Г. А. Баженова, О рациональных множествах в конечно порожденных нильпотентных группах,, *Алгебра и логика*, 2000, том 39, номер 4, 379–440

Алгебра и логика, 39, N 4 (2000), 379—394

УДК 512.54

О РАЦИОНАЛЬНЫХ МНОЖЕСТВАХ В КОНЕЧНО-ПОРОЖДЕННЫХ НИЛЬПОТЕНТНЫХ ГРУППАХ*)

Г. А. БАЖЕНОВА

Введение

Следуя [1], определяем класс рациональных подмножеств произвольного моноида M как минимальный класс, содержащий все конечные подмножества M и замкнутый относительно рациональных операций, т. е. объединения, произведения и порождения подмоноида. Выбирая в качестве моноида M группу G, получаем определение рациональных подмножеств G. Известен (см. [2]) другой подход к определению рациональных подмножеств, основанный на понятии рациональной структуры в группе. В § 4 мы доказываем, что два определения в некотором смысле эквивалентны тогда и только тогда, когда рациональные в смысле [1] подмножества G образуют булеву алгебру, т. е. класс, замкнутый относительно объединения, пересечения, взятия дополнения и теоретико-множественной разности множеств (поскольку объединение входит в число рациональных операций, достаточно говорить о замкнутости класса рациональных множеств относительно взятия дополнения).

Известно (см., например, [1]), что рациональные подмножества свободного конечно-порожденного (к. п.) моноида образуют булеву алгебру. Нетрудно также показать, что рациональные подмножества свободной

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект N 98-01-00932.

группы конечного ранга — булева алгебра. В данной статье доказывается, что рациональные подмножества к. п. нильпотентной группы G образуют булеву алгебру тогда и только тогда, когда группа G почти абелева.

Кроме того, изучается, когда множества решений уравнений в к. п. нильпотентных группах не являются рациональными. Приводится пример уравнения от одной переменной в свободной нильпотентной группе ранга два и ступени три, множество решений которого не будет рациональным (пример 1), это решает известную в данной области проблему о существовании таких уравнений над к. п. нильпотентными группами.

§ 1. Основные определения

ОПРЕДЕЛЕНИЕ 1. Пусть M — моноид. По индукции определим классы $\mathcal{R}_i, i = 0, 1, \dots$, подмножеств из M следующим образом:

1. $\mathcal{R}_0$ — это класс всех конечных подмножеств из M.

2. Если классы $\mathcal{R}_0, \dots, \mathcal{R}_n$ уже определены, то $\mathcal{R}_{n+1}$ — класс всех множеств $S \subseteq M$ таких, что S не принадлежит ни одному из классов $\mathcal{R}_0, \dots, \mathcal{R}_n$, но существуют множества $T_1 \in \mathcal{R}_k$, $T_2 \in \mathcal{R}_l$, $0 \leqslant k, l \leqslant n$ такие, что либо $S = T_1 \cup T_2$, либо $S = T_1T_2 = \{ab \mid a \in T_1, b \in T_2\}$, либо $S = T_1^* = \{1\} \cup T_1 \cup T_1T_1 \cup T_1T_1T_1 \cup \dots$.

Объединение всех классов $\mathcal{R}_i, i = 0, 1, \dots$, называется классом *рациональных подмножеств* M и обозначается $\mathcal{R}(M)$. Если множество $S \subseteq M$ принадлежит $\mathcal{R}_k$, то число k будем называть *сложностью* множества S. Хорошо известно описание рациональных множеств с помощью конечных автоматов.

ОПРЕДЕЛЕНИЕ 2. *Конечным автоматом* Γ над моноидом M называется четверка (Q, q_0, Q_t, Ω), где Q — конечное множество (*множество вершин*), q_0 — элемент Q (*начальная вершина*), Q_t — подмножество Q (*множество выходных вершин*), Ω — конечное подмножество декартова произведения $Q \times M \times Q$ (*множество стрелок*).

Правильный путь π в автомате Γ — это конечная последовательность стрелок вида $\omega_1, \dots, \omega_n$, где $\omega_i = (q_{i-1}, m_i, q_i)$, причем $q_n \in Q_t$. *Меткой* *стрелки* ω_i называется элемент m_i. *Меткой пути* π называется произведение $m_1 \cdots m_n$. Говорят, что автомат Γ *задает* множество $R \subseteq M$, если R — это множество меток всех правильных путей автомата Γ.

ТЕОРЕМА 1. *Пусть M — моноид. Тогда любой конечный автомат над M задает рациональное подмножество M, и наоборот, любое рациональное подмножество M задано некоторым автоматом.*

Следующая лемма, в основе которой лежит хорошо известная идея, дает полезное необходимое условие, при котором множество будет рациональным.

