_1$, для которых либо $y$ лежит в $Y$, либо $y$ в $L(X_1)$ делит $c$, либо $y$ делит $b$ для такой пары $(Z, b)\in T(A_1, X_1)$, что множество $\mathfrak{K}_1(b, c, Z, Y, A_1)$ не пусто. В этих случаях $X_1\{y\}\subseteq Y$, и можно найти такую целочисленную матрицу $\beta(y, Y, c)$, что (20) выполняется для подходящего $v_1$ конечного порядка. Используя (21), перепишем (25) в виде $\theta(Y, c)\cdot\eta_2(Y, c)=\tau_2(Y, c)$, где $\eta_2(Y, c), \tau_2(Y, c)$ — целочисленные прямоугольные матрицы, а затем в виде

$$\begin{pmatrix}1_{k(Y,c)} & 0\\ 0 & \theta(Y, c)\end{pmatrix}\begin{pmatrix}1_{k(Y,c)} & 0\\ \eta_2(Y, c) & 1_{l(Y,c)}\end{pmatrix}=\begin{pmatrix}1_{k(Y,c)} & 0\\ \tau_2(Y, c) & 1_{l(Y,c)}\end{pmatrix}\begin{pmatrix}1_{k(Y,c)} & 0\\ 0 & \theta(Y, c)\end{pmatrix}, \tag{27}$$

где $k(Y, c)$ — число столбцов в $\tau_2(Y, c)$.

Для преобразования (26) к нужному виду заметим, что для $y\in Y_{\text{нер}}[c]$ тождественное вложение $X_1\{y\}$ в $Y$ индуцирует гомоморфизм $L(X_1\{y\})/E_y$ в $G(Y, c)$. Это очевидно, если $y\in Y$ или если $y$ делит $c$. Пусть $y$ делит $b$, а $\mathfrak{K}(b, c, Z, Y, A_1)$ непусто. Если $u, v\in L(X_1\{y\})$ и $y+u=y+v$ в $A_1$, то $b+u=b+v$ в $A_1$. Значит, в $A_1$ имеем $b+h(Z, b)+w+u=b+h(Z, b)+{}$ $+w+v$ для $w\in\mathfrak{K}(b, c, Z, Y, A_1)$. Отсюда в $A_1$ имеем $c+h(Y, c)+u_1(w)+{}$ $+u=c+h(Y, c)+u_1(w)+v$. Значит, в $A_1$ $c+h(Y, c)+u=c+h(Y, c)+v$. Поэтому в $G(Y, c)$ значения $u$ и $v$ равны.

Предполагая выполненными равенства (20) и (22) и повторяя вычисления, аналогичные тем, которые мы проводили при выводе уравнения (19), получим, что $\theta^0(Y, c)$ и $\theta^0(X_1\{y\}, y)$ удовлетворяют уравнению (24).

Пусть теперь $Y_{\text{нер}}[c] = \{y_1, \ldots, y_l\}$, а $\lambda_1(Y, c)$ — прямоугольная матрица с неизвестными элементами, имеющая $l$ столбцов и $l(Y, c)$ строк. Пусть $\varepsilon_1(Y, c)$ — целочисленная матрица, строками которой являются $\varepsilon_1(y_1, Y, c), \ldots, \varepsilon_1(y_l, Y, c)$. Простые вычисления показывают, что вместо уравнения (26) можно взять систему уравнений, состоящую из первых из уравнений (23) для $y \in Y_{\text{нер}}[c]$ и следующих уравнений:

$$\begin{pmatrix} 1_l & 0 \\ \lambda_1(Y, c) & \theta(Y, c) \end{pmatrix} \cdot \begin{pmatrix} \eta_i(l) & 0 \\ 0 & 1_{l(Y,c)} \end{pmatrix} = \begin{pmatrix} \eta_i(l) & 0 \\ 0 & 1_{l(Y,c)} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda_1(y_i) & \theta(Y, c) \end{pmatrix} \tag{28}$$

для $i = 1, \ldots, l$, где $\eta_i(l)$ — столбец целых чисел, имеющий $l$ элементов, $i$-й из которых равен 1, а остальные — нулю,

$$\begin{pmatrix} 1_l & 0 \\ \lambda_1(Y, c) & \theta(Y, c) \end{pmatrix} \cdot \begin{pmatrix} \varepsilon_1(Y, c) \\ \eta_1(Y, c) \end{pmatrix} = \begin{pmatrix} \varepsilon_1(Y, c) \\ \tau_1(Y, c) \end{pmatrix}. \tag{29}$$

Действительно, из (28) получается, что $\lambda_1(Y, c) = (\lambda_1(y_1), \ldots, \lambda_1(y_l))$, из первых из уравнений (23) получается, что $\lambda_1(y_i) = \beta(y_i, Y, c) \cdot \lambda(y_i)$, а потому (29) равносильно (26).

