ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

УДК 512.54

СТРУКТУРА ПОДГРУПП ГРУППЫ ГЕЙЗЕНБЕРГА НАД ПРОСТЫМ ПОЛЕМ ГАЛУА И ПРИЛОЖЕНИЯ К КРИПТОГРАФИИ

В.М. Деундяк, Д.И. Кокшаров, *koksharovd06@yandex.ru*
Научно-исследовательский институт «Специализированные вычислительные устройства защиты и автоматика», Южный федеральный университет, г. Ростов-на-Дону

Изучается конечная группа Гейзенберга над простым полем Галуа, для которой найдены все собственные подгруппы, выделены нормальные подгруппы, и построены соответствующие факторгруппы. Результаты могут быть применимы для построения новых кодовых криптосистем, т.к. для построения соответствующих кодов на некоммутативных группах необходимо изучение структуры подгрупп этих групп. В настоящее время стойкость большинства ассиметричных криптосистем основана на сложности задач факторизации или дискретного логарифмирования. С развитием квантовых компьютеров эти задачи можно будет решить за полиномиальное время, что ставит стойкость таких криптосистем под угрозу, и в качестве альтернативы им рассматриваются кодовые криптосистемы. В связи с этим особый интерес представляют кодовые криптосистемы на некоммутативных групповых алгебрах.

Ключевые слова: группа Гейзенберга, простое поле Галуа, собственная подгруппа, нормальная подгруппа, факторгруппа, индуцированный код.

STRUCTURE OF SUBGROUPS OF THE HEISENBERG GROUP OVER A PRIME GALOIS FIELD AND AN APPLICATION TO CRYPTOGRAPHY

V.M. Deundyak, D.I. Koksharov
Scientific Research Institute "Specialized Security Computing Devices and Automation", Southern Federal University, Rostov-on-Don

We study a finite Heisenberg group over a prime Galois field for which all proper subgroups were found, normal subgroups were distinguished, and the corresponding factor groups were constructed. The results can be applied to the construction of new code cryptosystems, because for the construction of the corresponding codes on noncommutative groups it is necessary to study the structure of subgroups of these groups. Currently, the strength of most asymmetric cryptosystems is based on the complexity of the problem of factorization or discrete logarithm. With the development of quantum computers, these problems can be solved in polynomial time, which puts the strength of such cryptosystems at risk, and as an alternative, they are considered code cryptosystems. In this regard, code cryptosystems on noncommutative group algebras are of particular interest.

Keywords: Heisenberg group, prime Galois field, proper subgroup, normal subgroup, quotient group, induced code.

Введение

Стойкость применяемых на практике асимметричных криптосистем в большинстве случаев основана на сложности задач факторизации целых чисел или дискретного логарифмирования в конечной группе [1]. Но с развитием квантовых компьютеров эти задачи будет возможно решить за полиномиальное время, что позволит взломать многие известные криптосистемы [2], [3]. Для улучшения стойкости предлагается использовать системы на основе помехоустойчивых кодов – кодовые криптосистемы. Стойкость таких криптосистем интенсивно изучается в настоящее время, краткий обзор этой тематики содержится в [4]. В частности, уже были взломаны такие криптосистемы, как криптосистема Сидельникова [5] и криптосистема Нидеррайтера [6]. Существует предположение, что использование помехоустойчивых кодов, которые не обладают ярко выраженной алгебра-

ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

ической структурой, может улучшить стойкость кодовых криптосистем. Применение этого подхода использовано в [7], [8], где предлагается в криптосистеме типа Мак-Элиса использовать коды, индуцированные групповыми кодами на некоммутативных группах, а также тензорные произведения кодов. В связи с этим возникает задача описания структуры подгрупп некоммутативных групп и построение соответствующих групповых кодов. Коды на конечной диэдральной группе были изучены в [9,10]. Настоящая работа посвящена решению задачи исследования подгрупп группы Гейзенберга $\mathbb{H}(\mathbb{F}_{\mathrm{p}})$ над простым полем Галуа $\mathbb{F}_{\mathrm{p}}$. Полученные результаты могут быть применены в теории кодовых криптосистем.