ЛЕММА 1. *Пусть M — моноид, и $R \in \mathcal{R}(M)$. Тогда:*

1) *либо R конечно, либо существуют такие u, v, w из M, что $v \neq 1$ и для всех целых $n \geqslant 0$ элемент $uv^n w$ принадлежит R;*

2) *существуют такие конечные множества $T_0, T_1 \subseteq M$, что $1 \notin T_1$ и любое r из $R \setminus T_0$ можно представить в виде $r = utv$, где $t \in T_1$ и $ut^*v \subseteq R$.*

ДОКАЗАТЕЛЬСТВО. Ясно, что п. 1 следует из п. 2. Докажем п. 2. Пусть R задано с помощью конечного автомата Γ. Число правильных путей без петель в Γ конечно. Пусть T_0 — множество их меток. Множество петель, не содержащих подпетли, также конечно. Пусть T_1 — множество их меток, отличных от единицы. Если $r \in (R \setminus T_0)$, пусть $\pi = \omega_1, \ldots, \omega_n$, $\omega_i = (q_{i-1}, m_i, q_i)$ — кратчайший правильный путь в Γ с меткой r. Существуют индексы $0 \leqslant i < j \leqslant n$ такие, что $q_i = q_j$ и $q_i, \ldots, q_{j-1}$ попарно различны. Положим $u = m_1 \cdots m_i$, $t = m_{i+1} \cdots m_j$, $v = m_{j+1} \cdots m_n$. Заметим, что $t \neq 1$, иначе путь не был бы кратчайшим. Тогда $t \in T_1$, кроме того, $ut^*v \subseteq R$. Лемма доказана.

Пусть $M_1 \subseteq M_2$ — моноиды, $R \subseteq M_1$. Если R — рациональное подмножество M_1, то оно — рациональное подмножество M_2. Обратное, вообще говоря, неверно. Однако, как показывает следующее предложение, если M_1 и M_2 являются группами, то верно и обратное.

ПРЕДЛОЖЕНИЕ 1. *Пусть $H \leq G$ — группы, и множество $R \subseteq H$ принадлежит $\mathcal{R}(G)$. Тогда $R \in \mathcal{R}(H)$.*

ДОКАЗАТЕЛЬСТВО. Докажем индукцией по сложности $R \in \mathcal{R}(G)$, что $hRg \in \mathcal{R}(H)$ (для любых $h, g \in G$), если $hRg \subseteq H$.

Пусть $R = R_1R_2$, а для R_1 и R_2 утверждение верно. Можно считать R_1 и R_2 непустыми. Выберем $a \in R_1$ и $b \in R_2$. Пусть $hRg \subseteq H$. Тогда $hR_1bg \in \mathcal{R}(H)$ и $habg \in H$. Далее, $g^{-1}b^{-1}R_2g = (habg)^{-1}haR_2g \in \mathcal{R}(H)$. Значит, $hRg = (hR_1bg)(g^{-1}b^{-1}R_2g) \in \mathcal{R}(H)$.

Пусть $R = R_1^*$, и $hRg \subseteq H$. Тогда $hR_1h^{-1} = hR_1g(hg)^{-1} \in \mathcal{R}(H)$. Поэтому $(hR_1h^{-1})^* = hRh^{-1} \in \mathcal{R}(H)$ и $hRg = hRh^{-1}(hg) \in \mathcal{R}(H)$. Предложение доказано.

§ 2. Абелевы группы

В абелевых группах групповую операцию обозначаем знаком $+$.

ТЕОРЕМА 2. *Пусть G — почти абелева к. п. группа. Тогда $\mathcal{R}(G)$ — булева алгебра.*

ДОКАЗАТЕЛЬСТВО. Вначале установим ряд лемм.

ЛЕММА 2. *Пусть $A = Z^n$ — свободная абелева группа конечного ранга n. Тогда любое $R \in \mathcal{R}(A)$ можно представить в виде*

$$R = \bigcup_{i=1}^{k}(a_i + M_i), \tag{1}$$

где $k \geqslant 0$, $a_i \in A$, $M_i \subseteq A$ — к. п. моноид, $i = 1, \ldots, k$.

ДОКАЗАТЕЛЬСТВО. Поскольку $\{0\}$ — это к. п. моноид, то все конечные множества представимы в виде (1). Поэтому достаточно показать, что класс множеств, представимых в виде (1), замкнут относительно рациональных операций. Ясно, что он замкнут относительно суммы и объединения. Пусть R имеет вид (1). При всех $1 \leqslant i \leqslant k$ множество $(a_i + M_i)^* = \{0\} \cup a_i + (a_i^* + M_i)$ имеет вид (1), поскольку $a_i^* + M_i$ является к. п. моноидом. Тогда $R^* = \sum_{i=1}^{k}(a_i + M_i)^*$ — сумма множеств вида (1) и тоже имеет вид (1). Лемма доказана.

ОПРЕДЕЛЕНИЕ 3. Моноид M называется *свободным коммутативным*, если он либо тривиален, либо изоморфен моноиду

$$Z_+^n = \{(z_1, \ldots, z_n) \in Z^n \mid z_1 \geqslant 0, \ldots, z_n \geqslant 0\}.$$

Если $\varphi : Z_+^n \to M$ — изоморфизм, то $\varphi(1,0,\ldots,0)$, $\varphi(0,1,0,\ldots,0)$, …, $\varphi(0,\ldots,0,1)$ — *свободные порождающие* M.

ЛЕММА 3. *Пусть $A = Z^n$ — свободная абелева группа конечного ранга n. Тогда любое $R \in \mathcal{R}(A)$ можно представить в виде*

$$R = \bigcup_{i=1}^{k} (a_i + M_i), \tag{2}$$

где $k \geqslant 0$, $a_i \in A$, и $M_i \subseteq A$ — свободный коммутативный моноид, $i = 1, \ldots, k$.

