Неассоциативные структуры в гомоморфной криптографии*

В. Т. МАРКОВ

А. В. МИХАЛЁВ
Московский государственный университет им. М. В. Ломоносова, Московский центр фундаментальной и прикладной математики

Е. С. КИСЛИЦЫН
Московский государственный университет им. М. В. Ломоносова, Московский центр фундаментальной и прикладной математики
e-mail: kislicynevgeniy@mail.ru

УДК 512.552.7+512.554+519.72

Ключевые слова: квазигруппа, квазигрупповое кольцо, автоморфизм, гомоморфное шифрование.

Аннотация

В данной статье получен ответ на вопрос о классификации квазигрупповых колец по количеству элементов с левым нулевым аннулятором для различных квазигрупп. Эта классификация стала возможна благодаря доказательству критерия быть элементом с левым нулевым аннулятором в квазигрупповом кольце. На основе данного критерия произведены вычисления для различных полей и квазигруппы порядка 4 для нахождения закономерностей и получены два результата о том, когда в квазигрупповых кольцах содержится одинаковое число элементов с левым нулевым аннулятором и когда элемент квазигруппового кольца $\mathrm{GF}(p)Q$ с фиксированной квазигруппой Q будет иметь левый нулевой аннулятор в квазигрупповом кольце $\mathrm{GF}(p^n)Q$.

Abstract

V. T. Markov, A. V. Mikhalev, E. S. Kislitsyn, Non-associative structures in homomorphic encryption, Fundamentalnaya i prikladnaya matematika, vol. 23 (2020), no. 2, pp. 209—215.

In this paper, we obtain a classification of quasigroup rings by the quantity of elements with null left annihilator for different quasigroups. This classification becomes possible due to a criterion of being an element with null left annihilator in a quasigroup ring. By virtue of this criterion, we make a calculation to find regularities using various fields and quasigroups with order 4. This outcome helps us to obtain two results where any two quasigroup rings have the same number of elements with null left annihilator and the element of the quasigroup ring $\mathrm{GF}(p)Q$ with fixed quasigroup Q has null left annihilator in the quasigroup ring $\mathrm{GF}(p^n)Q$.

*Статья подготовлена при финансовой поддержке гранта «Структурная теория и комбинаторно-логические методы в теории алгебраических систем» Московского центра фундаментальной и прикладной математики.

Фундаментальная и прикладная математика, 2020, том 23, № 2, с. 209—215.

1. Введение

Результаты данной статьи были получены при изучении криптосхемы для квазигруппового кольца, предложенной А. В. Грибовым, П. А. Золотых, А. В. Михалёвым [2]. Исследовался вопрос о строгости изложенного алгоритма криптосхемы: сколько «достаточно» элементов с левым нулевым аннулятором в квазигрупповом кольце для корректной формулировки? Хотелось бы знать точное или приближённое значение количества элементов с левым нулевым аннулятором, чтобы понять, насколько устойчивой будет криптосхема. Для этого требуется классифицировать квазигрупповые кольца.

2. Основные алгебраические понятия

Определение 2.1. Квазигруппой (см. [1]) называется множество Q с определённой на нём бинарной операцией $\cdot\colon Q\times Q\to Q$, удовлетворяющее следующему условию: для любых $a,b\in Q$ найдутся единственные $x,y\in Q$, такие что

$$a\cdot x=b,\quad y\cdot a=b.$$

Определение 2.2. Квазигруппа (см. [1]) $(Q,\cdot)$ называется изотопной квазигруппе $(R,\circ)$, если можно установить биекцию между Q и R и при этом существуют перестановки α, β, γ, действующие на этих квазигруппах, такие что для любых $x,y\in Q$ выполняется

$$x\cdot y=\gamma^{-1}\bigl(\alpha(x)\circ\beta(y)\bigr).$$

Определение 2.3. Пусть R — некоммутативное кольцо, S — непустое подмножество кольца R. Тогда левым аннулятором подмножества S называется следующее множество:

$$\mathrm{LAnn}(S)=\{r\in R\colon rs=0 \text{ для каждого } s\in S\}.$$

Аналогично определяется правый аннулятор множества S с тем условием, что умножение на элемент кольца происходит справа. Также можно определить левый аннулятор для одного элемента $a\in R$, если положить $S=\{a\}$.