Теперь ясно, что в качестве $\Sigma(\hat{\varphi}, \varphi^*)$ надо взять

$$\{\theta(P), \theta(Y, c), \theta_1(Y, c), \theta_2(Y, c), \theta_3(Y, c), \theta_4(y, Y, c), \theta_5(z) \mid (Y, c) \in T(A_1, X_1);$$

$P$ — компонента в $A_1$; $y \in Y_{\text{нер}}[c]$; $z$ — нерегулярный элемент из $X_1\}$, а в качестве $Ю(\hat{\varphi}, \varphi^*)$ надо взять совокупность, состоящую из всех построенных уравнений (19), (24), (23), (27), (28), (29), в которых писать $\theta_1(Y, c)$ вместо $\begin{pmatrix} 1 & 0 \\ 0 & \theta(Y, c) \end{pmatrix}$, $\theta_2(Y, c)$ вместо $\begin{pmatrix} 1_{k(Y,c)} & 0 \\ 0 & \theta(Y, c) \end{pmatrix}$, $\theta_3(Y, c)$ вместо $\begin{pmatrix} 1_l & 0 \\ \lambda_1(Y,c) & \theta(Y,c) \end{pmatrix}$, $\theta_4(y, Y, c)$ вместо $\begin{pmatrix} 1 & 0 \\ \lambda_1(y) & \theta(Y,c) \end{pmatrix}$, $\theta_5(z)$ вместо $\begin{pmatrix} 1 & 0 \\ \lambda(z) & \theta(X_1\{z\}, z) \end{pmatrix}$, а также из уравнений

$$\theta_1(Y, c) = \begin{pmatrix} 1 & 0 \\ 0 & \theta(Y, c) \end{pmatrix}, \quad \theta_2(Y, c) = \begin{pmatrix} 1_{k(Y,c)} & 0 \\ 0 & \theta(Y, c) \end{pmatrix},$$

$$\theta_3(Y, c) = \begin{pmatrix} 1_l & 0 \\ \lambda_1(Y, c) & \theta(Y, c) \end{pmatrix},$$

$$\theta_4(y, Y, c) = \begin{pmatrix} 1 & 0 \\ \lambda_1(y) & \theta(Y, c) \end{pmatrix}, \quad \theta_5(z) = \begin{pmatrix} 1 & 0 \\ \lambda(z) & \theta(X_1\{z\}, z) \end{pmatrix}$$

для рассматриваемых $z$, $y$, $Y$, $c$. Этим заканчивается доказательство теоремы 1.

## § 4. Сведение проблемы изоморфизма к проблеме сопряженности

Через $GL(l, Z)$ мы обозначаем множество всех квадратных целочисленных с определителем $\pm 1$ матриц порядка $l$. Мы говорим, что конечные последовательности $(\alpha_1, \ldots, \alpha_k)$ и $(\beta_1, \ldots, \beta_k)$ из $GL(l, Z)$ сопряжены, если существует такой $\varphi \in GL(l, Z)$, что $\alpha_i\varphi = \varphi\beta_i$ для $i = 1, \ldots, k$.

Лемма. 8. *По заданным совокупности $\Sigma$ квадратных матриц с неизвестными элементами, но с заданными порядками, совокупности Ю матричных уравнений видов*

$$\alpha\theta_1 = \theta_2\beta, \ \theta_1 = \begin{pmatrix} \theta_2 & 0 \\ \varkappa & \theta_3 \end{pmatrix}, \ \theta_1 = \begin{pmatrix} \theta_2 & 0 \\ 0 & \theta_3 \end{pmatrix}, \ \theta_1 = 1_l \tag{30}$$

*и совокупности Я сравнений вида*

$$\theta_1 \equiv \alpha \pmod{m}, \tag{31}$$

*где $m$ — натуральное число; $\theta_1$, $\theta_2$ и $\theta_3$ — из $\Sigma$, а $\alpha$ и $\beta$ — заданные прямоугольные целочисленные матрицы, можно эффективно построить натуральные числа $k$ и $l$ и такие конечные последовательности $(\alpha_1, \ldots, \alpha_k)$, $(\beta_1, \ldots, \beta_k)$ элементов $GL(l, Z)$, что эти последовательности тогда и только тогда сопряжены, когда для каждой $\theta \in \Sigma$ существует такая целочисленная с определителем $\pm 1$ квадратная матрица $\theta^0$ одинакового с $\theta$ порядка, что набор $\{\theta^0 \mid \theta \in \Sigma\}$ является решением как совокупности уравнений Ю, так и совокупности сравнений Я.*