ДОКАЗАТЕЛЬСТВО. Покажем индукцией по числу порождающих, что любой к. п. моноид M имеет вид (2). Пусть элементы $x_1, \ldots, x_s$, где $s > 1$, порождают M. Если x_i не являются свободными порождающими, то найдутся наборы целых неотрицательных чисел $n_1, \ldots, n_s, n'_1, \ldots, n'_s$ такие, что $\sum\limits_{i=1}^{s} n_i x_i = \sum\limits_{i=1}^{s} n'_i x_i$ и для некоторого i имеем $n_i \neq n'_i$. Для $i = 1, \ldots, s$ положим $\eta_i = |n_i - n'_i|$, $\varepsilon_i = \operatorname{sgn}(n_i - n'_i)$ (считаем $\operatorname{sgn}(0) = 0$), и пусть $y_i = \eta_i x_i$ при $\eta_i > 0$ и $y_i = x_i$ при $\eta_i = 0$. Пусть $Y = \{y_1, \ldots, y_s\}$. Существует конечное множество K такое, что $Y^* + K = M$. Значит, достаточно показать, что Y^* имеет вид (2). Известно, что $\sum\limits_{i=1}^{s} \varepsilon_i y_i = 0$, и найдется $\varepsilon_i \neq 0$. Иначе говоря, имеем $\sum\limits_{i \in I} y_i = \sum\limits_{i \in J} y_i$, где множества $I, J \subseteq \{1, \ldots, s\}$ не пересекаются и одно из них (скажем, I) непусто. Тогда

$$Y^* = \bigcup_{i \in I} \{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_s\}^*. \tag{3}$$

Действительно, пусть $u = \sum\limits_{i=1}^{s} l_i y_i$, где $l_i \in Z$ и $l_i \geqslant 0$. Положим $\lambda = \min\{l_i \mid i \in I\}$, и пусть $\lambda = l_j$, где $j \in I$. Можно считать, что $l_j > 0$. Тогда

$$u = \sum_{i \notin I} l_i y_i + \sum_{i \in I} (l_i - \lambda) y_i + \lambda \sum_{i \in I} y_i$$

$$= \sum_{i \notin I} l_i y_i + \sum_{i \in I} (l_i - \lambda) y_i + \lambda \sum_{i \in J} y_i.$$

Получим равенство (3). Значит, по индукции Y^* имеет вид (2). Лемма доказана.

ЛЕММА 4. *Пусть $A = Z^n$, $R \in \mathcal{R}(A)$, а $K \subseteq A$ конечно. Тогда $(R \setminus K) \in \mathcal{R}(A)$.*

ДОКАЗАТЕЛЬСТВО. Пусть R — свободный коммутативный моноид, и $X = \{x_1, \ldots, x_s\}$ — множество его свободных порождающих. Пусть $K = \left\{ \sum\limits_{i=1}^{s} \lambda_i x_i \right\}$ состоит из одного элемента. Тогда $R \setminus K = R_1 \cup R_2$, где $R_1 = \left\{ \sum\limits_{i=1}^{s} l_i x_i \mid 0 \leqslant l_i \leqslant \lambda_i \right\} \setminus K$ — конечно, а $R_2 = \bigcup\limits_{i=1}^{s} ((1 + \lambda_i) x_i + R)$. Лемма доказана.

ЛЕММА 5. *Пусть G — группа, $\lambda : G \to H$ — гомоморфизм. Тогда:*

1) *если $R \in \mathcal{R}(G)$, то $\lambda(R) \in \mathcal{R}(H)$;*

2) *если $R \in \mathcal{R}(H)$ и λ — эпиморфизм с к. п. ядром, то $\lambda^{-1}(R) \in \mathcal{R}(G)$.*

ДОКАЗАТЕЛЬСТВО. 1) Это утверждение хорошо известно (см. [1]).

2) Воспользуемя индукцией по сложности рационального множества. Если $R \subseteq H$ конечно, то $\lambda^{-1}(R) = \bigcup\limits_{i=1}^{N} g_i(\ker\lambda)$, где $g_1, \ldots, g_N \in G$. Поскольку $\ker\lambda \in \mathcal{R}(G)$ как к. п. подгруппа, имеем $\lambda^{-1}(R) \in \mathcal{R}(G)$. Далее, $\lambda^{-1}(X \cup Y) = \lambda^{-1}(X) \cup \lambda^{-1}(Y)$, $\lambda^{-1}(XY) = \lambda^{-1}(X)\lambda^{-1}(Y)$, $\lambda^{-1}(X^*) = \lambda^{-1}(X)(\lambda^{-1}(X))^* \cup (\ker\lambda)$. Лемма доказана.

ЛЕММА 6. *Пусть G — группа, $H \leq G$ — подгруппа конечного индекса, а $D = \{d_1, \ldots, d_N\} \subseteq G$ — такое, что $DH = G$. Тогда любое $R \in \mathcal{R}(G)$ можно представить в виде $R = \bigcup\limits_{i=1}^{N} d_i S_i$, где $S_1, \ldots, S_N \in \mathcal{R}(H)$.*

ДОКАЗАТЕЛЬСТВО. Сначала покажем, что для любого $R \in \mathcal{R}(G)$ выполняется $R \cap H \in \mathcal{R}(G)$. Пусть Γ — конечный автомат, задающий R. Пусть Q — множество его вершин, q_0 — начальная вершина, Q_t — множество выходных вершин. Построим автомат Γ', множество вершин которого образовано множеством: $Q \times \{Hg \mid g \in G\}$, а стрелки получаются из стрелок автомата Γ по правилу: $\omega = (q_1, g, q_2)$ "порождает" все возможные стрелки вида $\omega' = ((q_1, Hh), g, (q_2, Hhg))$. Начальной вершиной объявляется (q_0, H), а множеством выходных — $Q_t \times \{H\}$. Легко видеть, что Γ' задает $R \cap H$.