Групповые алгебры и групповые коды

Пусть $\mathbb{G}$ - конечная группа, $\mathbb{F}_s$ - поле Галуа [11]. Рассмотрим групповую алгебру $\mathbb{F}_s\mathbb{G}$, элементами которой являются формальные суммы (функции):

$$\sum_{g\in\mathbb{G}} a_g g\,, a_g \in \mathbb{F}_s,$$

(см., например, [12]). Сложение в $\mathbb{F}_s\mathbb{G}$ выполняется покомпонентно, а умножение выполняется по правилу:

$$\left(\sum_{g\in\mathbb{G}} a_g g\right)\cdot\left(\sum_{g\in\mathbb{G}} b_g g\right)=\sum_{g\in\mathbb{G}}\left(\sum_{w\in\mathbb{G}} a_{gw^{-1}}b_w\right)g,$$

при этом внешняя сумма в правой части является формальной, а внутренняя сумма - это сумма над полем $\mathbb{F}_s$. Например, если в качестве группы $\mathbb{G}$ взять $\mathbb{Z}_n$, то умножение в групповой алгебре $\mathbb{F}_s\mathbb{Z}_n$ примет вид обычной свертки.

Для алгебры A идеалом называется подалгебра, замкнутая относительно умножения на элементы из A. При этом идеал называется левым (правым), если он замкнут относительно умножения слева (справа) на элементы из A. Идеал алгебры A, являющийся одновременно левым и правым, называется двусторонним.

В соответствии с [13], с.39, всякий отличный от $\{0\}$ левый идеал J в групповой алгебре $\mathbb{F}_s\mathbb{G}$ называется групповым кодом ($\mathbb{F}_s\mathbb{G}$-кодом) длины $n(J) = |\mathbb{G}|$. Эти коды будем называть кодами на группе $\mathbb{G}$.

Конечная группа Гейзенберга

Рассмотрим $\mathbb{F}_p$ – поле Галуа мощности p, где p – произвольное простое число, $p > 2$. Группа Гейзенберга $\mathbb{H}(\mathbb{F}_p)$ определяется как множество (3×3) - матриц вида

$$\begin{pmatrix}1 & x & t\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix},\ x,y,t\in\mathbb{F}_p,$$

[14], с. 293. Для удобства элементы группы будем обозначать тройками: (x,y,t). В качестве групповой операции используется обычное умножение матриц:

$$(x,y,t)\cdot(\hat{x},\hat{y},\hat{t})=(x+\hat{x},y+\hat{y},t+\hat{t}+x\hat{y}),$$

нейтральным элементом является $\boldsymbol{e}=(0,0,0)$, а обратный элемент вычисляется по формуле

$$(x,y,t)^{-1}=(-x,-y,xy-t).$$

Легко заметить, что группа Гейзенберга не является абелевой.

ISSN 2658 – 7505
Выпуск №6, 2019
Электронный научный журнал «Вестник молодёжной науки России»

Интерес для приложений в криптографии представляют коды в групповой алгебре $\mathbb{F}_s\mathbb{H}(\mathbb{F}_p)$.

Основные результаты

Теорема 1. Рассмотрим группу Гейзенберга $\mathbb{H}(\mathbb{F}_p)$. В этой группе содержатся следующие собственные подгруппы:

1) подгруппа

$$\mathcal{H}_1 = \{(0,0,t) \mid t \in \mathbb{F}_p\},$$

изоморфная группе $\mathbb{Z}_p$ и являющаяся центром группы $\mathbb{H}(\mathbb{F}_p)$;

2) серия подгрупп

$$\mathcal{H}_{\{2;x,y,t\}} = \langle (x,y,t) \rangle,$$

где $x \neq 0$ или $y \neq 0$, каждая из которых изоморфна группе $\mathbb{Z}_p$, при этом

$$\mathcal{H}_{\{2;x,y,t\}} = \mathcal{H}_{\{2;\hat{x},\hat{y},\hat{t}\}} \Leftrightarrow \exists k \in \{1,2,\dots,p\}:$$

$$(\hat{x},\hat{y},\hat{t}) = (kx, ky, kt + \frac{(k-1)k}{2}xy)$$

и различных подгрупп этой серии имеется $p^2 + p$;

