УДК 512.7+519.7+681.3

Skobelev V.

ON SYSTEMS OF POLYNOMIAL EQUATIONS OVER FINITE RINGS

Finding and storing the set of solutions for systems of polynomial equations with parameters over finite associative (not necessarily, commutative) rings is one of basic problems in various applications connected with exploring algebraic models over these rings.

In this paper, it developed unified approach for presenting in implicit form the set of solutions for systems of polynomial equations with parameters over any finite associative (not necessarily, commutative) ring with unit. Proposed approach is based on notions of classes of l-associated or r-associated elements of the ring developed in the paper.

Keywords: associative rings, systems of equations, classes of associated elements.

1. Introduction

Currently, there is a steady tendency to encryption of the transition from purely combinatorial models to combinatorial-algebraic models in the development of codes [2; 3]. Moreover, almost all candidates for modern stream ciphers standard are based on some computing into rings of residues. Thus, it is actual systematic investigation of automata-algebraic models over finite rings for development of automata theory itself, as well as for elaboration of mathematical backgrounds for modern cryptology.

Mealy and Moore automata over any finite associative-commutative ring with unit were investigated in [9; 10] (linear autonomous automata over these rings were investigated in [5; 6]). Established results imply that computational security analysis for an automation mapping can be reduced to finding the set of solutions for appropriate system of equations over corresponding ring.

It is well known that finding the set of solutions for systems of multi-variable non-linear polynomial equations over the field $GF(2^k)$ ($k \in \mathbf{N}$) is NP-complete problem (see [1], for example). Moreover, any method for resolving system of polynomial equations over any finite field can't be directly applied in the case of a ring with divisors of zero (see [11], for example).

The situation is much more complicated for systems of multi-variable non-linear polynomial equations with parameters over any finite associative (not necessarily, commutative) ring with unit [4], because in addition to difficulties with finding the set of solutions itself, there are problems to present this set into explicit form, since its cardinality can be sufficiently high (this situation is typical for any ring of square matrices of fixed size $n \geq 2$ over any finite associative ring with unit).

Thus, there is actual problem to develop some unified approach for finding the set S of solutions for system

$$\begin{cases} f_1(u_1,\ldots,u_n,a_1,\ldots,a_h)=0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_1(u_1,\ldots,u_n,a_1,\ldots,a_h)=0, \end{cases} \qquad (1)$$

of multi-variable polynomial equations with parameters (u_1, ..., u_n are variables and a_1, ..., a_h are parameters) over any finite associative (not necessarily, commutative) ring $\mathsf{K} = (K, +, \cdot)$ with unit, such that there hold the following three conditions:

1) some finite family $\{S_i\}_{i\in I}$ of non-empty subsets, such that $S = \bigcup_{i\in I} S_i$ is constructed;
2) every subset S_i ($i \in I$) is presented in implicit form via some set-theoretic formula exploring the structure of the ring K;
3) complexity of presentation of any subset S_i ($i \in I$) in explicit form depends mainly on the structure of the ring K.

It is evident that construction of the family $\{S_i\}_{i\in I}$ reflects real complexity for construction and storing the set of solutions for multi-variable polynomial equations with parameters over the ring K.

In the given paper we investigate this problem. The remainder of the paper is organized as follows. In Section 2 basic idea of proposed approach is presented. In Section 3 it is presented some generalization for the notion «associated elements» in the case of any associative (not necessarily, commutative) ring with unit. In Section 4 proposed some scheme for finding the set of solutions for multi-variable polynomial equations is presented and illustrated. Section 5 consists of some conclusions.

2. Basic idea of proposed approach

It is well known that for any polynomial $f(x)=\sum_{i=0}^{r} a_i x^i$ $(a_0,a_1,\ldots,a_r \in \mathbf{Z})$ and integer $m = p_1^{\beta_1}\ldots p_l^{\beta_l} \in \mathbf{N}$ (p_1, ..., p_l are prime integers) resolving of congruence relation $f(x) \equiv 0 (\mathrm{mod}\ m)$is reduced to resolving the system

$$\begin{cases} f(x) \equiv 0 \,(\mathrm{mod}\, p_1^{\beta_1}), \\ \dots\dots\dots\dots\dots \\ f(x) \equiv 0 \,(\mathrm{mod}\, p_l^{\beta_l}), \end{cases}$$

of congruence relations.