Пусть $R \in \mathcal{R}(G)$. Положим $S_i = H \cap d_i^{-1}R$, где $i = 1, \ldots, N$. Тогда $S_i \in \mathcal{R}(H)$, и $R = \bigcup\limits_{i=1}^{N} d_i S_i$. Лемма доказана.

ЛЕММА 7. *Пусть A — к. п. абелева группа, $R \in \mathcal{R}(A)$, а $K \subseteq A$ конечно. Тогда $R \setminus K \in \mathcal{R}(A)$.*

ДОКАЗАТЕЛЬСТВО. Группа A — прямая сумма конечной абелевой группы A_0 и свободной абелевой группы $A_1 \simeq Z^k$. По лемме 6, $R = \bigcup\limits_{a \in A_0} (a + R_a)$, где $R_a \in \mathcal{R}(A_1)$. Множество K можно представить в виде $K = \bigcup\limits_{a \in A_0} (a + K_a)$, где все $K_a \subseteq A_1$ конечны. Тогда $R \setminus K = \bigcup\limits_{a \in A_0} (a + (R_a \setminus K_a))$. По лемме 4 все $R_a \setminus K_a \in \mathcal{R}(A)$, поэтому $R \setminus K \in \mathcal{R}(A)$. Лемма доказана.

ЛЕММА 8. *Пусть $A = Z^n$ — свободная абелева группа конечного ранга. Пусть $M \subseteq A$ — свободный коммутативный моноид, $a \in A$. Тогда $A \setminus (a + M) \in \mathcal{R}(A)$.*

ДОКАЗАТЕЛЬСТВО. Так как $A \setminus (a + M) = (A \setminus M) + a$, то можно считать $a = 0$. Пусть $H = \langle M \rangle$. По лемме 7, $((A/H) \setminus \{0\}) \in \mathcal{R}(A/H)$. Тогда, по лемме 5, $A \setminus H \in \mathcal{R}(A)$. Покажем, что $H \setminus M \in \mathcal{R}(A)$. Пусть $u_1, \ldots, u_k$ — свободные порождающие моноида M. Тогда $u_1, \ldots, u_k$ свободно порождают $H \simeq Z^k$. Далее, $H \setminus M = \bigcup\limits_{i=1}^{k} (-u_i + (-u_i)^* + \sum\limits_{j \neq i} (u_j^* + (-u_j)^*)) \in \mathcal{R}(A)$. Поэтому $A \setminus M = ((A \setminus H) \cup (H \setminus M)) \in \mathcal{R}(A)$. Лемма доказана.

В силу лемм 3, 6 и 8 остается показать, что пересечение двух рациональных подмножеств свободной абелевой группы рационально. Для этого необходимо установить, что множества неотрицательных решений систем линейных уравнений с целыми коэффициентами рациональны.

ЛЕММА 9. *Пусть $A = Z^n$ — свободная абелева группа конечного ранга. Пусть задана произвольная система L линейных уравнений от n переменных с целыми коэффициентами. Тогда множество S ее решений $(x_1, \ldots, x_n) \in A$, для которых $x_i \geqslant 0$, $i = 1, \ldots, n$, рационально в A.*

ДОКАЗАТЕЛЬСТВО проводится индукцией по n. Случай $n = 1$

тривиален. Пусть $n \geqslant 2$. Сначала предположим, что L однородна. Пусть $X = (\xi_1, \dots, \xi_n) \in S$ — ненулевой. Положим $N = \max_i \xi_i$. Для $1 \leqslant i \leqslant n$, $0 \leqslant T \leqslant N$ положим $R_i(T) = \{(x_1, \dots, x_n) \in S \mid x_i = T\}$. По индукции эти множества рациональны. Проверим, что

$$S = X^* + \bigcup_{i=1}^{n} \bigcup_{T=0}^{N} R_i(T). \tag{4}$$

Действительно, пусть $Y = Y_0 = (y_1, \dots, y_n) \in S$. Положим $\mu = \min_i y_i$. Если μ больше N, то пусть $Y_1 = Y_0 - X$. Ясно, что Y_1 принадлежит S. Если минимальная координата вектора Y_1 все еще больше N, положим $Y_2 = Y_1 - X$ и т.д., пока не получим вектор $Y_r = Y - rX \in S$, у которого хотя бы одна координата не превосходит N. Поскольку $Y_r \in \bigcup_{i=1}^{n} \bigcup_{T=0}^{N} R_i(T)$, имеем $Y = rX + Y_r \in X^* + \bigcup_{i=1}^{n} \bigcup_{T=0}^{N} R_i(T)$. Итак, (4) доказано. Значит, S рационально.

Пусть L неоднородна. Можно считать $S \neq \varnothing$. Пусть $X = (\xi_1, \dots, \xi_n) \in (S \setminus \{0\})$. Определим N и $R_i(T), i = 1, \dots, n; T = 0, \dots, N$, так же, как выше. В силу тех же причин все $R_i(T)$ рациональны. Пусть S' — множество неотрицательных решений однородной системы, получающейся из L заменой всех свободных членов на нуль. По уже доказанному S' рационально. Так как

$$S = \bigcup_{i=1}^{n} \bigcup_{T=0}^{N} R_i(T) \cup (S' + X),$$

S будет рациональным. Лемма доказана.