Доказательство. Пусть $\Sigma = \{\theta_1, \ldots, \theta_n\}$, $l(i)$ — порядок матрицы $\theta_i$, $\theta$ — квадратная матрица порядка $l$ с неизвестными элементами. Пусть Ю состоит из уравнений

$$\alpha_i\theta_{\varphi(i)} = \theta_{\psi(i)}\beta_i \qquad (i = 1, \ldots, n_1), \tag{32}$$

$$\theta_{\tau(i)} = \begin{pmatrix} \theta_{\rho_1(i)} & 0 \\ 0 & \theta_{\rho_2(i)} \end{pmatrix} \qquad (i = 1, \ldots, n_2), \tag{33}$$

$$\theta_{\tau(i)} = \begin{pmatrix} \theta_{\rho_1(i)} & 0 \\ \varkappa_i & \theta_{\rho_2'(i)} \end{pmatrix} \qquad (i = 1, \ldots, n_3), \tag{34}$$

$$\theta_i = 1_{l(i)} \qquad (i \in I_1;\ I_1 \subseteq \{1, \ldots, n\}), \tag{35}$$

а Я состоит из сравнений

$$\theta_i \equiv \gamma_i \pmod{m} \qquad (i \in I_2;\ I_2 \subseteq \{1, \ldots, n\}), \tag{36}$$

где $\varphi, \psi$ — отображения $\{1, \ldots, n_1\}$ в $\{1, \ldots, n\}$, $\tau, \rho_1, \rho_2$ — отображения $\{1, \ldots, n_3\}$ в $\{1, \ldots, n\}$, $n_2 \leqslant n_3$, $l(\psi(i)) = l(\rho_1(i)) + l(\rho_2(i))$, $\alpha_i$, $\beta_i$ — целочисленные прямоугольные $l(\psi(i)) \times l(\varphi(i))$-матрицы, $\nu_i$ — квадратная целочисленная матрица порядка $l(i)$, $\varkappa_i$ — прямоугольная $l(\rho_2(i)) \times \times l(\rho_1(i))$-матрица с неизвестными элементами. Будем предполагать, что $l(1)\leqslant\ldots\leqslant l(n)$. Не ограничивая общности, будем предполагать, что $\varphi(i)\neq\psi(i)$ для $i=1,\ldots,n_1$. Через $\theta^0$ будем обозначать целочисленную квадратную матрицу порядка $l$ с определителем $\pm1$. В качестве $l$ возьмем $9l_1$, где $l_1=l(1)+\ldots+l(n)$.

Разобьем матрицу $\theta$ на клетки. В полученной клеточной матрице будет по $6n$ строк клеток и по $6n$ столбцов клеток. Клетки, находящиеся в $(i+1)$-й строке (столбце), где $i+1=jn+j_1+1$, $j<3$, $j_1<n$, содержат элементы строк (столбцов) матрицы $\theta$ от $jl_1+l(1)+\ldots+l(j_1)+1$ до $jl_1+l(1)+\ldots+l(j_1)+l(j_1+1)$ при $j_1>0$ и строк (столбцов) от $jl_1+1$ до $jl_1+l(1)$ при $j_1=0$. Иначе, клетки первой строки (столбца) содержат по $l(1)$ строк (столбцов), клетки второй строки (столбца) содержат по $l(2)$ строк (столбцов) и т. д., клетки $n$-й строки (столбца) содержат по $l(n)$ строк (столбцов), а затем клетки $(n+1)$-й строки (столбца) содержат опять по $l(1)$ строк (столбцов) и т. д. до клеток $3n$-й строки (столбца) включительно. При $j=3,4,5$ клетки, находящиеся в строке (столбце) $jn+j_1+1$ для $j_1<n$, содержат по $2l(j_1+1)$ строк (столбцов).

Через $[\delta]_{ij}$ для целочисленной клеточной матрицы $\delta=\begin{pmatrix}\delta_{11} & \delta_{12}\\ \delta_{21} & \delta_{22}\end{pmatrix}$ далее будем обозначать целочисленную квадратную матрицу порядка $l$, разбитую на клетки так же, как и матрица $\theta$, у которой клетка, стоящая на пересечении $i$-го столбца клеток и $i$-й строки клеток есть $\delta_{11}$, $i$-го столбца и $j$-й строки — $\delta_{21}$, $j$-го столбца и $i$-й строки — $\delta_{12}$, $j$-го столбца и $j$-й строки — $\delta_{22}$, а остальные клетки вне главной диагонали — нулевые матрицы, а на главной диагонали — единичные матрицы. Аналогично понимается $[\delta]_{i_1,i_2,i_3}$ и $[\delta]_{i_1}$.

