УДК 512.552+519.713

©2012. **В. В. Скобелев**

ОБ АВТОМАТАХ НА МНОГООБРАЗИЯХ НАД КОЛЬЦОМ

Определены автоматы на многообразиях над конечным кольцом. Охарактеризованы гомоморфизмы таких автоматов в терминах гомоморфизмов многообразий в следующих двух основных случаях. В первом случае гомоморфизмы многообразий определены посредством гомоморфизмов заданных на них алгебр, а автоматы определены посредством унарных и бинарных операций этих алгебр. Во втором случае гомоморфизмы многообразий определены посредством гомоморфизмов множеств траекторий, определяемых полиномиальными параметризациями многообразий, функции переходов автоматов обеспечивают их движение по указанным траекториям, а функции выходов автоматов – отображения многообразия в модуль над кольцом.

Ключевые слова: *кольца, многообразия, автоматы.*

1. Введение. Известно, что основным объектом алгебраической геометрии является многообразие. Это понятие, первоначально определенное как множество решений конечной системы полиномиальных уравнений над полем, постепенно трансформировалось в процессе развития алгебраической геометрии: аффинное многообразие, квазипроективные и проективные многообразия, абстрактные алгебраические многообразия, схемы, алгебраические пространства [1, 2]. Глубокая внутренняя связь понятий многообразие и идеал (ассоциативно-коммутативного кольца полиномов над полем) стимулировала формирование раздела компьютерной алгебры, предназначенного для реализации алгоритмов коммутативной алгебры [3, 4], основанных на построении конечного базиса идеала, и имеющего многочисленные приложения [5].

Хотя основные результаты алгебраической геометрии, как математической теории, получены в предположении, что поле алгебраически замкнуто, следует особо выделить успешное применение эллиптических кривых над конечным полем при решении задач защиты информации. Как следствие, понятие многообразие (а эллиптическая кривая, как и любая алгебраическая кривая, является многообразием) послужило основой для формирования эллиптической криптографии – перспективного направления современной криптографии [6, 7].

С другой стороны, использование в процессе решения задач криптографии вычислений в кольцах вычетов [8, 9] стимулировало исследование автоматов над конечными кольцами [10, 11]. При этом особое значение имеет анализ сложности идентификации (параметрической и начального состояния) автомата, а также анализ структуры множеств неподвижных точек автоматных отображений. Эти задачи естественно сводятся к поиску решений систем уравнений с параметрами над кольцом, т.е. к исследованию многообразий над соответствующим кольцом.

Известно, что преобразования, осуществляемые конечными автоматами, являются математической моделью тех вычислений, которые могут быть реализованы на компьютерах в реальном времени. Поэтому исследование автоматов, определенных

на многообразиях над конечным кольцом, актуально как с позиции алгебраической теории автоматов, так и с позиции их возможного применения в процессе решения задач защиты информации. При этом особый интерес представляет вопрос о том, как (определенные тем или иным образом) гомоморфизмы многообразий отражаются на множествах автоматов, определенных на этих многообразиях.

Пусть $M = (Q, X, Y, \delta, \lambda)$ – абстрактный автомат, где Q, X, Y – множество состояний, входной и выходной алфавит, а $\delta : Q \times X \to Q$ и $\lambda : Q \times X \to Y$ – функции переходов и выходов (всюду в работе предполагается, что $Val\ \lambda = Y$). В общем случае гомоморфным образом автомата $M = (Q, X, Y, \delta, \lambda)$ называется такой автомат $M' = (Q', X', Y', \delta', \lambda')$, что существуют такие сюръекции $\chi_1 : Q \to Q'$, $\chi_2 : X \to X'$ и $\chi_3 : Q \to Y'$, что равенства $\chi_1(\delta(q, x)) = \delta'(\chi_1(q), \chi_2(x))$ и $\chi_3(\lambda(q, x)) = \lambda'(\chi_1(q), \chi_2(x))$ истинны для всех $q \in Q$ и $x \in X$. В частности, если χ_1, χ_2, χ_3 – биекции, то автоматы M и M' изоморфны.

Целью настоящей работы является характеристика гомоморфизмов автоматов, определенных на многообразиях над кольцом, в терминах гомоморфизмов многообразий. Рассмотрены два основные как с позиции теории, так и с позиции приложений случая. В первом случае гомоморфизмы многообразий определены посредством гомоморфизмов алгебр, заданных на многообразиях, а функции переходов и выходов автоматов определены через унарные и бинарные операции этих алгебр. Во втором случае гомоморфизмы многообразий определены посредством гомоморфизмов множеств траекторий на многообразиях, определяемых полиномиальными параметризациями многообразий, функции переходов автоматов обеспечивают движение автомата по указанным траекториям, а функции выходов автоматов – произвольные отображения многообразия в модуль над кольцом.

Все не определяемые в работе понятия – такие же, как в [11, 12].

2. Основные понятия. Всюду под кольцом $\mathcal{K} = (K, +, \cdot)$ ($|K| \geq 2$) понимается конечное ассоциативно-коммутативное кольцо с единицей. Обозначим через K^d ($K^d \subseteq K \backslash \{0\}$) множество всех делителей нуля кольца $\mathcal{K}$, а через K^{non-d} – множество всех ненулевых элементов кольца $\mathcal{K}$, не являющихся делителями нуля. Так как $(K^{non-d}, \cdot)$ – гауссова полугруппа, то существует (наименьшее) расширение $\widetilde{\mathcal{K}} = (\widetilde{K}, +, \cdot)$ кольца $\mathcal{K}$, в котором каждый элемент множества K^{non-d} обратим. Если $K^d = \emptyset$ (т.е. $\mathcal{K}$ – область целостности), то $\widetilde{\mathcal{K}}$ – поле (оно называется полем дробей кольца $\mathcal{K}$).

В соответствии с [11] определим многообразие над кольцом $\mathcal{K}$ следующим образом. Многообразием в K^n ($n \in \mathbf{N}$) назовем множество

$$\mathbf{V} = \{(v_1, \ldots, v_n) \in K^n | f_i(v_1, \ldots, v_n) = 0 \text{ для всех } i = 1, \ldots, m\}, \qquad (1)$$

где $f_1, \ldots, f_m \in K[\tau_1, \ldots, \tau_n]$ – попарно различные ненулевые многочлены. Чтобы подчеркнуть, что многообразие V определяется многочленами $f_1, \ldots, f_m$, используют запись $\mathbf{V}(\{f_i | i = 1, \ldots, m\})$. В дальнейшем рассматриваются только непустые многообразия. При $m = 1$ многообразие (1) называется гиперповерхностью, если $n \geq 3$, и (алгебраической) кривой, если $n = 2$.

Система уравнений, определяющая многообразие (1) над кольцом $\mathcal{K}$, может рассматриваться и над любым его расширением $\mathcal{K}'$. Соответствующее расширение многообразия $\mathbf{V}$ обозначают $\mathcal{K}'(\mathbf{V})$.