ЛЕММА 10. *Пусть $A = Z^n$ — свободная абелева группа конечного ранга, $R_1, R_2 \in \mathcal{R}(A)$. Тогда $R_1 \cap R_2 \in \mathcal{R}(A)$.*

ДОКАЗАТЕЛЬСТВО. По лемме 3 достаточно рассмотреть случай $R_i = a_i + M_i, i = 1, 2$, где $a_i \in A$, $M_i \subseteq A$ — свободные коммутативные моноиды. Пусть $u_1^i, \dots, u_{k_i}^i$ — свободные порождающие моноида M_i, $i = 1, 2$. Положим $S = \Big\{(z_1^1, \dots, z_{k_1}^1, z_1^2, \dots, z_{k_2}^2) \mid z_i^j \in Z,\ z_i^j \geqslant 0,\ a_1 + \sum_{j=1}^{k_1} z_j^1 u_j^1 = a_2 + \sum_{j=1}^{k_2} z_j^2 u_j^2\Big\}$. По лемме 9, $S \in \mathcal{R}(Z^{k_1+k_2})$. Положим

$\lambda : (z_1^1, \ldots, z_{k_1}^1,\ z_1^2, \ldots, z_{k_2}^2) \mapsto \sum\limits_{j=1}^{k_1} z_j^1 u_j^1$. По лемме 5, $\lambda(S) \in \mathcal{R}(A)$. Тогда $R_1 \cap R_2 = \lambda(S) + a_1 \in \mathcal{R}(A)$. Лемма доказана.

ЛЕММА 11. *Пусть $A \simeq Z^n$ — свободная абелева группа конечного ранга, $R \in \mathcal{R}(A)$. Тогда $A \setminus R \in \mathcal{R}(A)$.*

ДОКАЗАТЕЛЬСТВО. Лемма следует из лемм 3, 8 и 10.

Завершим доказательство теоремы 2. Пусть $A \leq G$ — подгруппа конечного индекса и $A \simeq Z^k$. Пусть D — множество представителей левых смежных классов группы G по A. Тогда по лемме 6 любое $R \in \mathcal{R}(G)$ имеет вид $\bigcup\limits_{d \in D} dS_d$, где $S_d \in \mathcal{R}(A)$. Имеем $G \setminus R = \bigcup\limits_{d \in D} d(A \setminus S_d)$. Тогда, по лемме 11, $G \setminus R \in \mathcal{R}(G)$. Теорема доказана.

§ 3. Нильпотентные группы

ТЕОРЕМА 3. *Пусть G — к. п. нильпотентная группа. Тогда $\mathcal{R}(G)$ является булевой алгеброй в том и только в том случае, если группа G почти абелева.*

ДОКАЗАТЕЛЬСТВО. Достаточность следует из теоремы 2.

Ниже нам понадобится следующий хорошо известный факт.

ЛЕММА 12. *Если G — почти абелева к. п. нильпотентная группа, то центр группы G имеет в ней конечный индекс.*

Необходимость проверяется индукцией по ступени нильпотентности. Пусть G — нильпотентная группа ступени n. Из леммы 5 следует, что $\mathcal{R}(G/C)$ — булева алгебра (здесь C — центр группы G). По индукции группа G/C почти абелева, тогда по лемме 12 следующий за C член верхнего центрального ряда $\zeta_2(G)$ имеет конечный индекс в G. Покажем, что группа $\zeta_2(G)$ почти абелева. Достаточно показать, что при любых $x, y \in \zeta_2(G)$ порядок коммутатора $[x, y] = x^{-1}y^{-1}xy$ конечен (тогда коммутант $\zeta_2(G)$ конечен, и центр $\zeta_2(G)$ имеет конечный индекс). Если порядок у $[x, y]$ бесконеченый, то x, y — свободные порождающие свободной нильпотентной группы N ступени 2 и ранга 2. Любой $g \in N$ имеет вид

$$g = x^k y^l [x, y]^m, \tag{5}$$

где k, l, m — целые и определены однозначно. Обозначим через

$$R = (xy)^*([x, y]^* \cup [y, x]^*)$$

множество всех $g \in N$, для которых в формуле (5) $k = l \geqslant 0$. Далее, пусть $S = x^* y^*$ — это множество всех $g \in N$, для которых в формуле (5) $m = 0$, $k, l \geqslant 0$. Множество $R \cap S = \{x^n y^n \mid n \geqslant 0\}$ рационально, тогда по лемме 1 существуют такие $u, v \neq 1, w \in N$, что $uv^*w \subseteq R \cap S$. Положим $q = uvu^{-1}, r = uw$. Тогда $q^* r \subseteq R \cap S$. Пусть $q = x^k y^l [x, y]^m, r = x^\kappa y^\lambda [x, y]^\mu$. Тогда $q^n r = x^{nk+\kappa} y^{nl+\lambda} [x, y]^{nm+\mu-nl\kappa-\frac{1}{2}lkn(n-1)}$. Получаем для любого $n \geqslant 0$ равенства

$$nk + \kappa = nl + \lambda, \;\; nm + \mu - nl\kappa - (1/2)lkn(n-1) = 0,$$

откуда $k = l$, $kl = 0$, и $q = 1$. Полученное противоречие завершает доказательство.

§ 4. Связь двух определений рациональности

Следующее определение приводится и подробно изучается, например, в [2].