Определение 2.4. Пусть R — кольцо с единицей (необязательно ассоциативное), Q — конечная квазигруппа. Множество RQ, согласно [3] состоящее из всех формальных сумм вида $\sum\limits_{q\in Q}\alpha_q\cdot q$ ($\alpha_q\in R$), называется квазигрупповым кольцом с определёнными на нём операциями сложения и умножения

$$\sum_{q\in Q}\alpha_q\cdot q+\sum_{q\in Q}\beta_q\cdot q=\sum_{q\in Q}(\alpha_q+\beta_q)\cdot q,\quad \sum_{q\in Q}\alpha_q\cdot q\cdot\sum_{q\in Q}\beta_q\cdot q=\sum_{q\in Q}\gamma_q\cdot q,$$

где

$$\gamma_q=\sum_{q=q'\cdot q''\in Q}(\alpha_{q'}\cdot\beta_{q''})\cdot q.$$

Рассмотрим квазигруппу Q порядка n, $K = \mathrm{GF}(p^k)$, где p простое, $n, k \in \mathbb{N}$. Тогда в качестве элементов KQ будут выступать суммы $\sum\limits_{q \in Q} \alpha_q \cdot q$ ($\alpha_q \in K$). Значит, в качестве нулевого элемента будет выступать сумма $(0, x_1) + (0, x_2) + \ldots + (0, x_n)$, где $x_1, x_2, \ldots, x_n \in Q$. Таким образом, рассматривая произведение

$$b \cdot a = \sum_{q' \in Q} \beta'_q \cdot q' \cdot \sum_{q'' \in Q} \alpha_q \cdot q'' = \sum_{q \in Q} \gamma_q \cdot q \qquad (*)$$

($q = q' \cdot q''$ согласно таблице Кэли квазигруппы Q, $\alpha'_q \cdot \alpha''_q = \alpha_q$ согласно таблице Кэли K), получаем следующую теорему.

Теорема 2.1. *Пусть K — коммутативное ассоциативное кольцо с единицей, Q — квазигруппа порядка n. Элемент квазигруппового кольца $a = (\alpha_{q_1}, \ldots, \alpha_{q_n})$ будет иметь нулевой левый аннулятор тогда и только тогда, когда определитель матрицы вида*

$$\begin{pmatrix} \alpha_{i_1} & \ldots & \alpha_{i_n} \\ \vdots & \ddots & \vdots \\ \alpha_{j_1} & \ldots & \alpha_{j_n} \end{pmatrix}, \qquad (**)$$

где наборы $(i_1, \ldots, i_n), \ldots, (j_1, \ldots, j_n)$ являются строками таблицы Кэли, задающей квазигруппу Q, не равен нулю.

Доказательство. Элемент a имеет левый нулевой аннулятор тогда и только тогда, когда в выражении $(*)$ для каждого $q \in Q$ справедливо $\gamma_q = 0$, то имеет место тогда и только тогда, когда для каждого $q \in Q$ $\beta_q = 0$, т. е. тогда и только тогда, когда

$$\begin{aligned} &(\beta_{q_1} q_1 + \ldots + \beta_{q_n} q_n)(\alpha_{q_1} q_1 + \ldots + \alpha_{q_n} q_n) = \\ &\quad = \beta_{q_1}\alpha_{q_1}(q_1 \cdot q_1) + \ldots + \beta_{q_1}\alpha_{q_n}(q_1 \cdot q_n) + \\ &\quad + \beta_{q_2}\alpha_{q_1}(q_2 \cdot q_1) + \ldots + \beta_{q_2}\alpha_{q_n}(q_1 \cdot q_n) + \ldots + \\ &\quad + \beta_{q_n}\alpha_{q_1}(q_n \cdot q_1) + \ldots + \beta_{q_n}\alpha_{q_n}(q_n \cdot q_n) = \\ &\quad = 0 \cdot q_1 + \ldots + 0 \cdot q_n. \end{aligned}$$