Resolving any congruence relation $f(x) \equiv 0(\mathrm{mod}\, p^{\beta})$ (p is prime integer, $\beta \in \mathbf{N}$) is reduced to construction of all sums $x = \sum_{j=0}^{\beta-1} b_j p^j$, where integers $b_0, \dots, b_{\beta-1} \in \mathbf{Z}_p$ are determined successively in the following way:

1) integer b_0 is a solution of congruence relation $f(x) \equiv 0 \pmod{p}$;
2) for all $s = 1, \dots, \beta - 1$ integer b_h is any integer, such that $x = \sum_{j=0}^{s} b_j p^j$ is a solution of congruence relation $f(x) \equiv 0 \pmod{p^{s+1}}$.

It is evident that in the ring of residues $\mathsf{Z}_{p^\beta} = (\mathbf{Z}_{p^\beta}, +, \cdot)$ any sum $x = \sum_{j=0}^{\beta-1} b_j p^j$, such that $b_j \in \mathbf{Z}_p$ $(j = 0, 1, \dots, \beta - 1)$ is an element of the unique class of associated elements. Thus, it is natural to determine the family $\{S_i\}_{i \in I}$ for the system (1) in terms of classes of associated elements.

To develop this approach for any finite associative (not necessarily, commutative) ring with unit, some analogue for the notion 'class of associated elements' can be determined for such rings. This notion gives the possibility to analyze all cases when parameters a_1, ..., a_h are elements of specific classes of associated elements and to extract the set of admissible combinations of these classes. This set can be used in the role of the set I of indices for the family $\{S_i\}_{i \in I}$. For any admissible combination for classes of associated elements for parameters admissible combinations for classes of associated elements for variables u_1, ..., u_n can be extracted. For each such combination for classes of associated elements values for variables u_1, ..., u_n in corresponding classes of associated elements can be found.

This is basic idea of proposed approach for finding the set S of solutions for systems of multi-variable polynomial equations with parameters over any finite associative ring K with unit.

Remark 1. It is worth noting that above proposed approach is non-trivial generalization of approach intended for solving of multi-variable nonlinear polynomial equations with parameters over finite associative-commutative ring with unit presented in [7; 8; 10].

3. Classes of associated elements of associative ring with unit

Since $\mathsf{K} = (K, +, \cdot)$ is associative ring with unit, then the set K^{inv} of all invertible elements (in other words, divisors of unit) is a non-empty one. In what follows it is supposed that the set $K^{nov-inv} = K \setminus K^{inv}$ is also non-empty.

Remark 2. In the given section it is not supposed that the ring K is a finite one.

We define the following two equivalence relations $\equiv_l$ and $\equiv_r$ onto the set K:

$$(\forall x, y \in K)\ (x \equiv_l y \Leftrightarrow (\exists \alpha \in K^{inv})(x = \alpha y)),$$

$$(\forall x, y \in K)\ (x \equiv_r y \Leftrightarrow (\exists \beta \in K^{inv})(x = y\beta)).$$

Elements of the factor-set $\mathsf{B}_l = K/_{\equiv_l}$ (correspondingly, of the factor-set $\mathsf{B}_r = K/_{\equiv_r}$) we call the classes of l-associated (correspondingly, of r-associated) elements of the ring K.

Remark 3. It is evident that for any associative-commutative ring K with unit there hold identities

$$\equiv_l = \equiv_r = \equiv, \quad (2)$$

where $\equiv$ is usual equivalence relation 'to be associated elements' for the above pointed ring (see, [9], for example). Moreover identities (2) hold for any associative non-commutative ring K with unit, such that $K^{inv} \subseteq K^{cntr}$, where K^{cntr} is the center of the ring K.

For any $x \in K$ we denote via $\langle x \rangle_l$ (correspondingly, via $\langle x \rangle_r$) the class of elements of the ring K that are l-associated (correspondingly, r-associated) with the element x. It is evident that the following propositions hold:

1) $\langle 0 \rangle_l = \langle 0 \rangle_r = \{0\}$;
2) $\langle \alpha \rangle_l = \langle \alpha \rangle_r = K^{inv}$ for any element $\alpha \in K^{inv}$;
3) $\langle x \rangle_l = \langle x \rangle_r$ for any element $x \in K^{cntr}$;
4) $x \in \langle x \rangle_l \cap \langle x \rangle_r$ for any element $x \in K$.
5) for any element $x \in K \setminus \{0\}$ to determine any specific element of the class $\langle x \rangle_l$ (correspondingly, of the class $\langle x \rangle_r$) it is sufficiently to determine corresponding element of the set K^{inv};

For any subsets A and B of the set K we set

$$A * B = \{ab \mid a \in A,\ b \in B\}. \quad (3)$$

It is worth noting that the identity $K^{inv} * K^{inv} = K^{inv}$ holds for any associative ring with unit.