ОПРЕДЕЛЕНИЕ 4. Пусть G — к. п. группа, Δ — конечный алфавит, Δ^* — свободный моноид, $\lambda : \Delta^* \to G$ — сюръективный морфизм моноидов, $L \in \mathcal{R}(\Delta^*)$ и $\lambda(L) = G$. Тогда пару (Δ, λ) называют *выбором порождающих* для G, тройку (Δ, λ, L) — *рациональной структурой* на G. Множество $R \subseteq G$ называется *L-рациональным*, если $\lambda^{-1}(R) \cap L$ рационально. (Это не означает, что выбор порождающих фиксирован; имеется в виду, что "информация о Δ и λ содержится в L".)

Поскольку морфизмы моноидов переводят рациональные множества в рациональные, то L-рациональное (для некоторого L) множество рационально. С другой стороны, нетрудно привести пример подмножества Z^2, L-рационального для одного L, но не L-рационального при другоих L.

ПРЕДЛОЖЕНИЕ 2. *Пусть G — к. п. группа. Тогда эквивалентны следующие условия:*

1) $\mathcal{R}(G)$ — *булева алгебра*;

2) ***любое множество из класса*** $\mathcal{R}(G)$ ***является*** L***-рациональным при некотором*** L.

ДОКАЗАТЕЛЬСТВО. 1) $\Rightarrow$ 2). Пусть $R \in \mathcal{R}(G)$. Тогда $G \setminus R \in \mathcal{R}(G)$. Пусть Γ_1, Γ_2 — конечные автоматы над G, задающие соответственно множества R и $G \setminus R$. Пусть $g_1, \ldots, g_N$ — множество меток всех стрелок автоматов Γ_1 и Γ_2. Введем конечный алфавит $\Delta = \{\delta_1, \ldots, \delta_N\}$. Определим морфизм $\lambda : \Delta^* \to G$, полагая $\lambda(\delta_i) = g_i$. Пусть конечные автоматы Γ_1' и Γ_2' над Δ получаются из автоматов Γ_1 и Γ_2 соответственно заменой каждой метки g_i на соответствующую ей букву δ_i. Обозначим языки, заданные автоматами Γ_1' и Γ_2', через Λ_1 и Λ_2. Положим $L = \Lambda_1 \cup \Lambda_2$. Тогда L рационально, $\lambda(L) = G$, кроме того, $\lambda^{-1}(R) \cap L = \Lambda_1$ и $\lambda^{-1}(G \setminus R) \cap L = \Lambda_2$. Значит, множества R и $G \setminus R$ будут L-рациональными.

2) $\Rightarrow$ 1). Пусть $R \in \mathcal{R}(G)$. Тогда R является L-рациональным для некоторого L. Тогда $\Lambda = L \setminus (\lambda^{-1}(R) \cap L)$ рационально, поскольку рациональные подмножества к. п. свободного моноида образуют булеву алгебру. Отсюда $G \setminus R = \lambda(\Lambda)$ рационально. Предложение доказано.

§ 5. Множества решений уравнений в к. п. нильпотентных группах

ОПРЕДЕЛЕНИЕ 5. Уравнением от одной неизвестной x с коэффициентами в группе G называется выражение вида

$$g_1 x^{\varepsilon_1} \ldots g_n x^{\varepsilon_n} = 1, \text{ где } g_i \in G, \varepsilon_i = \pm 1 \ (i = 1, \ldots, n).$$

Известно (см. [3]), что в свободной группе конечного ранга множество решений любого уравнения от одной неизвестной рационально. Нетрудно доказать аналогичное утверждение для к. п. абелевых групп.

Ниже мы даем ответ на известный вопрос о рациональности множеств решений уравнений от одной неизвестной в классе к. п. нильпотентных групп: докажем, что любое уравнение от одной неизвестной в к. п.

двуступенно нильпотентной группе имеет рациональное множество решений, а также приведем пример уравнения от одной неизвестной в свободной трехступенно нильпотентной группе ранга два, множество решений которого не рационально.

ЛЕММА 13. *Пусть K — группа, G — ее подгруппа, H — нормальная подгруппа G, $[K,G] \subseteq H$, и периодическая часть абелевой группы G/H конечна. Предположим, что любое уравнение вида*

$$a_1 x^{\varepsilon_1} a_2 x^{\varepsilon_2} \cdots a_n x^{\varepsilon_n} = 1, \tag{6}$$

где $a_i \in K, \varepsilon_i = \pm 1, i = 1, \dots, n$, x — неизвестная, $s = \sum\limits_{i=1}^{n} \varepsilon_i \neq 0$, имеет в H конечное множество решений. Тогда в G множество решений любого уравнения вида (6) *конечно.*