Каждая скобка $(q_i \cdot q_j)$ будет переходить в элемент q_k согласно таблице Кэли квазигруппы Q. Таким образом, собирая при каждом элементе q_k слагаемые, получаем

$$(\beta_{q_1}\alpha_{i_1} + \ldots + \beta_{q_n}\alpha_{i_n})q_1 + \ldots + (\beta_{q_1}\alpha_{j_1} + \ldots + \beta_{q_n}\alpha_{j_n})q_n = 0 \cdot q_1 + \ldots + 0 \cdot q_n.$$

В итоге получается система

$$\begin{pmatrix} \alpha_{i_1} & \ldots & \alpha_{i_n} \\ \vdots & \ddots & \vdots \\ \alpha_{j_1} & \ldots & \alpha_{j_n} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix},$$

которая имеет только нулевое решение тогда и только тогда, когда матрица $(**)$ имеет ненулевой определитель. □

Для понимания, сколько элементов с левым нулевым аннулятором насчитывается в различных квазигрупповых кольцах, были рассмотрены квазигрупповые кольца, составленные на полях $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$, $\mathrm{GF}(2^2)$, $\mathrm{GF}(2^3)$ и неизоморфных квазигруппах порядка 4, полученные полным перебором (их оказалось 35). Далее были построены все элементы длины 4 над каждым из полей и из них получены матрицы, отвечающие таблице Кэли каждой квазигруппы. Таким образом на основе предыдущей теоремы были получены все элементы с левым нулевым аннулятором для каждого квазигруппового кольца и составлена следующая таблица (в таблице указано количество квазигрупп, в квазигрупповых кольцах которых имеется указанное количество элементов с левым нулевым аннулятором).

Количество элементов с левым нулевым аннулятором	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathrm{GF}(2^2)$	$\mathbb{Z}_5$	$\mathbb{Z}_7$	$\mathrm{GF}(2^3)$	$\mathbb{Z}_{11}$
8 (50 %)	35						
16 (20 %)		15					
32 (39.5 %)		20					
192 (75 %)			35				
256 (41 %)				35			
1296 (54 %)					15		
1728 (72 %)					20		
3584 (87 %)						35	
10000 (68 %)							15
12000 (82 %)							20

При изучении данных квазигрупповых колец получено, что квазигрупповые кольца для одного и того же поля могут иметь различное количество элементов с левым нулевым аннулятором в зависимости от квазигруппы. Относительно количества элементов с левым нулевым аннулятором квазигрупповые кольца будут относиться к одному из изотопических классов латинских квадратов, имеющих одинаковую размерность. В нашем случае это два класса для латинских квадратов размера 4×4. Для изотопического класса получено следующее утверждение.

Предложение 2.2. *В квазигрупповых кольцах содержится одинаковое число элементов с левым нулевым аннулятором, если квазигруппы, на которых построены эти кольца, изотопны. Иначе говоря, если Q_1 изотопна Q_2, то KQ_1 и KQ_2 имеют одинаковое число элементов с левым нулевым аннулятором.*

Доказательство. Два квазигрупповых кольца KQ_1 и KQ_2 имеют одинаковое количество элементов с левым нулевым аннулятором тогда и только тогда,

когда одинаковое количество систем линейных уравнений имеют тривиальное решение, т. е. тогда и только тогда, когда одинаковое количество матриц вида

$$\begin{pmatrix} \beta_{i_1} & \dots & \beta_{i_n} \\ \vdots & \ddots & \vdots \\ \beta_{j_1} & \dots & \beta_{j_n} \end{pmatrix}$$

имеют ненулевой определитель ($(i_1, \dots, i_n), \dots, (j_1, \dots, j_n)$ — строки таблицы Кэли соответствующей квазигруппы).