Для любых многообразий $\mathbf{V}_i = \mathbf{V}(\{f_j^{(i)} | j = 1, \ldots, m_j\})$ $(i = 1, 2)$ в K^n $(n \in \mathbf{N})$ истинны формулы:

$$\mathbf{V}_1 \cap \mathbf{V}_2 = \mathbf{V}(\{f_j^{(1)} | j = 1, \ldots, m_1\} \cup \{f_j^{(2)} | j = 1, \ldots, m_2\}), \tag{2}$$

$$\mathbf{V}_1 \cup \mathbf{V}_2 \subseteq \mathbf{V}(\{f_i^{(1)} f_j^{(2)} | i = 1, \ldots, m_1;\ j = 1, \ldots, m_2\}), \tag{3}$$

причем в (3) имеет место равенство, если кольцо $\mathcal{K}$ не содержит делителей нуля.

Многообразие $\mathbf{V}$ в K^n $(n \in \mathbf{N})$ назовем:

1) неприводимым, если для любых многообразий $\mathbf{V}_1$ и $\mathbf{V}_2$ в K^n из равенства $\mathbf{V} = \mathbf{V}_1 \cup \mathbf{V}_2$ вытекает, что $\mathbf{V} = \mathbf{V}_1$ или $\mathbf{V} = \mathbf{V}_2$;

2) неразложимым, если не существуют такие многообразия $\mathbf{V}_i$ $(i = 1, 2)$ в K^{n_i} $(n_1, n_2 \in \mathbf{N};\ n_1 + n_2 = n)$, что

$$\mathbf{V} = \mathbf{V}_1 \times \mathbf{V}_2. \tag{4}$$

Формулы (1)-(4) определяют алгебраическую систему на множестве всех многообразий над кольцом $\mathcal{K}$, предназначенную для исследования соотношений между многообразиями, как объектами. В то же время, сама по себе формула (1) мало что дает при исследовании свойств отображений многообразия в себя (напомним, что даже над полями $GF(2^k)$ поиск решений уравнения $f(\tau_1, \ldots, \tau_n) = 0$, где f – квадратичная форма, является NP-полной задачей). Поэтому при исследовании отображений многообразия в себя естественно ограничиться многообразиями $\mathbf{V}$ над кольцом $\mathcal{K}$, для которых выполнено одно из следующих двух условий.

Условие 1. Определена алгебра $(\mathbf{V}, \mathcal{F}_1 \cup \mathcal{F}_2)$, где $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ – множество унарных операций, а $\mathcal{F}_2 = \{\beta_1, \ldots, \beta_{k_2}\}$ – множество бинарных операций, причем каждая операция, принадлежащая множеству $\mathcal{F}_1 \cup \mathcal{F}_2$, вычислима за полиномиальное время.

Условие 2. Определена полиномиальная параметризация многообразия $\mathbf{V}$, т.е. задан такой набор многочленов $h_1, \ldots, h_n \in K[\tau_1, \ldots, \tau_m]$ $(m < n)$, что точки с координатами

$$\begin{cases} v_1 = h_1(\tau_1, \ldots, \tau_m) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ v_n = h_n(\tau_1, \ldots, \tau_m) \end{cases} \qquad ((\tau_1, \ldots, \tau_m) \in K^m)$$

принадлежат многообразию $\mathbf{V}$.

Там где это не вызывает недоразумений, будем компактно представлять полиномиальную параметризацию многообразия $\mathbf{V}$ в векторном виде, а именно:

$$\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})\ (\overrightarrow{\tau} \in K^m). \tag{5}$$

Замечание 1. Безусловным достоинством полиномиальной параметризации (5) является то, что зафиксировав легко вычислимое отображение $\theta : K^m \to K^m$,

мы тем самым определяем на многообразии $\mathbf{V}$ множество траекторий (т.е. последовательностей точек), элементы которых вычислимы за полиномиальное время. Действительно, для каждой точки $P_0 \in K^m$ однозначно определена траектория $P_0, P_1, \ldots, P_j, \ldots$ во множестве K^m, где $P_{j+1} = \theta(P_j)$ $(j \in \mathbf{Z}_+)$. В свою очередь, эта траектория однозначно определяет на многообразии $\mathbf{V}$ траекторию $\mathbf{h}(P_0), \mathbf{h}(P_1), \ldots, \mathbf{h}(P_j), \ldots$, точки которой вычислимы за полиномиальное время.

Множество всех многообразий над кольцом $\mathcal{K}$, удовлетворяющих условию 1, обозначим через $\mathcal{V}_1(\mathcal{K})$, а условию 2 – через $\mathcal{V}_2(\mathcal{K})$.

Пример 1. 1. Пусть эллиптическая кривая γ определена уравнением

$$v_2^2 + a_1 v_1 v_2 + a_3 v_2 = v_1^3 + a_2 v_1^2 + a_4 v_1 + a_6 \tag{6}$$

над областью целостности $\mathcal{K}$. Известно, что в поле дробей $\widetilde{\mathcal{K}}$ множество $\widetilde{\mathcal{K}}(\gamma)$ точек кривой (6) (включая бесконечно удаленную точку O) образует абелеву группу $(\widetilde{\mathcal{K}}(\gamma), +_\gamma)$, для которой точка O – нейтральный элемент. Таким образом, определена алгебра $(\widetilde{\mathcal{K}}(\gamma), \mathcal{F}_1 \cup \mathcal{F}_2)$, где $\mathcal{F}_2 = \{+_\gamma\}$, а множество унарных операций $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ $(1 \le k_1 < |\widetilde{\mathcal{K}}(\gamma)|)$ определено равенствами: $\alpha_0(P) = O$ $(P \in \widetilde{\mathcal{K}}(\gamma))$ и $\alpha_i(P) = \underbrace{P +_\gamma \ldots +_\gamma P}_{i \text{ раз}}$ $(P \in \widetilde{\mathcal{K}}(\gamma))$ для всех $i = 1, \ldots, k_1$, т.е. многообразие $\widetilde{\mathcal{K}}(\gamma) \subseteq \widetilde{K}^2$ принадлежит множеству $\mathcal{V}_1(\widetilde{\mathcal{K}})$.

2. Любая алгебраическая кривая $v_2 = a_0 v_1^n + a_1 v_1^{n-1} + \cdots + a_n$ над кольцом $\mathcal{K}$ может рассматриваться как полиномиально параметризованное многообразие

$$\begin{cases} v_1 = \tau \\ v_2 = a_0 \tau^n + a_1 \tau^{n-1} + \cdots + a_n \end{cases} \qquad (\tau \in K)$$

в K^2, т.е. как элемент множества $\mathcal{V}_2(\mathcal{K})$.