ДОКАЗАТЕЛЬСТВО. Пусть S — множество решений (6) в G. Можно считать его непустым. Пусть $\xi, \eta \in S$. Элемент $v_\xi = a_1\xi^{\varepsilon_1} \cdots a_n\xi^{\varepsilon_n}$ можно представить в виде $v_\xi = \xi^s c_\xi a_1 \cdots a_n$, где $c_\xi \in [K,G]$. Аналогично $v_\eta = a_1\eta^{\varepsilon_1} \cdots a_n\eta^{\varepsilon_n} = \eta^s c_\eta a_1 \cdots a_n$, где $c_\eta \in [K,G]$. Поскольку $v_\xi = 1 = v_\eta$, то $\xi^s c_\xi = \eta^s c_\eta$ и $\eta^{-s}\xi^s = c_\eta c_\xi^{-1}$, а так как для некоторого $h \in H$ верно $\eta^{-s}\xi^s = (\eta^{-1}\xi)^s h$, то элемент $\overline{\eta^{-1}\xi}$ факторгруппы G/H имеет конечный порядок. Пусть $\overline{b_1}, \dots, \overline{b_m}$ — периодическая часть G/H. Тогда $\overline{\eta^{-1}\xi}$ равно некоторому $\overline{b_i}$, и $\xi \in D = \bigcup\limits_{i=1}^{m} \eta b_i H$. Пусть $Q_i, i = 1, \dots, m$, — множество решений уравнения

$$a_1(\eta b_i x)^{\varepsilon_1} \cdots a_n(\eta b_i x)^{\varepsilon_n} = 1$$

в H. По условию Q_i конечны. Кроме того, $S = \bigcup\limits_{i=1}^{m} \eta b_i Q_i$. Лемма доказана.

ЛЕММА 14. *Пусть K — к. п. нильпотентная группа. Тогда в K множество решений любого уравнения вида* (6) *конечно.*

ДОКАЗАТЕЛЬСТВО. Возьмем произвольный центральный ряд

$$1 = K_0 \leq K_1 \leq \cdots \leq K_l = K.$$

Докажем по индукции, что в K_i множество решений уравнения (6) конечно. Если для i утверждение верно, то по лемме 13, где в качестве G возьмем K_{i+1}, а в качестве H — K_i, оно верно и для $i+1$. Лемма доказана.

ЗАМЕЧАНИЕ. Хорошо известно, что к. п. нильпотентная группа без кручения K имеет центральный ряд, факторы которого — без кручения. Поэтому для такой группы леммы 13 и 14 можно уточнить: любое уравнение вида (6) либо не имеет решений, либо имеет единственное решение.

ПРЕДЛОЖЕНИЕ 3. *Пусть G — к. п. двуступенно нильпотентная группа. Тогда любое уравнение над G от одной неизвестной имеет в G рациональное множество решений.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим уравнение

$$a_1x^{\varepsilon_1}a_2x^{\varepsilon_2}\cdots a_nx^{\varepsilon_n} = 1, \tag{7}$$

где $a_i \in G$, $\varepsilon_i = \pm 1$, $i = 1, \ldots, n$. Если $\sum\limits_{i=1}^{n} \varepsilon_i \neq 0$, то по лемме 14 множество решений (7) конечно. Иначе (7) можно привести к виду $[a, x] = b$, где $a, b \in G$. Пусть ξ — решение (7). Тогда множество решений (7) равно $\mathcal{Z}(a)\xi$, где $\mathcal{Z}(a)$ — централизатор a. Поскольку $\mathcal{Z}(a)$ рационально как к. п. подгруппа, то предложение доказано.

ПРИМЕР 1. Пусть G — свободная трехступенно нильпотентная группа ранга 2 со свободными порождающими a, b. Множество S решений уравнения $[x, a] = [x, b, x]$ в G не рационально.

В самом деле, любой элемент $g \in G$ можно однозначно записать в виде

$$g = a^k b^l [a, b]^m [a, b, a]^r [a, b, b]^s, k, l, m, r, s \in Z. \tag{8}$$

Легко проверить, что условие $g \in S$ равносильно

$$\begin{cases} -l &= 0, \\ m &= k^2, \\ -l(l-1)/2 &= kl. \end{cases}$$

Пусть α, β — свободные порождающие свободной нильпотентной группы H ступени два и ранга два. Гомоморфизм $\lambda : G \to H$, заданный соотношениями $\lambda(a) = \alpha$, $\lambda(b) = \beta$, переводит множество S в множество $S' = \{\alpha^k[\alpha, \beta]^{k^2} \mid k \in Z\}$. Достаточно доказать, что множество S' не рационально. В противном случае по лемме 1 существуют такие $u, v \neq 1$, $w \in H$, что $uv^*w \subseteq S'$. Пусть $u = \alpha^{n_1}\beta^{n_2}[\alpha, \beta]^{n_3}$, $v = \alpha^{m_1}\beta^{m_2}[\alpha, \beta]^{m_3}$,

$w = \alpha^{r_1}\beta^{r_2}[\alpha,\beta]^{r_3}$. Из условия $uw \in S'$ получаем $n_2 + r_2 = 0$, из условия $uvw \in S'$ находим $n_2 + r_2 + m_2 = 0$ и $m_2 = 0$. Тогда при натуральном t имеем

$$uv^t w = \alpha^{n_1+tm_1+r_1}[\alpha,\beta]^{n_3+tm_3+r_3-n_2tm_1-n_2r_1}.$$

Так как uv^tw принадлежит S', то

$$(n_1 + tm_1 + r_1)^2 = n_3 + tm_3 + r_3 - n_2tm_1 - n_2r_1. \qquad (9)$$

Формула (9) — это равенство двух многочленов от t, справедливое при всех натуральных t. Тогда все коэффициенты этих многочленов должны совпадать. Отсюда $m_1 = 0$, $m_3 = 0$. Тогда $v = 1$. Полученное противоречие завершает рассмотрение.

Следующий пример показывает, что множества решений уравнений от большего числа неизвестных могут быть нерациональными уже в двуступенно нильпотентных группах.