Let D be the set of all elements of the ring K which commute with every element of the set K^{inv}. For any element $x \in D$ we get $\langle x \rangle_l = \langle x \rangle_r = \langle x \rangle$. Moreover, there hold identities $\langle x \rangle * \langle y \rangle = \langle xy \rangle$ $(x, y \in D)$. Therefore, $(\{\langle x \rangle \mid x \in D\}, *)$ is some semigroup.

The following theorem establishes that above pointed situation can be different for elements of the set $K \setminus D$, i.e. in case of associative non-commutative ring K with unit accordance of formula (3) with the sets $\mathsf{B}_l = K/_{\equiv_l}$ and $\mathsf{B}_r = K/_{\equiv_r}$ can fail.

Theorem 1. For any associative ring K with the unit relations

$$\langle xy\rangle_l \subseteq \langle x\rangle_l * \langle y\rangle_l, \quad (4)$$

$$\langle xy\rangle_r \subseteq \langle x\rangle_r * \langle y\rangle_r, \quad (5)$$

hold for all elements $x, y \in K^{non-inv} \setminus \{0\}$.

Proof. Let $x, y \in K^{non-inv} \setminus \{0\}$. Since K is associative ring with unit, we get

$$\langle x\rangle_l * \langle y\rangle_l = \{(\alpha x)(\beta y) \mid \alpha, \beta \in K^{inv}\} = \{\alpha((x\beta)y) \mid \alpha, \beta \in K^{inv}\} \supseteq \{\alpha(xy) \mid \alpha \in K^{inv}\} = \langle xy\rangle_l.$$

Thus, relation (4) holds.

Proof of relation (5) is similar.

Q.E.D.

Remark 4. For any associative ring K with unit, such that $K^{inv} \subseteq K^{cntr}$ (in particular, for any associative-commutative ring with unit) there hold identities $\langle x\rangle_l = \langle x\rangle_r = \langle x\rangle$. For these rings theorem 1 is transformed into the following proposition: for any elements $x, y \in K$ there holds identity $\langle xy\rangle = \langle x\rangle * \langle y\rangle$. Therefore, above determined generalization of the notion 'associated elements' for any associative (not necessarily, commutative) ring K with unit is nontrivial and has substantial sense.

Theorem 2. For any associative ring K with unit for all elements $x, y \in K$ there hold the following relations

$$\langle x\rangle_l * \langle y\rangle_r = \langle xy\rangle_l * K^{inv} = K^{inv} * \langle xy\rangle_r, \quad (6)$$

$$xy \in \langle x\rangle_r * \langle y\rangle_l. \quad (7)$$

Proof. Since K is associative ring with unit, we get

$$\langle x\rangle_l * \langle y\rangle_r = \{(\alpha x)(y\beta) \mid \alpha, \beta \in K^{inv}\} = \{\alpha(xy)\beta \mid \alpha, \beta \in K^{inv}\}. \quad (8)$$

Since

$$\{\alpha(xy) \mid \alpha \in K^{inv}\} = \langle xy\rangle_l,$$

then identity (8) implies that

$$\langle x\rangle_l * \langle y\rangle_r = \{u\beta \mid u \in \langle xy\rangle_l, \beta \in K^{inv}\} = \langle xy\rangle_l * K^{inv}.$$

Similarly, since

$$\{(xy)\beta \mid \beta \in K^{inv}\} = \langle xy\rangle_r,$$

then identity (8) implies that

$$\langle x\rangle_l * \langle y\rangle_r = \{\alpha v \mid \alpha \in K^{inv}, v \in \langle xy\rangle_r\} = K^{inv} * \langle xy\rangle_r.$$

Thus, relation (6) holds.