3. Автоматы на многообразии $\mathbf{V} \in \mathcal{V}_1(\mathcal{K})$. Так как $\mathbf{V} \in \mathcal{V}_1(\mathcal{K})$, то определена алгебра $(\mathbf{V}, \mathcal{F}_1 \cup \mathcal{F}_2)$, где $\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ – множество унарных операций, а $\mathcal{F}_2 = \{\beta_1, \ldots, \beta_{k_2}\}$ – множество бинарных операций. Системы уравнений

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_2)) \end{cases} \qquad (t \in \mathbf{Z}_+) \tag{7}$$

и

$$\begin{cases} \mathbf{q}_{t+1} = \beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t), \alpha_{x_{t+1}}(\mathbf{v}_1)) \\ \mathbf{y}_{t+1} = \beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}), \mathbf{v}_2) \end{cases} \qquad (t \in \mathbf{Z}_+), \tag{8}$$

где $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$ – фиксированные точки, $i_1, i_2 \in \mathbf{Z}_{k_1+1}$ и $j_1, j_2 \in \mathbf{N}_{k_2}$ – фиксированные числа, а $\mathbf{q}_0 \in \mathbf{V}$ и $x_{t+1} \in \mathbf{Z}_{k_1+1}$ $(t \in \mathbf{Z}_+)$, определяют множество автоматов, соответственно, $\mathcal{A}^{(1)}(\mathbf{V})$ Мили и $\mathcal{A}^{(2)}(\mathbf{V})$ Мура.

Замечание 2. Таким образом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ – соответственно, входной символ, состояние и выходной символ автомата $M \in \mathcal{A}^{(1)}(\mathbf{V}) \cup \mathcal{A}^{(2)}(\mathbf{V})$ в момент t.

Пусть $\mathbf{V}, \mathbf{U} \in \mathcal{V}_1(\mathcal{K})$ – такие многообразия, что для алгебр $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ и $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ ($\mathcal{F}_1^{(i)} = \{\alpha_0^{(i)}, \alpha_1^{(i)}, \ldots, \alpha_{k_1}^{(i)}\}$ $(i = 1, 2)$ и $\mathcal{F}_2^{(i)} = \{\beta_1^{(i)}, \ldots, \beta_{k_2}^{(i)}\}$ $(i = 1, 2)$ – множество, соответственно, унарных и бинарных операций) существует тройка отображений $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ $(\varphi_1 : \mathbf{V} \to \mathbf{U}, \varphi_2 : \mathcal{F}_1^{(1)} \to \mathcal{F}_1^{(2)}, \varphi_3 : \mathcal{F}_2^{(1)} \to \mathcal{F}_2^{(2)})$, где φ_1 – сюръекция, а φ_2 и φ_3 – биекции, для которой равенства

$$\varphi_1(\alpha(\mathbf{v}_1)) = \varphi_2(\alpha)(\varphi_1(\mathbf{v}_1)), \tag{9}$$

$$\varphi_1(\beta(\mathbf{v}_1, \mathbf{v}_2)) = \varphi_3(\beta)(\varphi_1(\mathbf{v}_1), \varphi_1(\mathbf{v}_2)) \tag{10}$$

истинны для всех $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{V}$, $\alpha \in \mathcal{F}_1^{(1)}$ и $\beta \in \mathcal{F}_2^{(1)}$. Тогда будем говорить, что:

1) многообразие $\mathbf{U}$ является гомоморфным образом многообразия $\mathbf{V}$;

2) многообразия $\mathbf{V}$ и $\mathbf{U}$ изоморфны, если отображение φ_1 – биекция.

Замечание 3. Иными словами: 1) многообразие $\mathbf{U} \in \mathcal{V}_1(\mathcal{K})$ – гомоморфный образ многообразия $\mathbf{U} \in \mathcal{V}_1(\mathcal{K})$ тогда и только тогда, когда алгебра $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ – гомоморфный образ алгебры $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$; 2) многообразия $\mathbf{V}, \mathbf{U} \in \mathcal{V}_1(\mathcal{K})$ изоморфны тогда и только тогда, когда алгебры $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ и $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ изоморфны.

Теорема 1. *Пусть $\boldsymbol{U}, \boldsymbol{V} \in \mathcal{V}_1(\mathcal{K})$. Если $\boldsymbol{U}$ – гомоморфный образ $\boldsymbol{V}$, то существуют такие отображения $\Psi_j : \mathcal{A}^{(j)}(\boldsymbol{V}) \to \mathcal{A}^{(j)}(\boldsymbol{U})$ $(j = 1, 2)$, что автомат $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\boldsymbol{V}))$ – гомоморфный образ автомата M_j.*

Доказательство. Предположим, что многообразие $\mathbf{U} \in \mathcal{V}_1(\mathcal{K})$ является гомоморфным образом многообразия $\mathbf{V} \in \mathcal{V}_1(\mathcal{K})$, а тройка отображений $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ $(\varphi_1 : \mathbf{V} \to \mathbf{U}, \varphi_2 : \mathcal{F}_1^{(1)} \to \mathcal{F}_1^{(2)}, \varphi_3 : \mathcal{F}_2^{(1)} \to \mathcal{F}_2^{(2)})$ определяет гомоморфизм алгебры $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ на алгебру $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$.

Рассмотрим такие отображения $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$, что:

1) для автомата $M_1 \in \mathcal{A}^{(1)}(\mathbf{V})$, заданного системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(1)} = \beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)})) \\ \mathbf{y}_{t+1}^{(1)} = \beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_2^{(1)})) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{11}$$

автомат $\Psi_1(M_1) \in \mathcal{A}^{(1)}(\mathbf{U})$ определен системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(2)} = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_1^{(2)})) \\ \mathbf{y}_{t+1}^{(2)} = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_2^{(2)})) \end{cases} \quad (t \in \mathbf{Z}_+); \tag{12}$$

2) для автомата $M_2 \in \mathcal{A}^{(2)}(\mathbf{V})$, заданного системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(1)} = \beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)})) \\ \mathbf{y}_{t+1}^{(1)} = \beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_{t+1}^{(1)}), \mathbf{v}_2^{(1)}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{13}$$

автомат $\Psi_2(M_2) \in \mathcal{A}^{(2)}(\mathbf{U})$ определен системой уравнений

$$\begin{cases} \mathbf{q}_{t+1}^{(2)} = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\mathbf{q}_t^{(2)}), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\mathbf{v}_1^{(2)})) \\ \mathbf{y}_{t+1}^{(2)} = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\mathbf{q}_{t+1}^{(2)}), \mathbf{v}_2^{(2)})) \end{cases} \quad (t \in \mathbf{Z}_+). \tag{14}$$

Из (9)-(14) вытекает, что для всех $t \in \mathbf{Z}_+$ истинны равенства

$$\varphi_1(\beta_{j_1}^{(1)}(\alpha_{i_1}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_1^{(1)}))) = \varphi_3(\beta_{j_1}^{(1)})(\varphi_2(\alpha_{i_1}^{(1)})(\varphi_1(\mathbf{q}_t^{(1)})), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\varphi_1(\mathbf{v}_1^{(1)}))),$$

$$\varphi_1(\beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_t^{(1)}), \alpha_{x_{t+1}}^{(1)}(\mathbf{v}_2^{(1)}))) = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\varphi_1(\mathbf{q}_t^{(1)})), \varphi_2(\alpha_{x_{t+1}}^{(1)})(\varphi_1(\mathbf{v}_2^{(1)}))),$$

$$\varphi_1(\beta_{j_2}^{(1)}(\alpha_{i_2}^{(1)}(\mathbf{q}_{t+1}^{(1)}), \mathbf{v}_2^{(1)})) = \varphi_3(\beta_{j_2}^{(1)})(\varphi_2(\alpha_{i_2}^{(1)})(\varphi_1(\mathbf{q}_{t+1}^{(1)})), \varphi_1(\mathbf{v}_2^{(1)})),$$