ПРИМЕР 2. Пусть G — свободная нильпотентная группа ступени два и ранга два со свободными порождающими a, b. Тогда множество решений уравнения $[x,y] = 1$ не рационально в $G \times G$, т. е. множество $S = \{(x,y) \in G \times G \mid [x,y] = 1\}$ не рационально.

В самом деле, пусть $g = a^kb^m[b,a]^l$, $h = a^\kappa b^\mu[b,a]^\lambda \in G$. Элементы g и h коммутируют тогда и только тогда, когда $\begin{vmatrix} m & k \\ \mu & \kappa \end{vmatrix} = 0$. Отображение $G \times G \ni (g,h) \mapsto (k,m,\kappa,\mu) \in Z^4$ — гомоморфизм. Поэтому достаточно доказать, что $A = \left\{ (k,m,\kappa,\mu) \in Z^4 \;\middle|\; \begin{vmatrix} m & k \\ \mu & \kappa \end{vmatrix} = 0 \right\}$ не принадлежит $\mathcal{R}(Z^4)$. Если $A \in \mathcal{R}(Z^4)$, то по лемме 1 существуют такие конечные множества $D = \{d_1,\dots,d_n\}$ и $E = \{e_1,\dots,e_r\}$ из Z^4, что нулевой вектор не содержится в E и для любого вектора $v \in A \setminus D$ найдется некоторый $e_i \in E$ такой, что $v + Ne_i \in A$ для всех натуральных N. Построим вектор $v = (k,m,\kappa,\mu) \in A$, который не удовлетворяет этому условию. Обозначим $e_i = (e_i^1, e_i^2, e_i^3, e_i^4)$.

1) Пусть (k,m) — вектор вида $(1,m)$, $m \geqslant 1$, не пропорциональный ни одному из ненулевых векторов вида (e_i^1, e_i^2), (e_i^3, e_i^4).

2) Пусть $R = \{\rho \mid \text{для некоторого } i \text{ верно } (e_i^3, e_i^4) = \rho(e_i^1, e_i^2)\}$. Выберем натуральное $m' \neq 0$ такое, что $m' \notin R$ и $(1, m, m', mm') \notin D$. Положим $(\kappa, \mu) = (m', mm')$.

Пусть $e_j \in E$. Положим

$$\Delta(N) = \begin{vmatrix} 1 + Ne_j^1 & m + Ne_j^2 \\ m' + Ne_j^3 & mm' + Ne_j^4 \end{vmatrix} = N^2 \begin{vmatrix} e_j^1 & e_j^2 \\ e_j^3 & e_j^4 \end{vmatrix}$$

$$+ N \begin{vmatrix} e_j^1 & e_j^2 \\ m' & mm' \end{vmatrix} - N \begin{vmatrix} e_j^3 & e_j^4 \\ 1 & m \end{vmatrix}.$$

Если при всех целых $N \geqslant 1$ выполняется $\Delta(N) = 0$, то определитель $\begin{vmatrix} e_j^1 & e_j^2 \\ e_j^3 & e_j^4 \end{vmatrix}$ равен нулю, его строки пропорциональны и

$$0 = \begin{vmatrix} e_j^1 & e_j^2 \\ m' & mm' \end{vmatrix} - \begin{vmatrix} e_j^3 & e_j^4 \\ 1 & m \end{vmatrix} = \begin{vmatrix} m'e_j^1 & m'e_j^2 \\ 1 & m \end{vmatrix} - \begin{vmatrix} e_j^3 & e_j^4 \\ 1 & m \end{vmatrix}$$

$$= \begin{vmatrix} m'e_j^1 - e_j^3 & m'e_j^2 - e_j^4 \\ 1 & m \end{vmatrix} = 0.$$

Если вектор (e_j^1, e_j^2) нулевой, то вектор (e_j^3, e_j^4) ненулевой и пропорционален вектору $(1, m)$, что противоречит нашему выбору. Поэтому вектор (e_j^1, e_j^2) ненулевой и $(e_j^3, e_j^4) = \rho(e_j^1, e_j^2)$ для некоторого ρ. Тогда вектор $(m' - \rho)(e_j^1, e_j^2)$ пропорционален вектору $(1, m)$. Если $m' - \rho \neq 0$, то векторы (e_j^1, e_j^2) и $(1, m)$ пропорциональны, что противоречит нашему выбору. Если же $m' - \rho = 0$, то $m' \in R$, что опять-таки противоречит нашему выбору. Итак, множество A не рационально, поэтому множество S не рационально.

В заключение автор благодарит научного руководителя В. А. Романькова за поставленную задачу и Г. А. Носкова за полезное обсуждение.

ЛИТЕРАТУРА

1. *R. H. Gilman*, Formal Languages and Infinite Groups, in: Geometric and computational perspectives on infinite groups (DIMACS, Ser. Discrete Math. Theor. Comput. Sci., **25**), Providence, RI, Am. Math. Soc., 1996, 27—51.

2. *S. M. Gersten, H. B. Short*, Rational subgroups of biautomatic groups, Ann. Math., II. Ser., **134**, N 1 (1991), 125–158.

3. *Р. Линдон, П. Шупп*, Комбинаторная теория групп, М., Мир, 1980.

Адрес автора:

БАЖЕНОВА Галина Александровна,
РОССИЯ,
644116, г. Омск,
ул. Осоавиахимовская, д. 290, кв. 86.

Поступило 12 мая 1998 г.

Окончательный вариант
7 июня 1999 г.