Since K is associative ring with unit, we get

$$\langle x\rangle_r * \langle y\rangle_l = \{(x\alpha)(\beta y) \mid \alpha, \beta \in K^{inv}\} = \{x(\alpha\beta)y \mid \alpha, \beta \in K^{inv}\} = \{x\delta y \mid \delta \in K^{inv}\}. \quad (9)$$

If we set $\delta = 1$ in (9), we get (7).

Q.E.D.

For any subsets A and B of the set K we set

$$A + B = \{a + b \mid a \in A, b \in B\}. \quad (10)$$

It is evident that:

1) $A + B = B + A$ for any subsets A and B of the set K, i.e. addition of subsets of the set K determined via formula (10) is commutative operation;
2) $\{0\} + A = A$ for any subset A of the set K.

The following theorem establishes that formula (10) is not in accordance with the sets $B_l = K/_{\equiv_l}$ and $B_r = K/_{\equiv_r}$.

Theorem 3. For any associative ring K with unit for any $x \in K$ and $i \in \mathbf{N}$, such that $i1 \in K^{inv}$ there hold the following relations

$$\langle x\rangle_l + K^{inv} \supseteq \langle x + i1\rangle_l, \quad (11)$$

$$\langle x\rangle_r + K^{inv} \supseteq \langle x + i1\rangle_r. \quad (12)$$

Proof. Since K is associative ring with unit, then for any integer $i \in \mathbf{N}$, such that $i1 \in K^{inv}$ we get

$$\langle x\rangle_l + K^{inv} = \{\alpha x + \beta \mid \alpha, \beta \in K^{inv}\} \supseteq$$
$$\supseteq \{\alpha x + \alpha(i1) \mid \alpha \in K^{inv}\} =$$
$$= \{\alpha(x + i1) \mid \alpha \in K^{inv}\} = \langle x + i1\rangle_l.$$

Thus, relation (11) holds.

Proof of relation (12) is similar.

Q.E.D.

To illustrate above established results we consider the following simple example.

Example 1. Since any ring $Z_{p^\beta} = (\mathbf{Z}_{p^\beta}, +, \cdot)$ (where p is prime integer and $\beta \geq 2$) is associative-commutative ring with unit, we get

$$B_l = B_r = B$$

and

$$B = \{\langle 0\rangle, \langle 1\rangle\} \cup B',$$

where

$$\langle 0\rangle = \{0\},$$

$$\langle 1\rangle = \mathbf{Z}_{p^\beta}^{inv} = \{a \in \mathbf{Z}_{p^\beta} \mid a \text{ is not multiple of } p\},$$

$$B' = \{C_i \mid i = 1, \ldots, \beta - 1\},$$

where

$$C_i = \{ap^i \mid a \in \mathbf{Z}_{p^\beta}^{inv}\} \ (i = 1, \ldots, \beta - 1\}.$$

Since Z_{p^β} is associative-commutative ring with unit, then $(B, *)$ is commutative semigroup, such that:

1) $\langle 0\rangle * \langle x\rangle = \langle 0\rangle$ for any $x \in \mathbf{Z}_{p^\beta}$;
2) $\langle 1\rangle * \langle x\rangle = \langle x\rangle$ for any $x \in \mathbf{Z}_{p^\beta}$;
3) for all $C_i, C_j \in B'$

$$C_i * C_j = \begin{cases} C_{i+j}, \text{if } i+j \le \beta - 1 \\ \langle 0 \rangle, \text{ if } i+j \ge \beta \end{cases}.$$

For addition of classes of associated elements of the ring Z_{p^β} determined via formula (10) we get:

1) $(\langle 1 \rangle + \langle 1 \rangle) \cap \langle x \rangle \ne \varnothing$ for any $x \in K$;
2) $\langle 0 \rangle \subseteq C_i + C_i$ for any $i = 1, \ldots, \beta - 1$;
3) $C_i \subseteq C_i + C_i$ for any $i = 1, \ldots, \beta - 1$;
4) $(C_i + C_i) \cap C_j \ne \varnothing$ for any $i = 1, \ldots, \beta - 2$ and $j = i+1, \ldots, \beta - 1$;
5) $C_i + C_j = C_i$ for all $1 \le i < j \le \beta - 1$.

4. Proposed scheme

On the base of above developed notions the following scheme for finding the set *S* of solutions for system (1) of multi-variable polynomial equations with parameters over any finite associative (not necessarily, commutative) ring $\mathsf{K} = (K, +, \cdot)$ with unit can be proposed.