откуда, в свою очередь, вытекает, что автомат $\Psi_j(M_j)$ ($M_j \in \mathcal{A}^{(j)}(\mathbf{V})$) – гомоморфный образ автомата M_j. □

Замечание 4. Таким образом, в теореме 1 установлено, что если многообразие $\mathbf{U} \in \mathcal{V}_1(\mathcal{K})$ – гомоморфный образ многообразия $\mathbf{V} \in \mathcal{V}_1(\mathcal{K})$, то существуют такие отображения $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ ($j = 1, 2$), что автомат $\Psi_j(M_j)$ ($M_j \in \mathcal{A}^{(j)}(\mathbf{V})$) является гомоморфным образом автомата M_j. При этом тройка сюръекций (χ_1, χ_2, χ_3), определяющая гомоморфизм автомата $M_j \in \mathcal{A}^{(j)}(\mathbf{V}))$ на автомат $\Psi_j(M_j)$ удовлетворяет следующим двум условиям: 1) $\chi_1 = \chi_3 = \varphi_1$; 2) χ_2 – тождественное отображение.

Из теоремы 1 вытекает, что истинно следующее следствие.

Следствие 1. *Пусть* $\boldsymbol{U}, \boldsymbol{V} \in \mathcal{V}_1(\mathcal{K})$. *Если многообразия* $\boldsymbol{V}$ *и* $\boldsymbol{U}$ *изоморфны, то существуют такие отображения* $\Psi_j : \mathcal{A}^{(j)}(\boldsymbol{V}) \to \mathcal{A}^{(j)}(\boldsymbol{U})$ ($j = 1, 2$), *что автоматы* $M_j \in \mathcal{A}^{(j)}(\boldsymbol{V})$ *и* $\Psi_j(M_j)$ *изоморфны.*

Пример 2. Пусть γ – эллиптическая кривая, заданная над областью целостности $\mathcal{K}$. Из (7) и (8) вытекает, что (см. пример 1.1) алгебра $(\widetilde{\mathcal{K}}(\gamma), \mathcal{F}_1 \cup \mathcal{F}_2)$ ($\mathcal{F}_1 = \{\alpha_0, \alpha_1, \ldots, \alpha_{k_1}\}$ ($1 \leq k_1 < |\widetilde{\mathcal{K}}(\gamma)|$), $\mathcal{F}_2 = \{+_\gamma\}$) определяет на многообразии $\widetilde{\mathcal{K}}(\gamma) \in \mathcal{V}_1(\widetilde{\mathcal{K}})$ множества автоматов Мили $\mathcal{A}^{(1)}(\widetilde{\mathcal{K}}(\gamma))$ и Мура $\mathcal{A}^{(2)}(\widetilde{\mathcal{K}}(\gamma))$, заданных, соответственно, системами уравнений:

$$\begin{cases} q_{t+1} = \alpha_{i_1}(q_t) +_\gamma \alpha_{x_{t+1}}(P_1) \\ y_{t+1} = \alpha_{i_2}(q_t) +_\gamma \alpha_{x_{t+1}}(P_2) \end{cases} \quad (t \in \mathbf{Z}_+) \tag{15}$$

и

$$\begin{cases} q_{t+1} = \alpha_{i_1}(q_t) +_\gamma \alpha_{x_{t+1}}(P_1) \\ y_{t+1} = \alpha_{i_2}(q_{t+1}) +_\gamma P_2 \end{cases} \quad (t \in \mathbf{Z}_+), \tag{16}$$

где $i_1, i_2 \in \mathbf{Z}_{k_1+1}$ – фиксированные числа, $P_1, P_2 \in \widetilde{\mathcal{K}}(\gamma)$ – фиксированные точки, $q_0 \in \widetilde{\mathcal{K}}(\gamma)$ и $x_{t+1} \in \mathbf{Z}_{k_1+1}$ ($t \in \mathbf{Z}_+$).

Если γ_1 и γ_2 – эллиптические кривые, заданные над областью целостности $\mathcal{K}$, то говорят, что:

1) эллиптическая кривая γ_2 – гомоморфный образ эллиптической кривой γ_1, если абелева группа $(\widetilde{\mathcal{K}}(\gamma_2), +_{\gamma_2})$ – гомоморфный образ абелевой группы $(\widetilde{\mathcal{K}}(\gamma_1), +_{\gamma_1})$;

2) эллиптические кривые γ_1 и γ_2 изоморфны, если абелевы группы $(\widetilde{\mathcal{K}}(\gamma_1), +_{\gamma_1})$ и $(\widetilde{\mathcal{K}}(\gamma_2), +_{\gamma_2})$ изоморфны.

Пусть $\varphi_1 : \widetilde{\mathcal{K}}(\gamma_1) \to \widetilde{\mathcal{K}}(\gamma_2)$ – гомоморфизм эллиптической кривой γ_1 на эллиптическую кривую γ_2. Тогда для любого числа $k_1 \in \{1, \ldots, |\widetilde{\mathcal{K}}(\gamma_2)| - 1\}$ алгебра

$(\widetilde{\mathcal{K}}(\gamma_2), \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ $(\mathcal{F}_1^{(2)} = \{\alpha_0^{(2)}, \alpha_1^{(2)}, \ldots, \alpha_{k_1}^{(2)}\},\ \mathcal{F}_2^{(2)} = \{+_{\gamma_2}\})$ – гомоморфный образ алгебры $(\widetilde{\mathcal{K}}(\gamma_1), \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ $(\mathcal{F}_1^{(1)} = \{\alpha_0^{(1)}, \alpha_1^{(1)}, \ldots, \alpha_{k_1}^{(1)}\},\ \mathcal{F}_2^{(1)} = \{+_{\gamma_1}\})$. При этом для гомоморфизма $\Phi = (\varphi_1, \varphi_2, \varphi_3)$ алгебры $(\widetilde{\mathcal{K}}(\gamma_1), \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ на алгебру $(\widetilde{\mathcal{K}}(\gamma_2), \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ биекции $\varphi_2 : \mathcal{F}_1^{(1)} \to \mathcal{F}_1^{(2)}$ и $\varphi_3 : \mathcal{F}_2^{(1)} \to \mathcal{F}_2^{(2)})$ определяются равенствами $\varphi_2(\alpha_i^{(1)}) = \alpha_i^{(2)}$ $(i \in \mathbf{Z}_{k_1+1})$ и $\varphi_3(+_{\gamma_1}) = +_{\gamma_2}$. В частности, если φ_1 – биекция, то алгебры $(\widetilde{\mathcal{K}}(\gamma_1), \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ и $(\widetilde{\mathcal{K}}(\gamma_2), \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$ изоморфны.