Если две квазигруппы Q_1 и Q_2 изотопны, то изотопны и их латинские квадраты (т. е. таблицы Кэли). Тогда нужно проверить неравенство нулю определителя двух матриц, составленных на изотопных таблицах Кэли. Перестановка строк и столбцов может только поменять знак определителя, следовательно, неравенство нулю сохраняется. Подстановка из S_n элементов латинского квадрата даст, очевидно, другой латинский квадрат, который можно привести к предыдущему с помощью конечного числа перестановок строк и столбцов, из чего получаем, что опять же неравенство нулю сохранится.

В обратную сторону предложение неверно ввиду контрпримеров, приведённых выше. Действительно, два квазигрупповых кольца $\mathbb{Z}_2 Q_1$ и $\mathbb{Z}_2 Q_2$ с квазигруппами из разных изотопических классов будут иметь одинаковое количество элементов с левым нулевым аннулятором (а именно 8), но сами квазигруппы Q_1 и Q_2 изотопны не будут. □

При изучении данных, полученных при компьютерных вычислениях, оказалось верно следующее утверждение.

Предложение 2.3. *Пусть имеется квазигруппа Q порядка n и поля* $\mathrm{GF}(p)$ *и* $\mathrm{GF}(p^n)$. *Тогда если элемент r имеет левый нулевой аннулятор в квазигрупповом кольце* $\mathrm{GF}(p)Q$, *то он имеет левый нулевой аннулятор в кольце* $\mathrm{GF}(p^n)Q$.

Доказательство. Очевидно, что $\mathrm{GF}(p)Q$ вкладывается в $\mathrm{GF}(p^n)Q$. Согласно теореме 2.1 достаточно доказать, что если элемент r и составленная матрица R, отвечающая таблице Кэли указанной квазигруппы Q, имеет ненулевой определитель над $\mathrm{GF}(p)$, то он имеет ненулевой определитель над $\mathrm{GF}(p^n)$. Действительно, допустим, что матрица R имеет нулевой определитель в $\mathrm{GF}(p^n)$. Тогда R имеет нулевой определитель в $\mathrm{GF}(p)$, так как, совершая элементарные преобразования, мы не покинем подполе $\mathrm{GF}(p)$. Противоречие. □

3. Приложение: шифрование, основанное на квазигрупповых кольцах

Данная теория используется в шифровании на квазигрупповых кольцах, так как от количества элементов в квазигрупповом кольце зависит стойкость шифрования. Шифрование, в свою очередь, предлагает вариант гомоморфного шифрования (см. [4]).

Предполагаем, что группы автоморфизмов $\operatorname{Aut} K$ кольца K и $\operatorname{Aut} Q$ квазигруппы Q некоммутативны, причём $|\operatorname{Aut} K| \geqslant t_1$, $|\operatorname{Aut} Q| \geqslant t_2$, где t_1 и t_2 — параметры безопасности. Также предполагаем, что в KQ достаточно элементов с нулевым левым аннулятором. На вопрос, сколько элементов будет достаточно, пока ответа нет, но классификация групп автоморфизмов, описанная выше, может помочь решить эту задачу.

Для лучшего понимания предложен упрощённый вариант криптосхемы [2].

Участник A:

1) конструирует такой автоморфизм $\sigma \in \operatorname{Aut} K$, что его порядок больше, чем t_3, $|\sigma| \geqslant t_3$, причём σ имеет нетривиальный централизатор $C(\sigma)$ в группе $\operatorname{Aut} K$ и $|C(\sigma) \setminus \langle\sigma\rangle| \geqslant t_4$, где t_3, t_4 — параметры безопасности;
2) конструирует такой автоморфизм $\eta \in \operatorname{Aut} Q$, что его порядок больше, чем t_5, $|\eta| \geqslant t_5$, причём η имеет нетривиальный централизатор $C(\eta)$ в группе $\operatorname{Aut} Q$ и $|C(\eta) \setminus \langle\eta\rangle| \geqslant t_6$, где t_5, t_6 — параметры безопасности;
3) случайно выбирает автоморфизмы $\tau \in C(\sigma) \setminus \langle\sigma\rangle$ и $\omega \in C(\eta) \setminus \langle\eta\rangle$;
4) по τ и ω строит автоморфизм $\varphi \in \operatorname{Aut} KQ$ (назовём его секретным автоморфизмом, он же является секретным ключом) так: для любого $h \in KQ$ вида
$$h = a_{q_1} q_1 + \ldots + a_{q_n} q_n,$$
где $Q = \{q_1, \ldots, q_n\}$ — исходная квазигруппа, $a_{q_1}, \ldots, a_{q_n} \in K$, пусть
$$\varphi(h) = \tau(a_{q_1})\omega(q_1) + \ldots + \tau(a_{q_n})\omega(q_n);$$
5) выбирает элемент $x \in KQ$ и вычисляет $\varphi(x)$.