$\theta^0$ тогда и только тогда удовлетворяет уравнениям

$$\theta\cdot\left[\begin{pmatrix}1_{l(i)\cdot r(i_1)} & 0\\ 0 & (-1)_{l(j)\cdot r(j_1)}\end{pmatrix}\right]_{ni_1+i,nj_1+j}=\left[\begin{pmatrix}1_{l(i)\cdot r(i_1)} & 0\\ 0 & (-1)_{l(j)\cdot r(j_1)}\end{pmatrix}\right]_{ni_1+i,nj_1+j}\cdot\theta \tag{37}$$

для $i_1, j_1<6$, $0<i$, $j\leqslant n$, где $r(i)=1$ для $i=0,1,2$ и $r(i)=2$ для $i=3,4,5$, когда $\theta^0$ имеет клеточно-диагональную форму. Далее предполагаем, что $\theta^0$ удовлетворяет всем уравнениям (37) для указанных $i_1$, $j_1$, $i$, $j$.

Если $\theta^0$ удовлетворяем уравнениям

$$\theta\cdot\left[\begin{pmatrix}1_{l(\varphi(i))} & 0\\ \beta_i & 1_{l(\psi(i))}\end{pmatrix}\right]_{\varphi(i),\psi(i)}=\left[\begin{pmatrix}1_{l(\varphi(i))} & 0\\ \alpha_i & 1_{l(\psi(i))}\end{pmatrix}\right]_{\varphi(i),\psi(i)}\cdot\theta \tag{38}$$

для $i=1,\ldots,n_1$, а через $\theta_1^0,\ldots,\theta_n^0$ обозначены первые $n$ клеток главной диагонали $\theta^0$, то $\theta_1^0,\ldots,\theta_n^0$ удовлетворяют всем уравнениям (32). Наоборот, клеточно-диагональная матрица, у которой первые $n$ диагональных клеток удовлетворяют уравнениям (32), сама удовлетворяет уравнениям (38).

$\theta^0$ тогда и только тогда удовлетворяет уравнениям

$$\theta\cdot\left[\begin{pmatrix}1_{l(i_1)} & \delta_1\\ 0 & 1_{l(i_2)}\end{pmatrix}\right]_{i_1,i_2}=\left[\begin{pmatrix}1_{l(i_1)} & \delta_1\\ 0 & 1_{l(i_2)}\end{pmatrix}\right]_{i_1,i_2}\cdot\theta, \tag{39}$$

$$\theta \cdot \left[\begin{pmatrix} 1_{l(i_3)} & \delta_2 \\ 0 & 1_{l(i_2)} \end{pmatrix}\right]_{i_3, i_2} = \left[\begin{pmatrix} 1_{l(i_3)} & \delta_2 \\ 0 & 1_{l(i_2)} \end{pmatrix}\right]_{i_3, i_2} \cdot \theta, \qquad (40)$$

где $l(i_2) = l(i_1) + l(i_3)$, $\delta_1 = (1_{l(i_1)}\ 0)$, $\delta_2 = (0\ 1_{l(i_3)})$, для $i_1 = \rho_1(i)$, $i_2 = \tau(i)$, $i_3 = \rho_2(i)$ и $i = 1, \ldots, n_3$, когда $\theta_1^0, \ldots, \theta_n^0$ удовлетворяют уравнениям (34).

Если $\theta^0$, кроме того, удовлетворяет уравнениям

$$\theta \cdot \left[\begin{pmatrix} 1_{l(i_1)} & 0 \\ 0 & (-1)_{l(i_3)} \end{pmatrix}\right]_{i_2} = \left[\begin{pmatrix} 1_{l(i_1)} & 0 \\ 0 & (-1)_{l(i_3)} \end{pmatrix}\right]_{i_2} \cdot \theta \qquad (41)$$

для $i_2 = \tau(1), \ldots, \tau(n_2)$, то $\theta_1^0, \ldots, \theta_n^0$ удовлетворяют также уравнениям (33). Наоборот, если $\theta_1^0, \ldots, \theta_n^0$ удовлетворяют уравнениям (33), то $\theta^0$ удовлетворяет уравнениям (41) при указанных значениях $i_2$.