Таким образом, если эллиптическая кривая γ_2 – гомоморфный образ эллиптической кривой γ_1, то многообразие $\widetilde{\mathcal{K}}(\gamma_2) \in \mathcal{V}_1(\widetilde{\mathcal{K}})$ – гомоморфный образ многообразия $\widetilde{\mathcal{K}}(\gamma_1) \in \mathcal{V}_1(\widetilde{\mathcal{K}})$ (соответственно, если эллиптические кривые γ_1 и γ_2 изоморфны, то многообразия $\widetilde{\mathcal{K}}(\gamma_1) \in \mathcal{V}_1(\widetilde{\mathcal{K}})$ и $\widetilde{\mathcal{K}}(\gamma_2) \in \mathcal{V}_1(\widetilde{\mathcal{K}})$ изоморфны).

Следовательно, из теоремы 1 вытекает, что если эллиптическая кривая γ_2 – гомоморфный образ эллиптической кривой γ_1, то существуют такие отображения $\Psi_j : \mathcal{A}^{(j)}(\widetilde{\mathcal{K}}(\gamma_1)) \to \mathcal{A}^{(j)}(\widetilde{\mathcal{K}}(\gamma_2))$ $(j = 1, 2)$, что автомат $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\widetilde{\mathcal{K}}(\gamma_1)))$ – гомоморфный образ автомата M_j. При этом, из доказательства теоремы 1 вытекает, что:

1) для автомата $M_1 \in \mathcal{A}^{(1)}(\widetilde{\mathcal{K}}(\gamma_1))$, заданного системой уравнений

$$\begin{cases} q_{t+1}^{(1)} = \alpha_{i_1}^{(1)}(q_t^{(1)}) +_{\gamma_1} \alpha_{x_{t+1}}^{(1)}(P_1^{(1)}) \\ y_{t+1}^{(1)} = \alpha_{i_2}^{(1)}(q_t^{(1)}) +_{\gamma_1} \alpha_{x_{t+1}}^{(1)}(P_2^{(1)}) \end{cases} \qquad (t \in \mathbf{Z}_+),$$

автомат $\Psi_1(M_1) \in \mathcal{A}^{(1)}(\widetilde{\mathcal{K}}(\gamma_2))$ определен системой уравнений

$$\begin{cases} q_{t+1}^{(2)} = \alpha_{i_1}^{(2)}(q_t^{(2)}) +_{\gamma_2} \alpha_{x_{t+1}}^{(2)}(P_1^{(2)}) \\ y_{t+1}^{(2)} = \alpha_{i_2}^{(2)}(q_t^{(2)}) +_{\gamma_2} \alpha_{x_{t+1}}^{(2)}(P_2^{(2)}) \end{cases} \qquad (t \in \mathbf{Z}_+);$$

2) для автомата $M_2 \in \mathcal{A}^{(2)}(\widetilde{\mathcal{K}}(\gamma_1))$, заданного системой уравнений

$$\begin{cases} q_{t+1}^{(1)} = \alpha_{i_1}^{(1)}(q_t^{(1)}) +_{\gamma_1} \alpha_{x_{t+1}}^{(1)}(P_1^{(1)}) \\ y_{t+1}^{(1)} = \alpha_{i_2}^{(1)}(q_{t+1}^{(1)}) +_{\gamma_1} P_2^{(1)} \end{cases} \qquad (t \in \mathbf{Z}_+),$$

автомат $\Psi_1(M_2) \in \mathcal{A}^{(2)}(\widetilde{\mathcal{K}}(\gamma_2))$ определен системой уравнений

$$\begin{cases} q_{t+1}^{(2)} = \alpha_{i_1}^{(2)}(q_t^{(2)}) +_{\gamma_2} \alpha_{x_{t+1}}^{(2)}(P_1^{(2)}) \\ y_{t+1}^{(2)} = \alpha_{i_2}^{(2)}(q_{t+1}^{(2)}) +_{\gamma_2} P_2^{(2)} \end{cases} \qquad (t \in \mathbf{Z}_+).$$

4. Автоматы на многообразии $\mathbf{V} \in \mathcal{V}_2(\mathcal{K})$. Пусть $\mathbf{V} \in \mathcal{V}_2(\mathcal{K})$ – многообразие в K^n. Тогда определена полиномиальная параметризация $\mathbf{v} = \mathbf{h}(\overrightarrow{\tau})$ $(\overrightarrow{\tau} \in K^m)$ многообразия $\mathbf{V}$. Зафиксируем семейство $\Theta = \{\theta_i\}_{i \in \mathbf{Z}_k}$ легко вычислимых отображений $\theta_i : K^m \to K^m$. Системы уравнений

$$\begin{cases} P_{t+1} = \theta_{x_{t+1}}(P_t) \\ \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{r}_{x_{t+1}}(\mathbf{q}_t) \end{cases} \qquad (t \in \mathbf{Z}_+) \tag{17}$$

и

$$\begin{cases} P_{t+1} = \theta_{x_{t+1}}(P_t) \\ \mathbf{q}_{t+1} = \mathbf{h}(P_{t+1}) \\ \mathbf{y}_{t+1} = \mathbf{r}(\mathbf{q}_{t+1}) \end{cases} \qquad (t \in \mathbf{Z}_+), \tag{18}$$

где $P_0 \in K^m$ – фиксированная точка, $\mathbf{q}_0 = \mathbf{h}(P_0)$, $\mathbf{r}_i : K^n \to K^l$ $(i \in \mathbf{Z}_k)$ и $\mathbf{r} : K^n \to K^l$ – фиксированные отображения, а $x_{t+1} \in \mathbf{Z}_k$ $(t \in \mathbf{Z}_+)$, определяют множество автоматов, соответственно, $\mathcal{A}^{(1)}(\mathbf{V}, \Theta)$ Мили и $\mathcal{A}^{(2)}(\mathbf{V}, \Theta)$ Мура.

Замечание 5. Таким образом, x_t, $\mathbf{q}_t$ и $\mathbf{y}_t$ – соответственно, входной символ, состояние и выходной символ автомата $M \in \mathcal{A}^{(1)}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}(\mathbf{V}, \Theta)$ в момент t. Отметим также, что из (17) и (18) вытекает, что на отображения, определяющие функции выходов автомата $M \in \mathcal{A}^{(1)}(\mathbf{V}, \Theta) \cup \mathcal{A}^{(2)}(\mathbf{V}, \Theta)$ в момент t, наложено единственное ограничение: они являются отображениями модуля над кольцом $\mathcal{K}$ в модуль над этим кольцом.