Открытым ключом участника A является
$$\big(\sigma, \eta, x, \varphi(x)\big).$$

Отметим, что при должных параметрах безопасности t_3, t_4, t_5, t_6 автоморфизмов, подходящих для открытого ключа, достаточно много. Сформированный открытый ключ участник A передаёт участнику B по открытому каналу.

Участник B:

1) выбирает натуральные числа (k, l);
2) используя открытый ключ участника A, получает пары автоморфизмов (σ^k, η^l) и по ним строит автоморфизм $\psi \in \operatorname{Aut} KQ$ таким же способом, как и участник A, т. е. для любого $h \in KQ$ вида $h = a_{q_1} q_1 + \ldots + a_{q_n} q_n$ полагает
$$\psi(h) = \sigma^k(a_{q_1})\eta^l(q_1) + \ldots + \sigma^k(a_{q_n})\eta^l(q_n).$$
Автоморфизм ψ будем называть сеансовым;
3) вычисляет $\psi(x)$, $\psi\big(\varphi(x)\big)$ и левый аннулятор $\operatorname{Ann}\big(\psi\big(\varphi(x)\big)\big)$;
4) если полученный аннулятор $\operatorname{Ann} \psi\big(\varphi(x)\big)$ ненулевой, то производится новый сеанс связи с выбором нового элемента x или же выбираются другие сеансовые автоморфизмы;

5) записывает исходный текст, который надо передать, в виде $m \in KQ$ и вычисляет $m \cdot \big[\psi\big(\varphi(x)\big)\big]$;
6) отправляет для A криптограмму

$$\big(\psi(x), m \cdot \big[\psi\big(\varphi(x)\big)\big]\big).$$

Получив криптограмму, участник A расшифровывает её:

1) используя секретный автоморфизм φ, вычисляет $\varphi\big(\psi(x)\big)$;
2) расшифровывает посланный текст, пользуясь тем, что ψ и φ коммутируют, поскольку сеансовый автоморфизм ψ построен на степенях выбранных автоморфизмов σ, η, а секретный автоморфизм φ построен с помощью элементов из централизаторов элементов σ, η.

Участник A знает $m \cdot \big[\varphi\big(\psi(x)\big)\big] = h$ и $\varphi\big(\psi(x)\big) = r$; следовательно, для получения сообщения m достаточно решить линейную систему $m \cdot r = h$ с коэффициентами из кольца K.

Если в квазигрупповом кольце этого алгоритма будет мало элементов с левым нулевым аннулятором, то, помимо того что нужно будет находить другой сеансовый автоморфизм, если он будет найден, у злоумышленника, ввиду малого количества элементов с левым нулевым аннулятором, будет возможность перебрать и дешифровать криптосхему. По результатам проделанного опыта (см. таблицу выше) можно сформулировать гипотезу, что с увеличением количества элементов в квазигрупповом кольце (а именно количества элементов поля, на котором построено квазигрупповое кольцо) будет увеличиваться количество элементов с нулевым аннулятором.

Литература

[1] Белоусов В. Д. Основы теории квазигрупп и луп. — М.: Наука, 1967.

[2] Грибов А. В., Золотых П. А., Михалёв А. В. Построение алгебраической криптосистемы над квазигрупповым кольцом // Матем. вопросы криптографии. — 2010. — Т. 4, № 4. — С. 23—33.

[3] Катышев С. Ю., Марков В. Т., Нечаев А. А. Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей. — 2014.

[4] Gentry C. A fully homomorphic encryption scheme: PhD thesis. — Stanford Univ., 2009.