МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 65 – 76

УДК 519.719.2

Non-commutative Hamilton – Cayley theorem and roots of characteristic polynomials of skew maximal period linear recurrences over Galois rings

M. A. Goltvanitsa

Certification Research Center, LLC, Moscow

Получено 17.III.2016

Abstract. Let p be a prime number, $R = \mathrm{GR}(q^d, p^d)$, where $q = p^r$, be a Galois ring, $S = \mathrm{GR}(q^{nd}, p^d)$ be its extension. We prove a non-commutative generalization of the well-known Hamilton – Cayley theorem. Using this result we prove the existence of roots in some extension $\mathcal{K}$ of $\check{S}$ for characteristic polynomials of skew maximal period linear recurrent sequences over S. Also for these polynomials we investigate the structure of the set of their roots.

Keywords: non-commutative Hamilton – Cayley theorem, skew LRS, maximal period, Galois ring

Некоммутативная теорема Гамильтона – Кэли и корни характеристических многочленов скрученных линейных рекуррент над кольцами Галуа

М. А. Гольтваница

ООО «Центр сертификационных исследований», Москва

Аннотация. Пусть p — простое число, $q = p^r$, $R = \mathrm{GR}(q^d, p^d)$ — кольцо Галуа, $S = \mathrm{GR}(q^{nd}, p^d)$ — его расширение. Рассматриваются скрученные линейные рекуррентные последовательности максимального периода (ЛРП МП) над S. В работе доказано некоммутативное обобщение хорошо известной теоремы Гамильтона – Кэли. С использованием этого результата устанавливается существование корней характеристических многочленов скрученных ЛРП МП в некотором расширении $\mathcal{K}$ кольца $\check{S}$. Изучается структура множества корней этих многочленов.

Ключевые слова: некоммутативная теорема Гамильтона – Кэли, скрученные ЛРП, максимальный период, кольцо Галуа

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 65–76 (Russian)

References

[1] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A., "Linear recurring sequences over rings and modules", *J. Math. Sci.*, **76**:6 (1995), 2793–2915.

[2] Nechaev A. A., "Kerdock code in a cyclic form", *Discrete Math. Appl.*, **1**:4 (1991), 365–384.

[3] Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., "Skew linear recurring sequences of maximal period over Galois rings", *J. Math. Sci.*, **187**:2 (2012), 115–128.

[4] Kurakin V. L., Mikhalev A. V., Nechaev A. A., Tsypyschev V. N., "Linear and polylinear recurring sequences over Abelian groups and modules", *J. Math. Sci.*, **102**:6 (2000), 4598–4626.

[5] Goltvanitsa M. A., Nechaev A. A., Zaitsev S. N., "Skew LRS of maximal period over Galois rings", *Mathematical Aspects of Cryptography*, **4**:2 (2013), 59–72.

[6] Goltvanitsa M. A., "A construction of skew LRS of maximal period over finite fields based on the defining tuples of factors", *Mathematical Aspects of Cryptography*, **5**:2 (2014), 37–46.

[7] Goltvanitsa M. A., "Digit sequences of skew linear recurrences of maximal period over Galois rings", *Mathematical Aspects of Cryptography*, **6**:2 (2015), 189–197.

[8] Goltvanitsa M. A., "The first digit sequence of skew linear recurrence of maximal period over Galois ring", *Mathematical Aspects of Cryptography*, **7**:3 (2016), 5–18.

[9] Goltvanitsa M. A., "About one class of skew linear recurrences of maximal period over Galois rings", *Vysoko dostupnye systemy*, **11**:3 (2015), 28–48 (in Russian).

[10] Glukhov M. M., Elizarov V. P., Nechaev A. A., *Algebra, I*, M.: Gelios ARV, 2003 (in Russian), 336 pp.

[11] Glukhov M. M., Elizarov V. P., Nechaev A. A., *Algebra, II*, M.: Gelios ARV, 2003 (in Russian), 416 pp.