Пусть для многообразия $\mathbf{V} \in \mathcal{V}_2(\mathcal{K})$ определена полиномиальная параметризация $\mathbf{v} = \mathbf{h}_1(\overrightarrow{\tau}_1)$ $(\overrightarrow{\tau}_1 \in K^{m_1})$ и зафиксировано семейство $\Theta_1 = \{\theta_i^{(1)}\}_{i \in \mathbf{Z}_k}$ легко вычислимых отображений $\theta_i^{(1)} : K^{m_1} \to K^{m_1}$, а для многообразия $\mathbf{U} \in \mathcal{V}_2(\mathcal{K})$ – полиномиальная параметризация $\mathbf{v} = \mathbf{h}_2(\overrightarrow{\tau}_2)$ $(\overrightarrow{\tau}_2 \in K^{m_2})$ и зафиксировано семейство $\Theta_2 = \{\theta_i^{(2)}\}_{i \in \mathbf{Z}_k}$ легко вычислимых отображений $\theta_i^{(2)} : K^{m_2} \to K^{m_2}$. Предположим, что существует пара сюръекций $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 : \mathbf{V} \to \mathbf{U}, \varphi_2 : K^{m_1} \to K^{m_2})$, для которой равенства

$$\varphi_2(\theta_i^{(1)}(\overrightarrow{\tau}_1)) = \theta_i^{(2)}(\varphi_2(\overrightarrow{\tau}_1)), \tag{19}$$

$$\varphi_1(\mathbf{h}_1(\overrightarrow{\tau}_1)) = \mathbf{h}_2(\varphi_2(\overrightarrow{\tau}_1)) \tag{20}$$

истинны для всех $\overrightarrow{\tau}_1 \in K^{m_1}$ и всех $i \in \mathbf{Z}_k$. Тогда будем говорить, что:

1) пара $(\mathbf{U}, \Theta_2)$ является гомоморфным образом пары $(\mathbf{V}, \Theta_1)$;

2) пары $(\mathbf{V}, \Theta_1)$ и $(\mathbf{U}, \Theta_2)$ изоморфны, если φ_1 и φ_2 – биекции.

Замечание 6. Ясно, что для изоморфных пар $(\mathbf{V}, \Theta_1)$ и $(\mathbf{U}, \Theta_2)$ истинны равенства $|\mathbf{V}| = |\mathbf{U}|$ и $m_1 = m_2$.

Теорема 2. *Пусть $\boldsymbol{U}, \boldsymbol{V} \in \mathcal{V}_2(\mathcal{K})$ и существует гомоморфизм $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 : \boldsymbol{V} \to \boldsymbol{U}, \varphi_2 : K^{m_1} \to K^{m_2})$ пары $(\boldsymbol{V}, \Theta_1)$ на пару $(\boldsymbol{U}, \Theta_2)$. Тогда существуют такие отображения $\Psi_j : \mathcal{A}^{(j)}(\boldsymbol{V}, \Theta_1) \to \mathcal{A}^{(j)}(\boldsymbol{U}, \Theta_2)$ $(j = 1, 2)$, что автомат $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\boldsymbol{V}, \Theta_1))$ – гомоморфный образ автомата M_j.*

Доказательство. Пусть $\mathbf{U}, \mathbf{V} \in \mathcal{V}_2(\mathcal{K})$, а $\mathbf{v} = \mathbf{h}_1(\overrightarrow{\tau}_1)$ $(\overrightarrow{\tau}_1 \in K^{m_1})$ и $\mathbf{u} = \mathbf{h}_2(\overrightarrow{\tau}_2)$ $(\overrightarrow{\tau}_2 \in K^{m_2})$ – полиномиальная параметризация, соответственно, многообразия $\mathbf{V} \in K^{n_1}$ и многообразия $\mathbf{U} \in K^{n_2}$. Предположим, что пара $(\mathbf{U}, \Theta_2)$ – гомоморфный образ пары $(\mathbf{V}, \Theta_1)$, где $\Theta_j = \{\theta_i^{(j)}\}_{i \in \mathbf{Z}_k}$ $(j = 1, 2)$ – семейство легко вычислимых отображений $\theta_i^{(j)} : K^{m_j} \to K^{m_j}$ $(i \in \mathbf{Z}_k)$, а гомоморфизм $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 : \mathbf{V} \to \mathbf{U}, \varphi_2 : K^{m_1} \to K^{m_2})$ состоит из легко вычислимых сюръекций.

Рассмотрим такие отображения $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}, \Theta_1) \to \mathcal{A}^{(j)}(\mathbf{U}, \Theta_2)$ $(j = 1, 2)$, что:

1) для автомата $M_1 \in \mathcal{A}^{(1)}(\mathbf{V}, \Theta_1)$, заданного системой уравнений

$$\begin{cases} P_{t+1}^{(1)} = \theta_{x_{t+1}}^{(1)}(P_t^{(1)}) \\ \mathbf{q}_{t+1}^{(1)} = \mathbf{h}_1(P_{t+1}^{(1)}) \\ \mathbf{y}_{t+1}^{(1)} = \mathbf{r}_{x_{t+1}}^{(1)}(\mathbf{q}_t^{(1)}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{21}$$

где $\mathbf{r}_i^{(1)} : K^{n_1} \to K^{l_1}$ $(i \in \mathbf{Z}_k)$, автомат $\Psi_1(M_1) \in \mathcal{A}^{(1)}(\mathbf{U}, \Theta_2)$ определен системой уравнений

$$\begin{cases} P_{t+1}^{(2)} = \theta_{x_{t+1}}^{(2)}(P_t^{(2)}) \\ \mathbf{q}_{t+1}^{(2)} = \mathbf{h}_2(P_{t+1}^{(2)}) \\ \mathbf{y}_{t+1}^{(2)} = \mathbf{r}_{x_{t+1}}^{(2)}(\mathbf{q}_t^{(2)}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{22}$$

где число l_2 и отображения $\mathbf{r}_i^{(2)} : K^{n_2} \to K^{l_2}$ $(i \in \mathbf{Z}_k)$ будут определены ниже;

2) для автомата $M_2 \in \mathcal{A}^{(2)}(\mathbf{V}, \Theta_2)$, заданного системой уравнений

$$\begin{cases} P_{t+1}^{(1)} = \theta_{x_{t+1}}^{(1)}(P_t^{(1)}) \\ \mathbf{q}_{t+1}^{(1)} = \mathbf{h}_1(P_{t+1}^{(1)}) \\ \mathbf{y}_{t+1}^{(1)} = \mathbf{r}^{(1)}(\mathbf{q}_{t+1}^{(1)}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{23}$$

где $\mathbf{r}^{(1)} : K^{n_1} \to K^{l_1}$, автомат $\Psi_2(M_2) \in \mathcal{A}^{(2)}(\mathbf{U}, \Theta_2)$ определен системой уравнений

$$\begin{cases} P_{t+1}^{(2)} = \theta_{x_{t+1}}^{(2)}(P_t^{(2)}) \\ \mathbf{q}_{t+1}^{(2)} = \mathbf{h}_2(P_{t+1}^{(2)}) \\ \mathbf{y}_{t+1}^{(2)} = \mathbf{r}^{(2)}(\mathbf{q}_{t+1}^{(2)}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{24}$$

где число l_2 и отображение $\mathbf{r}^{(2)} : K^{n_2} \to K^{l_2}$ будет определено ниже.