3) подгруппа

$$\mathcal{H}_3 = \{(x,0,t) \mid x,t \in \mathbb{F}_p\},$$

которая разлагается в прямую сумму $\mathcal{H}_1 \oplus \mathcal{H}_{\{2;1,0,0\}}$ и изоморфна группе $\mathbb{Z}_p \oplus \mathbb{Z}_p$;

4) серия подгрупп

$$\mathcal{H}_{\{4;\mathrm{i}\}} = \{(iy,y,t) \mid y,t \in \mathbb{F}_p\},\ i \in \mathbb{F}_p,$$

каждая из которых разлагается в прямую сумму $\mathcal{H}_1 \oplus \mathcal{H}_{\{2;i,1,0\}}$ и изоморфна группе $\mathbb{Z}_p \oplus \mathbb{Z}_p$, при этом все подгруппы этой серии различны.

Других собственных подгрупп группы Гейзенберга нет.

Отметим, что хотя сама группа Гейзенберга $\mathbb{H}(\mathbb{F}_p)$ абелевой не является, все ее собственные подгруппы абелевы.

Теорема 2. Подгруппы $\mathcal{H}_1$, $\mathcal{H}_3$ и $\mathcal{H}_{\{4;\mathrm{i}\}}$ являются нормальными подгруппами, подгруппы вида $\mathcal{H}_{\{2;x,y,t\}}$ не являются нормальными.

Теорема 3. Рассмотрим в группе Гейзенберга $\mathbb{H}(\mathbb{F}_p)$ нормальные подгруппы: $\mathcal{H}_1$, $\mathcal{H}_3$, $\mathcal{H}_{\{4;\mathrm{i}\}}$, где $i \in F_p$. Тогда

1. Факторгруппа $\mathbb{H}(\mathbb{F}_p)/\mathcal{H}_1$ изоморфна $\mathbb{Z}_p \oplus \mathbb{Z}_p$.
2. Факторгруппа $\mathbb{H}(\mathbb{F}_p)/\mathcal{H}_3$ изоморфна $\mathbb{Z}_p$.
3. Факторгруппа $\mathbb{H}(\mathbb{F}_p)/\mathcal{H}_{\{4;\mathrm{i}\}}$ изоморфна $\mathbb{Z}_p$.

О применении в криптографии

Рассмотрим некоторую алгебру A и произвольное непустое подмножество $X \subseteq A$. Для подмножества X алгебры A в [13], с.69, определен левый идеал

$$A \cdot X = \sum_{x \in X} Ax \subseteq A,$$

порожденный множеством X. Следовательно, если $A = \mathbb{F}_s\mathbb{G}$, то $A \cdot X$ - групповой код. Например, для произвольного подмножества X групповой алгебры $\mathbb{F}_s\mathbb{H}(\mathbb{F}_p)$ можно определить групповой код $\mathbb{F}_s\mathbb{H}(\mathbb{F}_p) \cdot X$.

Пусть $\mathbb{G}$ - конечная группа, $\mathcal{H}$ - ее подгруппа, $\lambda = |\mathbb{G}|/|\mathcal{H}|$ - индекс подгруппы $\mathcal{H}$ в группе $\mathbb{G}$. Рассмотрим некоторый $\mathbb{F}_s\mathcal{H}$-код N размерности $k(N)$ и

длины $n(N) = |\mathcal{H}|$. Тогда код $\mathbb{F}_s\mathbb{G} \cdot N$ является $\mathbb{F}_s\mathbb{G}$-кодом и называется кодом, индуцированным $\mathbb{F}_s\mathcal{H}$-кодом N [7]. При этом

$$k(\mathbb{F}_s\mathbb{G} \cdot N) = \lambda k(N), n(\mathbb{F}_s\mathbb{G} \cdot N) = |\mathbb{G}| = \lambda n(N).$$

В силу [13], с. 84, код $\mathbb{F}_s\mathbb{G} \cdot N$ изоморфен тензорному произведению $\mathbb{F}_s\mathbb{G} \otimes_{\mathbb{F}_s\mathcal{H}} N$. Далее эти коды будем отождествлять.