Обозначим для $i = n+1, \ldots, 2n$ через $\varepsilon_{i-n}$ клетку, стоящую на $i$-м месте главной диагонали $\theta$. Пусть $\eta_{ij}$ — квадратная матрица порядка $l$, у которой на главной диагонали стоят числа 1, а все элементы вне главной диагонали, кроме элемента, стоящего на пересечении $i$-й строки и $j$-го столбца, — нули. Элемент, находящийся одновременно в $j$-м столбце и $i$-й строке матрицы $\eta_{ij}$, равен 1. $\theta^0$ удовлетворяет уравнениям

$$\theta \cdot \eta_{ij} = \eta_{ij} \cdot \theta \qquad (42)$$

для $i = l_1 + 1, \ldots, l_1 + l_1$ и $j = l_1 + 1, \ldots, l_1 + l_1$ тогда и только тогда, когда $\varepsilon_1^0 = 1_{l(1)}, \ldots, \varepsilon_n^0 = 1_{l(n)}$, либо $\varepsilon_1^0 = (-1)_{l(1)}, \ldots, \varepsilon_n^0 = (-1)_{l(n)}$.

$\theta^0$ удовлетворяет уравнениям (42) для $i, j = l(1) + \ldots + l(i_1 - 1) + 1, \ldots, l(1) + \ldots + l(i_1 - 1) + l(i_1)$, а также для $i, j = l_1 + l(1) + \ldots + l(i_1 - 1) + 1, \ldots, l_1 + l(1) + \ldots + l(i_1 - 1) + l(i_1)$ и для $i_1 \in I_1$, тогда и только тогда, когда

$$\theta_{i_1}^0 = \varepsilon_{i_1}^0 \quad (i_1 \in I_1). \qquad (43)$$

Осталось самое сложное — промоделировать в новой ситуации сравнения (36).

$\theta^0$ тогда и только тогда удовлетворяет уравнениям

$$\theta \cdot \left[\begin{pmatrix} 1_{l(i_1)} & 0 \\ 1_{l(i_1)} & 1_{l(i_1)} \end{pmatrix}\right]_{n+i_1, 2n+i_1} = \left[\begin{pmatrix} 1_{l(i_1)} & 0 \\ \gamma_{i_1} & 1_{l(i_1)} \end{pmatrix}\right]_{n+i_1, 2n+i_1} \cdot \theta \qquad (44)$$

для $i_1 \in I_2$, когда для таких $i_1$ имеем $\theta_{2n+i_1}^0 = \varepsilon_{i_1}^0 \cdot \gamma_{i_1}$.

$\theta^0$ тогда и только тогда удовлетворяет уравнениям (44), (39), (40) для $i_1 \in I_2$, $i_2 = 3n + i_1$, $4n + i_1$, $5n + i_1$ и $i_3 = 2n + i_1$, когда $\theta_{nj+i_1}^0$ имеет для $j = 3, 4, 5$ и $i_1 \in I_2$ вид

$$\begin{pmatrix} \theta_{i_1}^0 & 0 \\ \varkappa_{i_1, j}^0 & \varepsilon_{i_1}^0 \cdot \gamma_{i_1} \end{pmatrix}. \qquad (45)$$

$\theta^0$ тогда и только тогда для $i \in I_2$ удовлетворяет уравнениям

$$\theta \cdot \left[\begin{pmatrix} \begin{pmatrix} 1_{l(i)} & 0 \\ 0 & m_{l(i)} \end{pmatrix} & \begin{matrix} 1_{2l(i)} \\ 1_{2l(i)} \end{matrix} \end{pmatrix}\right]_{3n+i,4n+i} = \left[\begin{pmatrix} \begin{pmatrix} 1_{l(i)} & 0 \\ 0 & m_{l(i)} \end{pmatrix} & \begin{matrix} 1_{2l(i)} & 0 \\ & 1_{2l(i)} \end{matrix} \end{pmatrix}\right]_{3n+i,4n+i} \cdot \theta, \quad (46)$$

где $m_j$ — квадратная матрица порядка $j$, у которой все элементы вне главной диагонали — нули, а каждый элемент главной диагонали — это число $m$, когда

$$\varkappa_{i,4}^0 = m \cdot \varkappa_{i,3}^0. \quad (47)$$

$\theta^0$ тогда и только тогда для $i \in I_2$ удовлетворяет уравнениям

$$\theta \cdot \left[\begin{pmatrix} 1_{l(i)} & 0 & (1_{l(i)} \ \ 0) \\ 0 & 1_{l(i)} & (1_{l(i)} \ \ 1_{l(i)}) \\ 0 & 0 & 1_{2l(i)} \end{pmatrix}\right]_{i,2n+i,5n+i} = \left[\begin{pmatrix} 1_{l(i)} & 0 & (1_{l(i)} \ \ 0) \\ 0 & 1_{l(i)} & (0 \ \ 1_{l(i)}) \\ 0 & 0 & 1_{2l(i)} \end{pmatrix}\right]_{i,2n+i,5n+i} \cdot \theta,$$
$$(48)$$