Из (19)-(24) вытекает, что истинны равенства $\varphi_2(\theta_{x_{t+1}}^{(1)}(P_t^{(1)})) = \theta_{x_{t+1}}^{(2)}(\varphi_2(P_t^{(1)}))$ и $\varphi_1(\mathbf{h}_1(P_{t+1}^{(1)})) = \mathbf{h}_2(\varphi_2(P_{t+1}^{(1)}))$. Из этих равенств вытекает, что функция переходов автомата (22) (соответственно, автомата (24)) удовлетворяет требованиям, накладываемым на функцию переходов гомоморфного образа автомата (21) (соответственно, автомата (23)) в случае, когда $\chi_1 = \varphi_1$, а χ_2 – тождественное отображение.

Определим теперь функции выходов автоматов (22) и (24).

Рассмотрим автомат (24). Пусть $\mathcal{S}_{M_2} = \{S_{\mathbf{u}} | \mathbf{u} \in \mathbf{U}\}$, где $S_{\mathbf{u}} = \mathbf{r}^{(1)}(\varphi_1^{-1}(\mathbf{u}))$, а $\equiv_{M_2}$ – отношение эквивалентности на множестве $\mathcal{S}_{M_2}$, определенное следующим образом: $S_{\mathbf{u}'} \equiv_{M_2} S_{\mathbf{u}''}$ $(\mathbf{u}', \mathbf{u}'' \in \mathbf{U})$ тогда и только тогда, когда существует такая последовательность $\mathbf{u}_1 = \mathbf{u}', \mathbf{u}_2, \ldots, \mathbf{u}_n = \mathbf{u}''$ элементов многообразия $\mathbf{U}$, что $S_{\mathbf{u}_i} \cap S_{\mathbf{u}_{i+1}} \neq \emptyset$ для всех $i = 1, \ldots, n-1$. Обозначим через ξ_{M_2} такую сюръекцию множества $Val\ \mathbf{r}^{(1)}$ в фактор-множество $\mathcal{S}_{M_2}/_{\equiv_{M_2}}$, что $\xi_{M_2}(\mathbf{y}) = \mathtt{S}$ тогда и только тогда, когда существует такое $S_{\mathbf{u}} \in \mathtt{S}$, что $\mathbf{y} \in S_{\mathbf{u}}$. Положим $l_2 = \lceil (\log |\mathcal{S}_{M_2}|) \cdot (\log |K|)^{-1} \rceil$ и зафиксируем инъекцию η_{M_2} фактор-множества $\mathcal{S}_{M_2}/_{\equiv_{M_2}}$ в множество K^{l_2}. Определим отображение $\mathbf{r}^{(2)}$ равенством

$$\mathbf{r}^{(2)}(\mathbf{u}) = (\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}^{(1)}(\varphi_1^{-1}(\mathbf{u}))) \ (\mathbf{u} \in \mathbf{U}). \tag{25}$$

Из (25) вытекает, что истинно равенство $(\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}^{(1)}(\mathbf{q}^{(1)}_{t+1})) = \mathbf{r}^{(2)}(\varphi_1(\mathbf{q}^{(1)}_{t+1}))$, т.е. функции выходов автомата (24), определенная равенством (25), удовлетворяет требованиям, накладываемым на функцию выходов гомоморфного образа автомата (23), если $\chi_1 = \varphi_1$, χ_2 – тождественное отображение, а $\chi_3 = \eta_{M_2} \circ \xi_{M_2}$.

Рассмотрим автомат (22). Пусть $\mathcal{S}_{M_1} = \bigcup\limits_{i \in \mathbf{Z}_k} \mathcal{S}_{M_1,i}$, где $\mathcal{S}_{M_1,i} = \{S_{\mathbf{u},i} | \mathbf{u} \in \mathbf{U}\}$ $(i \in \mathbf{Z}_k)$, а $S_{\mathbf{u},i} = \mathbf{r}^{(1)}_i(\varphi_1^{-1}(\mathbf{u}))$, а $\equiv_{M_1}$ – такое отношение эквивалентности на множестве $\mathcal{S}_{M_1}$, что $S_{\mathbf{u}',i_1} \equiv_{M_1} S_{\mathbf{u}'',i_2}$ $(\mathbf{u}', \mathbf{u}'' \in \mathbf{U}; i_1, i_2 \in \mathbf{Z}_k)$ тогда и только тогда, когда существуют такая последовательность элементов $\mathbf{u}_1 = \mathbf{u}', \mathbf{u}_2, \ldots, \mathbf{u}_n = \mathbf{u}''$ многообразия $\mathbf{U}$ и такая последовательность $r_1 = i_1, r_2, \ldots, r_n = i_2$ элементов множества $\mathbf{Z}_k$, что $S_{\mathbf{u}_j,r_j} \cap S_{\mathbf{u}_{i+1},r_{j+1}} \neq \emptyset$ для всех $j = 1, \ldots, n-1$. Обозначим через ξ_{M_1} такую сюръекцию множества $\bigcup\limits_{i \in \mathbf{Z}_k} Val\ \mathbf{r}^{(1)}_i$ в фактор-множество $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$, что $\xi_{M_1}(\mathbf{y}) = \mathtt{S}$ тогда и только тогда, когда существует такое $S_{\mathbf{u},i} \in \mathtt{S}$, что $\mathbf{y} \in S_{\mathbf{u},i}$. Положим $l_2 = \lceil (\log |\mathcal{S}_{M_1}|) \cdot (\log |K|)^{-1} \rceil$ и зафиксируем инъекцию η_{M_1} фактор-множества $\mathcal{S}_{M_1}/_{\equiv_{M_1}}$ в множество K^{l_2}. Определим отображения $\mathbf{r}^{(2)}_i$ $(i \in \mathbf{Z}_k)$ равенствами

$$\mathbf{r}^{(2)}_i(\mathbf{u}) = (\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}^{(1)}_i(\varphi_1^{-1}(\mathbf{u}))) \ (\mathbf{u} \in \mathbf{U}) \ (i \in \mathbf{Z}_k). \tag{26}$$

Из (26) вытекает, что истинны равенства $(\eta_{M_2} \circ \xi_{M_2})(\mathbf{r}^{(1)}_i(\mathbf{q}^{(1)}_{t+1})) = \mathbf{r}^{(2)}_i(\varphi_1(\mathbf{q}^{(1)}_{t+1}))$ $(i \in \mathbf{Z}_k)$, т.е. функция выходов автомата (22), определенная равенствами (26), удовлетворяет требованиям, которые накладываются на функцию выходов гомоморфного образа автомата (21), если $\chi_1 = \varphi_1$, χ_2 – тождественное отображение, а $\chi_3 = \eta_{M_2} \circ \xi_{M_2}$. □