Рассмотрим группу Гейзенберга $\mathbb{H}(\mathbb{F}_p)$ и ее подгруппу $\mathcal{H}$. Пусть N - некоторый $\mathbb{F}_s\mathcal{H}$-код. Тогда можно построить индуцированный код

$$\mathbb{F}_s\mathbb{H}(\mathbb{F}_p) \cdot N = \mathbb{F}_s\mathbb{H}(\mathbb{F}_p) \otimes_{\mathbb{F}_s\mathcal{H}} N.$$

Из теоремы 1 вытекает, что у группы Гейзенберга подгруппы изоморфны либо $\mathbb{Z}_p$, либо $\mathbb{Z}_p \oplus \mathbb{Z}_p$. Следовательно, можно перенести известные циклические коды длины p на эти подгруппы. Полученные групповые коды индуцируют коды на всей группе Гейзенберга.

Индуцированные коды на некоммутативных группах позволяют определить новые кодовые криптосистемы, которые по некоторым параметрам могут быть лучше известных [7].

Заключение

В работе для конечной группы Гейзенберга над простым полем Галуа найдены все собственные подгруппы, определено, какие из этих подгрупп являются нормальными, и вычислены соответствующие факторгруппы. На найденных подгруппах группы Гейзенберга можно моделировать индуцированные коды, например, на циклических подгруппах можно моделировать коды Рида-Соломона. Применение индуцированных кодов позволяет переносить эти коды на группу Гейзенберга, что дает возможность строить новые кодовые криптосистемы.

Список цитируемой литературы

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 815 с.
2. Shor P.W. Algorithms for quantum computation: Discrete logarithms and factoring, Proceedings 35th Annual Symposium on Foundations of Computer Science // IEEE Computer Society Press. – 1994. – P. 124-134.
3. Bernstein D.J., Buchmann J., Dahmen E. Post-Quantum Cryptography. – Berlin, Springer, 2009. – 245 p.
4. Deundyak V.M., Kosolapov Yu.V. On the Berger–Loidreau cryptosystem on the tensor product of codes // J. Comp. Eng. Math. – 2018. – Vol. 5, Issue 2. – P. 16–33
5. Сидельников В.М. Открытое шифрование на основе двоичных кодов Рида-Маллера // Дискретная математика. – 1994. – Т.6. – №2. – С. 3-20.
6. Niederreiter H. Knapsack-Type Cryptosystem and Algebraic Coding Theory // Problems of Control and Information Theory. – 1986. – Vol.15. – P. 159-166.
7. Деундяк В.М., Косолапов Ю.В. Криптосистема на индуцированных групповых кодах // Моделирование и анализ информационных систем. – 2016. – Т.23. – №2. – С. 137-152.
8. Деундяк В.М., Косолапов Ю.В., Лелюк Е.А. Декодирование тензорного произведения MLD-кодов и приложения к кодовым криптосистемам // Моделирование и анализ информационных систем. 2017. – Т.24. – №2. – С. 239-252.
9. Веденев К.В., Деундяк В.М. Коды в диэдральной групповой алгебре // Моделирование и анализ информационных систем. – 2018. – Т.25. – №2. – С. 232-245.
10. Веденев К.В., Деундяк В.М. Решетки подгрупп и кодов на диэдральной группе // Известия вузов. Северо-Кавказский регион. Естественные науки. – 2018. – №3. – С. 18-23.
11. Лидл Р., Нидеррайтер Г. Конечные поля. Т.1 – М.: Мир, 1988. – 430 с.
12. Винберг Э.Б. Курс алгебры. – М.: Факториал Пресс, 2001. – 544 с.

13.Циммерман К.-Х. Методы теории модулярных представлений в алгебраической теории кодирования. М.: МЦНМО, 2011. – 246 с.
14.Terras A. Fourier Analysis on Finite Groups and Applications. – Cambridge University Press. Cambridge, 2001. – 442 p.