когда

$$\varkappa_{i,5}^0 = \varepsilon_i^0 \cdot \gamma_i. \quad (49)$$

Наконец, $\theta^0$ тогда и только тогда для $i \in I_2$ удовлетворяет уравнениям

$$\theta \cdot \left[\begin{pmatrix} 1_{2l(i)} & 1_{2l(i)} \\ 0 & 1_{2l(i)} \end{pmatrix}\right]_{4n+i,5n+i} = \left[\begin{pmatrix} 1_{2l(i)} & \begin{pmatrix} 1_{l(i)} & 0 \\ (-1)_{l(i)} & 1_{l(i)} \end{pmatrix} \\ 0 & 1_{2l(i)} \end{pmatrix}\right]_{4n+i,5n+i} \cdot \theta, \quad (50)$$

когда

$$\varepsilon_i^0 \cdot \gamma_i - \theta_i^0 = m \cdot \varkappa_{i,3}^0. \quad (51)$$

Запишем теперь в виде последовательности уравнения (37), (38), (39), (40), (41), (42), (44), (46), (48), (50) для указанных значений параметров. Пусть $k$ — это общее число построенных уравнений. Для $i=1,\ldots,k$ через $\alpha_i$ обозначим целочисленную матрицу, фигурирующую в левой части $i$-го уравнения, а через $\beta_i$ — фигурирующую в правой части.

$\theta^0$ тогда и только тогда удовлетворяет уравнениям

$$\theta \cdot \alpha_i = \beta_i \cdot \theta \quad (i = 1, \ldots, k), \quad (52)$$

когда $\theta_1^0, \ldots, \theta_n^0$ удовлетворяют уравнениям (32) — (34), (43) и (51) (при подходящих $\varkappa_{i,3}^0$). Значит, если $\theta_1^0, \ldots, \theta_n^0$ имеют определитель $\pm 1$ и удовлетворяют *Ю* и *Я*, то система (52) имеет решение в $GL(l, Z)$. Наоборот, если система (52) имеет решение $\theta^0$ в $GL(l, Z)$ и $\varepsilon_1^0 = 1_{l(1)}$ для этого $\theta^0$, то $\theta_1^0, \ldots, \theta_n^0$ удовлетворяют *Я* и *Ю*. Если же $\varepsilon_1^0 = (-1)_{l(1)}$, то $-\theta_1^0, \ldots, -\theta_n^0$

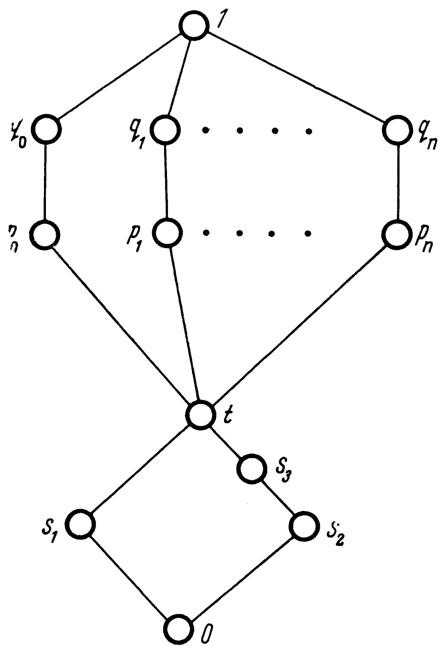
удовлетворяют *Я* и *Ю*. Остается заметить, что последовательности $(\alpha_1, \ldots, \alpha_k)$ и $(\beta_1, \ldots, \beta_k)$ тогда и только тогда сопряжены, когда имеет решение в $GL(l, Z)$ система (52).

Объединяя теорему 1 и лемму 8, получаем следующую теорему.

Теорема 2. *С каждой парой конечно определенных коммутативных полугрупп $A_1$ и $A_2$ можно эффективно сопоставить натуральные числа $l$ и $k$ и конечное число пар последовательностей длины $k$ элементов $GL(l, Z)$ так, что полугруппы $A_1$ и $A_2$ тогда и только тогда изоморфны, когда одна из сопоставленных пар является парой сопряженных последовательностей.*

## § 5. Сведение проблемы сопряженности к проблеме изоморфизма для регулярных полугрупп

Напомним, что полугруппа называется регулярной, если все ее элементы регулярны. Коммутативная полугруппа регулярна, если она порождается множеством, все элементы которого регулярны. Компоненты регулярной коммутативной полугруппы $A$ являются группами. Если $A$ конечно порождена, то эти группы тоже конечно порождены. Если $P, Q \in S(A)$ и $P \lhd^* Q$, а $o(Q)$ — нуль группы $Q$, то отображение $P$ в $Q$, переводящее $x$ в $x + o(Q)$, является гомоморфизмом $P$ в $Q$. Обозначим этот гомоморфизм через $\tau(P, Q)$. Ясно, что $\tau(P, P)$ — тождественное отображение $P$ на $P$. Набор гомоморфизмов $\{\tau(P, Q) \mid P, Q \in S(A); P \lhd^* Q\}$ удовлетворяет условиям $\tau(Q, R) \circ \tau(P, Q) = \tau(P, R)$ для любых $P \lhd^* Q$, $Q \lhd^* R$.