Пример 3. Алгебраические кривые

$$v_2 = a_0 v_1^{n_1} + a_1 v_1^{n_1-1} + \cdots + a_{n_1},$$

$$u_2 = b_0 u_1^{n_2} + b_1 u_1^{n_2-1} + \cdots + b_{n_2}$$

над кольцом $\mathcal{K}$ определяют в K^2 многообразия (см. пример 1.2), соответственно,

$$\mathbf{V} = \{(\tau_1, a_0\tau_1^{n_1} + a_1\tau_1^{n_1-1} + \cdots + a_{n_1}) | \tau_1 \in K\},$$

$$\mathbf{U} = \{(\tau_2, b_0\tau_2^{n_2} + a_1\tau_2^{n_2-1} + \cdots + b_{n_2}) | \tau_2 \in K\}.$$

Зафиксируем элементы $c, b_0, \ldots, b_k \in K^{non-d}$. Определим семейство $\Theta = \{\theta_i\}_{i \in \mathbf{Z}_k}$ легко вычислимых отображений $\theta_i : K \to K$ равенствами

$$\theta_i(\tau) = b_i\tau \quad (i \in \mathbf{Z}_k, \tau \in K),$$

а пару биекций $\Phi = (\varphi_1, \varphi_2)$ $(\varphi_1 : \mathbf{V} \to \mathbf{U}, \varphi_2 : K \to K)$ – равенствами

$$\varphi_1((\tau, a_0\tau^{n_1} + a_1\tau^{n_1-1} + \cdots + a_{n_1})) =$$

$$= (c\tau, b_0c^{n_2}\tau^{n_2} + a_1c^{n_2-1}\tau^{n_2-1} + \cdots + b_{n_2}) \quad (\tau \in K),$$

$$\varphi_2(\tau) = c\tau \quad (\tau \in K).$$

Пары $(\mathbf{V}, \Theta)$ и $(\mathbf{U}, \Theta)$ изоморфны, так как для биекций $\Phi = (\varphi_1, \varphi_2)$ истинны равенства (19) и (20). Поэтому из теоремы 2 вытекает, что существуют такие отображения $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}, \Theta) \to \mathcal{A}^{(j)}(\mathbf{U}, \Theta)$ $(j = 1, 2)$, что автомат $\Psi_j(M_j)$ $(M_j \in \mathcal{A}^{(j)}(\mathbf{V}))$ – гомоморфный образ автомата M_j.

5. Заключение. В настоящей работе в терминах гомоморфизмов многообразий над конечным кольцом охарактеризованы гомоморфизмы автоматов, определенных на этих многообразиях. Рассмотрены два основные как с позиции теории, так и с позиции приложений случая. В первом случае гомоморфизмы многообразий определены посредством гомоморфизмов алгебр, заданных на многообразиях, а функции переходов и выходов автоматов определены через унарные и бинарные операции этих алгебр. Во втором случае гомоморфизмы многообразий определены посредством гомоморфизмов множеств траекторий на многообразиях, определяемых полиномиальными параметризациями многообразий, функции переходов автоматов обеспечивают движение автомата по указанным траекториям, а функциями выходов автоматов – произвольные отображения многообразия в модуль над кольцом. Анализ свойств отображений $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$ в терминах абстрактных свойств алгебр $(\mathbf{V}, \mathcal{F}_1^{(1)} \cup \mathcal{F}_2^{(1)})$ и $(\mathbf{U}, \mathcal{F}_1^{(2)} \cup \mathcal{F}_2^{(2)})$, а также свойств отображений $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}, \Theta_1) \to \mathcal{A}^{(j)}(\mathbf{U}, \Theta_2)$ $(j = 1, 2)$ в терминах свойств семейств легко вычислимых отображений Θ_1 и Θ_2 представляет одно из дальнейших направлений исследований.

Алгебраическая система на множестве многообразий над кольцом $\mathcal{K}$, определяемая формулами (2)-(4), естественно определяет алгебраическую систему на множествах автоматов на многообразиях. Анализ свойств композиций отображений $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}) \to \mathcal{A}^{(j)}(\mathbf{U})$ $(j = 1, 2)$ и $\Psi_j : \mathcal{A}^{(j)}(\mathbf{V}, \Theta_1) \to \mathcal{A}^{(j)}(\mathbf{U}, \Theta_2)$ $(j = 1, 2)$, соответствующих композициям автоматов, представляет другое направление исследований.

1. *Шафаревич И.Р.* Основы алгебраической геометрии. Т.1. – М.: Наука, 1988. – 352 с.
2. *Шафаревич И.Р.* Основы алгебраической геометрии. Т. 2. – М.: Наука, 1988. – 304 с.
3. *Зарисский О., Самуэль П.* Коммутативная алгебра. Т. 1. – М.: ИЛ, 1963. – 373 с.
4. *Зарисский О., Самуэль П.* Коммутативная алгебра. Т. 2. – М.: ИЛ, 1963. – 438 с.
5. *Кокс Д., Литтл Дж., О'Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. – М.: Мир, 2000. – 687 с.
6. *Болотов А.А., Гашков С.Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. – 280 с.
7. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии. – М.: МЦМНО, 2003. – 328 с.
8. *Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
9. *Харин Ю.С., Берник В.И., Матвеев Г.В. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
10. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАНУ, 2009. – 479 с.
11. *Скобелев В.В., Глазунов Н.М., Скобелев В.Г.* Многообразия над кольцами. Теория и приложения. – Донецк: ИПММ НАНУ, 2009. – 323 с.
12. *Курош А.Г.* Лекции по общей алгебре. – М. Наука, 1973. – 400 с.

V. V. Skobelev

On automata over varieties into a ring.

Automata over varieties into finite ring are determined. Homomorphisms of these automata are characterized via homomorphisms of varieties for two basic cases. In the first case homomorphisms of varieties are determined via homomorphisms of algebras determined onto varieties and automata are determined via unary and binary operations of these algebras. In the second case homomorphisms of varieties are determined via homomorphisms of sets of trajectories determined via polynomial parametrization of varieties, transition mappings of automata provide moving of automata on these trajectories, and output mappings of automata transforms varieties into some module over the ring.

Keywords: *rings, varieties, automata.*

В. В. Скобелєв

Про автомати на многовидах над кільцем.

Визначено автомати на многовидах над скінченним кільцем. Охарактеризовано гомоморфізми цих автоматів у термінах гомоморфізмів многовидів у наступних двох базових випадках. У першому випадку гомоморфізми многовидів визначено за допомогою гомоморфізмів заданих на них алгебр, а автомати визначено за допомогою унарних і бінарних операцій цих алгебр. У другому випадку гомоморфізми многовидів визначено за допомогою гомоморфізмів множин траєкторій, які визначаються за допомогою поліноміальних параметризацій многовидів, функції переходів автоматів забезпечують їх рух вздовж вказаних траєкторій, а функції виходів автоматів – довільні відображення многовида у модуль над кільцем.

Ключові слова: *кільця, многовиди, автомати.*

Ин-т прикл. математики и механики НАН Украины, Донецк
vv_skobelev@iamm.ac.donetsk.ua

Получено 17.05.12