Step 1. $S := \varnothing$.

Step 2. Replace each parameter a_j $(j = 1, \ldots, h)$ by some *l*-associated or *r*-associated class of elements (in other words, for each class $\langle x \rangle_l$ (correspondingly, for each class $\langle y \rangle_r$) present each parameter a_j $(j = 1, \ldots, h)$ in the form $b_j x$ (correspondingly, in the form $y b_j$), where $b_j \in K^{inv}$).

Step 3. Find the set *I* of all admissible combinations of *l*-associated or *r*-associated classes for parameters.

Step 4. If $I = \varnothing$, then HALT.

Step 5. Select $i \in I$, $I := I \setminus \{i\}$, $S_i := \varnothing$.

Step 6. Replace each variable u_j $(j = 1, \ldots, n)$ by some *l*-associated or *r*-associated class of elements (in other words, for each class $\langle z \rangle_l$ (correspondingly, for each class $\langle w \rangle_r$) present each variable u_j $(j = 1, \ldots, n)$ in the form $d_j z$ (correspondingly, in the form $w d_j$), where $d_j \in K^{inv}$).

Step 7. Find the set $Q(i)$ of all admissible combinations of *l*-associated or *r*-associated classes for variables.

Step 8. If $Q(i) = \varnothing$, then go to step 5, else go to step 9.

Step 9. Select $q \in Q(i)$, $Q(i) := Q(i) \setminus \{q\}$.

Step 10. Find the set S_{iq} of all solutions which values are in *q*, $S_i := S_i \cup S_{iq}$.

Step 11. If $Q(i) \ne \varnothing$, then go to step 9, else $S := S \cup S_i$ and go to step 12.

Step 12. If $I = \varnothing$, then HALT, else go to step 5.

Correctness of proposed scheme is implied by the factor that any solution of the system (1) can be uniquely determined in terms of classes of *l*-associated or *r*-associated elements.

The following simple example illustrates proposed scheme.

Example 2. Consider the following equation

$$a_1 u_1 u_2 = a_2$$

with parameters over associative-commutative ring $\mathsf{Z}_{p^2} = (\mathbf{Z}_{p^2}, +, \cdot)$ with unit, where *p* is prime integer.

After steps 1 and 2 we get

$$I = \{(\langle 0 \rangle, \langle 0 \rangle), (\langle 1 \rangle, \langle 0 \rangle), (\langle C_1 \rangle, \langle 0 \rangle), (\langle 1 \rangle, \langle 1 \rangle), (\langle 1 \rangle, \langle C_1 \rangle), (\langle C_1 \rangle, \langle C_1 \rangle)\}$$

Applying steps 3-12 to these indexes, we get

$$S_{(\langle 0 \rangle, \langle 0 \rangle)} = \mathbf{Z}^2_{p^2},$$

$$S_{(\langle 1 \rangle, \langle 0 \rangle)} = \{0\} \times \mathbf{Z}_{p^2} \cup \mathbf{Z}_{p^2} \times \{0\} \cup C_1 \times C_1,$$

$$S_{(C_1, \langle 0 \rangle)} = (\{0\} \cup C_1) \times \mathbf{Z}_{p^2} \cup \mathbf{Z}_{p^2} \times (\{0\} \cup C_1),$$

$$S_{(\langle 1 \rangle, \langle 1 \rangle)} = \{(d_1, d_1^{-1} a_1^{-1} a_2) \mid d_1 \in \mathbf{Z}^{inv}_{p^2}\},$$

$$S_{(\langle 1 \rangle, C_1)} = \{(d_1 p, d_1^{-1} a_1^{-1} b_2) \mid d_1 \in \mathbf{Z}^{inv}_{p^2}\} \cup$$
$$\cup \{(d_1 p, d_1^{-1} a_1^{-1} (b_2 + fp)) \mid d_1, f \in \mathbf{Z}^{inv}_{p^2}\} \cup$$
$$\cup \{(d_2^{-1} a_1^{-1} b_2, d_2 p) \mid d_2 \in \mathbf{Z}^{inv}_{p^2}\} \cup$$
$$\cup \{(d_2^{-1} a_1^{-1} (b_2 + fp), d_2 p) \mid d_2, f \in \mathbf{Z}^{inv}_{p^2}\},$$