Пусть, напротив, задана конечная структура $\langle S; \leqslant \rangle$, каждому элементу $s \in S$ поставлена в соответствие конечно порожденная абелева группа $G_s$ и задан набор гомоморфизмов $\{\tau_{sr} : G_s \to G_r \mid s, r \in S, s \leqslant r\}$ так, что $G_s \cap G_t$ пусто для $s \neq t$ из $S$; для любых таких $t, s, r$ из $S$, что $t \leqslant s \leqslant r$, выполняются равенства $\tau_{sr} \circ \tau_{ts} = \tau_{tr}$ и гомоморфизм $\tau_{ss}$ является тождественным отображением $G_s$ на $G_s$ для любого $s \in S$. Тогда на множестве $A = \bigcup\limits_{s \in S} G_s$ определим операцию $+$, полагая $x + y$ для $x \in G_s$ и $y \in G_t$ равным сумме $\tau_{sr}(x)$ и $\tau_{tr}(y)$ в группе $G_r$, где $r$ — точная верхняя грань $s$ и $t$ в $S$. Непосредственно проверяется, что тогда $A$ будет регулярной конечно порожденной коммутативной полугруппой, множество $\{G_s \mid s \in S\}$ будет множеством компонент $A$, $\tau(G_s, G_t) = \tau_{st}$ для $s \leqslant t$, а $G_s \lhd^* G_t \Leftrightarrow s \leqslant t$. Если $s$ — наименьший элемент в $S$, то нуль группы $G_s$ будет нулем и в $A$. Если для $i=1, 2$ полугруппа $A_i$ определяется конечной структурой $S_i$, набором конечно порожденных абелевых групп $\{G_s(A_i) \mid s \in S_i\}$ и набором гомоморфизмов $\{\tau_{sr}(A_i): G_s(A_i) \to G_r(A_i) \mid s, r \in S_i; s \leqslant r\}$, а $\varphi$ — изоморфизм $A_1$ на $A_2$, то $\varphi$ индуцирует изоморфизм $\hat{\varphi}$ $S_1$ на $S_2$ и набор изоморфизмов

$$\{\varphi_s: G_s(A_1) \to G_{\hat{\varphi}(s)}(A_2) \mid s \in S_1\}, \tag{53}$$

где $\varphi(G_s(A_1)) = G_{\hat{\varphi}(s)}(A_2)$ и $\varphi_s(x) = \varphi(x)$ для $x \in G_s(A_1)$. При этом выполняются для любых $s < r$ из $S_1$ равенства

$$\varphi_r \circ \tau_{sr}(A_1) = \tau_{\hat{\varphi}(s), \hat{\varphi}(r)}(A_2) \circ \varphi_s. \tag{54}$$

Наоборот, изоморфизм $\hat{\varphi} S_1$ на $S_2$ вместе с набором изоморфизмов (53), удовлетворяющих для любых $s<r$ из $S_1$ равенствам (54), определяет изоморфизм $\varphi$ $A_1$ на $A_2$, если положить $\varphi(x) = \varphi_s(x)$ для любых $x \in G_s(A_1)$ и $s \in S_1$.

Теорема 3. *По натуральным числам $l$ и $n$ и по паре* $(\alpha_1, \ldots, \alpha_n)$, $(\beta_1, \ldots, \beta_n)$ *последовательностей элементов $GL(l, Z)$ можно эффективно построить две регулярные конечно порожденные коммутативные полугруппы $A_1$ и $A_2$ так, что $A_1$ тогда и только тогда изоморфна $A_2$, когда данные последовательности сопряжены.*

Доказательство. В качестве $S_1$ и $S_2$ возьмем структуру $S$, определяемую рисунком.

Для задания $A_1$ и $A_2$ надо еще каждому элементу $s \in S$ поставить в соответствии группы $G_s(A_1)$ и $G_s(A_2)$ и указать гомоморфизмы $\tau_{sr}(A_1) = \tau_{sr}(1)$, $\tau_{sr}(A_2) = \tau_{sr}(2)$ для $s < r$ из $S$. Сразу договоримся, что $G_s(A_1) = G_s(A_2) = G^s$ для всех $s \in S$. Для $s \in \{s_1, s_2, s_3, p_0, p_1, \ldots, p_n\}$ в качестве $G_s$ возьмем свободную абелеву группу с множеством $\{a^1(s), \ldots, a^l(s)\}$ свободных образующих. $G_t$ — свободная абелева группа с множеством $\{a^1(t), \ldots, a^l(t), b^1(t), \ldots, b^l(t)\}$ свободных образующих. Группы $G_0$ и $G_1$ одноэлементные, а группа $G_{q_i}$ циклическая порядка $2^i$ для $i = 0, 1, \ldots, n$. Гомоморфизмы $\tau_{s,r}(j)$ $(\langle s, r\rangle \in \{\langle 0, s_1\rangle, \langle 0, s_2\rangle, \langle s_2, s_3\rangle, \langle s_1, t\rangle, \langle s_3, t\rangle, \langle t, p_0\rangle, \langle p_i, q_i\rangle, \langle q_i, 1\rangle \mid i = 0, \ldots, n\})$ не зависят от $j \in \{1, 2\}$. При этом для $k = 1, \ldots, l$; $j = 1, 2$

$$\tau_{tp_0}(j)(a^k(t)) = a^k(p_0),\ \tau_{tp_0}(j)(b^k(t)) = a^k(p_0),\quad \tau_{s_1t}(j)(a^k(s_1)) = $$
$$= a^k(t),\ \tau_{s_3t}(j)(a^k(s_3)) = b^k(t),\ \tau_{s_2s_3}(j)(a^k(s_2)) = a^k(s_3).$$

Остальные из этих гомоморфизмов — нулевые. Далее для $k = 1, \ldots, l$; $i = 1, \ldots, n$ и $j = 1, 2$ имеем

$$\tau_{tp_i}(j)(a^k(t)) = a^k(p_i);\quad \tau_{tp_i}(1)(b^k(t)) = \sum_{m=1}^{l} \alpha^i_{mk} \cdot a^m(p_i);$$

$$\tau_{tp_i}(2)(b^k(t)) = \sum_{m=1}^{l} \beta^i_{mk} \cdot a^m(p_i),$$

где через $\alpha^i_{mk}$ и $\beta^i_{mk}$ мы обозначаем элементы матриц $\alpha_i$ и $\beta_i$, стоящие одновременно в $m$-й строке и в $k$-м столбце. $\tau_{sr}(j)$ в других случаях однозначно определяются из вышеприведенных условий. Так определенные $A_1$ и $A_2$ удовлетворяют заключению теоремы. Проверка этого сводится к рутинным вычислениям, и мы ее опускаем.

Следствие 1. *Следующие три алгоритмические проблема рекурсивно эквивалентны (и, значит, одна из них разрешима тогда и только тогда, когда разрешимы две другие):*

1) *проблема изоморфизма для коммутативных полугрупп;*

2) *проблема изоморфизма для регулярных коммутативных полугрупп;*

3) *проблема определения по натуральным числам $l$ и $n$ и по двум последовательностям длины $n$ элементов $GL(l, Z)$, сопряжены ли эти последовательности.*

Следствия 2. *По двум конечно определенным коммутативным полугруппам $A$ и $B$ можно эффективно построить конечное число пар конечно определенных регулярных коммутативных полугрупп так, что полугруппы $A$ и $B$ тогда и только тогда изоморфны, когда одна из построенных пар является парой изоморфных полугрупп.*

(Поступила в редакцию 26/III 1973 г.)

### Литература

1. А. Клиффорд, Г. Престон, Алгебраическая теория полугрупп, т. 1, Москва, изд-во «Мир», 1972.
2. А. Клиффорд, Г. Престон, Алгебраическая теория полугрупп, т. 2, Москва, изд-во «Мир», 1972.
3. В. А. Емеличев, Об алгоритмической разрешимости некоторых массовых проблем в теории коммутативных полугрупп, Сиб. матем. ж., **4**, **№ 4** (1963), 788—798.
4. М. А. Тайцлин, Об элементарных теориях коммутативных полугрупп, Алгебра и логика, **5**, **№ 4**, (1966), 55—89.
5. М. А. Тайцлин, Об алгоритмических проблемах для коммутативных полугрупп, ДАН СССР, **178**, **№ 4** (1968), 786—789.
6. М. А. Тайцлин, К проблеме изоморфизма для коммутативных полугрупп, Сиб. матем. ж., **9**, **№ 2** (1968), 375—401.
7. М. А. Тайцлин, Эквивалентность автоматов относительно коммутативной полугруппы, Алгебра и логика, **8**, **№ 5** (1969), 553—600.