where $a_2 = b_2 p$ $(b_2 \in \mathbf{Z}^{inv}_{p^2})$,

$$S_{(C_1, C_1)} = \{d_1, d_1^{-1} b_1^{-1} b_2 \mid d_1 \in \mathbf{Z}^{inv}_{p^2}\} \cup$$
$$\cup \{d_1, d_1^{-1} b_1^{-1} (b_2 + fp) \mid d_1, f \in \mathbf{Z}^{inv}_{p^2}\},$$

where $a_1 = b_1 p$ $(b_1 \in \mathbf{Z}^{inv}_{p^2})$ and $a_2 = b_2 p$ $(b_2 \in \mathbf{Z}^{inv}_{p^2})$.

5. Conclusions

In the given paper it is developed unified approach for presenting in implicit form the set of solutions for systems of polynomial equations with parameters over any finite associative (not necessarily, commutative) ring K with unit. Proposed implicit form is based on notions of classes of *l*-associated or *r*-associated elements of the ring K and its structure reflects real complexity for finding the set of solutions for specific system of equations. This complexity is justified by the factor that the result of addition for classes of associated elements can intersect with different classes of associated elements. Additional complexity for non-commutative rings is justified by the factor that the result of multiplication for classes of associated elements can also intersect with different classes of associated elements. Future investigations can be connected with extraction types of systems of polynomial equations with parameters over any finite associative (not necessarily, commutative) ring with unit with the determined in terms of complexity for finding the set of solutions in proposed implicit form.

References

1. Агибалов Г. П. Методы решения систем полиномиальных уравнений над конечным полем / Г. П. Агибалов // Вестник Томского государственного университета. Приложение. – 2006. – № 17. – С. 4–9.
2. Основы криптографии / Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. – М. : Гелиос АРВ, 2002. – 480 с.
3. Математические и компьютерные основы криптологии / Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. – Минск : Новое знание, 2003. – 382 с.
4. Курош А. Г. Лекции по общей алгебре / А. Г. Курош. – М. : Наука, 1973. – 400 с.
5. Кузьмин А. С. Псевдослучайные и полилинейные последовательности / А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев // Труды по дискретной математике. – Т. 1. – М. : Научное изд-во «ТВП», 1997. – С. 139–202.
6. Кузьмин А. С. Свойства линейных и полилинейных рекуррент над кольцами Галуа (I) / А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев // Труды по дискретной математике. – Т. 2. – М. : Научное изд-во «ТВП», 1998. – С. 191–222.
7. Skobelev V. V. Analysis of non-linear automata with the lag 2 over fi nite ring / V. V. Skobelev, V. G. Skobelev // Applied discrete mathematics. – 2010. – № 1. – P. 68–85.
8. Skobelev V. V. On complexity of analysis of automata over finite ring / V. V. Skobelev, V. G. Skobelev // Cybernetics and systematic analysis. – 2010. – № 4. – P. 17–30.
9. Скобелев В. В., Скобелев В. Г. Анализ шифрсистем / В. В. Скобелев, В. Г. Скобелев. – Донецк : ИПММ НАН Украины, 2009. – 479 с.
10. Скобелев В. В. Многообразия над кольцами. Теория и приложения / В. В. Скобелев, Н. М. Глазунов, В. Г. Скобелев. – Донецк : ИПММ НАН Украины, 2011. – 323 с.
11. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 328 с.

Скобелєв В. В.

ПРО СИСТЕМИ ПОЛІНОМІАЛЬНИХ РІВНЯНЬ НАД СКІНЧЕННИМИ КІЛЬЦЯМИ

Пошук та зберігання множини розв'язків систем поліноміальних рівнянь із параметрами над скінченними асоціативними (не обов'язково комутативними) кільцями є однією з основних проблем для різних прикладень, у яких використовуються алгебраїчні моделі над такими кільцями. У цій статті розвинемо уніфікований підхід для представлення у неявному вигляді множини розв'язків систем поліноміальних рівнянь із параметрами над довільним скінченним асоціативним (не обов'язково комутативним) кільцем з одиницею. Запропонований підхід засновано на поняттях класів l-асоційованих або r-асоційованих елементів кільця, які розвинемо у статті.

Ключові слова: асоціативні кільця, системи рівнянь, класи асоційованих елементів.

Матеріал надійшов 20.02.2012

УДК 004.056.5