Math-Net.Ru

Общероссийский математический портал

А. В. Акишин, О группах с автоморфизмами, порождающими рекуррентные последовательности максимального периода, *Дискрет. матем.*, 2014, том 26, выпуск 1, 3–9

DOI: <https://doi.org/10.4213/dm1263>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.84.234.179

26 апреля 2023 г., 10:38:42

О группах с автоморфизмами, порождающими рекуррентные последовательности максимального периода

© 2014 г. А. В. Акишин¹

Пусть G – конечная группа, f – автоморфизм группы G . Тогда автоморфизм f задает рекуррентную последовательность $\{a_i\}$ на группе G , $i = 0, 1, \dots$, если положить $a_{i+1} = f(a_i)$. Если a_0 – начальный элемент последовательности, то ее период не превышает числа элементов порядка, равного порядку a_0 . Таким образом, можно поставить вопрос о существовании групп, у которых такая рекуррентная последовательность при некотором автоморфизме имеет максимальный период для любого начального состояния.

В данной статье вводится понятие автоморфизма максимального периода и находятся все конечные абелевы группы и конечные группы нечетного порядка, обладающие втоморфизмами максимального периода. Доказывается ряд результатов для конечных групп четного порядка.

Ключевые слова: конечные группы, регулярные автоморфизмы, рекуррентные последовательности на группах.

1. Введение

Генераторы псевдослучайных последовательностей используются для решения целого ряда прикладных задач, в частности, в криптографии и кодировании информации. Одним из требований к генераторам псевдослучайных последовательностей является обеспечение большого периода вырабатываемой им последовательности. Широко известным примером генераторов псевдослучайных последовательностей является регистр сдвига с линейной обратной связью, генерирующий линейную рекуррентную последовательность над конечным полем или кольцом [9].

Пусть F – поле, V – n -мерное векторное пространство над полем F . Тогда если f – характеристический многочлен некоторой линейной рекуррентной последовательности степени n над полем F , то сопровождающая матрица A_f многочлена f , если она невырождена, задает автоморфизм векторного пространства V . Однако пространство V можно рассматривать и как абелеву группу, изоморфную прямому произведению n циклических групп. Тогда невырожденная матрица A_f задает автоморфизм этой группы.

¹ Место работы: Московский Государственный Институт Радиотехники, Электроники и Автоматики (МИРЭА)

e-mail: sd45ki91@yandex.ru

Линейные рекуррентные последовательности над полями хорошо изучены, и известны методы построения последовательностей максимального периода. В настоящее время в трудах Нечаева А.А., Кузьмина А.С. [4, 5, 6, 11] и других авторов изучаются линейные и полилинейные рекуррентные последовательности над кольцами.

В связи со сказанным выше имеет смысл рассмотреть более общий случай. Пусть G – конечная группа, f – автоморфизм группы G . Тогда с помощью автоморфизма f можно построить рекуррентную последовательность, положив

$$a_{i+1} = f(a_i), \quad i = 0, 1, \dots,$$

где $a_0 \in G$ – некоторый фиксированный элемент группы G . С точки зрения приложений, важным параметром рекуррентной последовательности является ее период. Поэтому уместно поставить вопрос о возможных периодах такой рекуррентной последовательности и о существовании последовательностей с максимальным периодом.

Следует отметить, что генераторы на группах изучались в целом ряде работ и имеют многочисленные применения. Например, часто используемыми на практике являются конгруэнтные генераторы на кольце вычетов $\mathbb{Z}_n$ – линейные [3] и полиномиальные [8]. Обобщение линейных конгруэнтных генераторов на произвольные группы рассматривалось в работе [15], где описаны все группы G , допускающие транзитивные аффинные преобразования вида $x \mapsto \varphi(x)b$, где $\varphi \in \text{Aut } G$, $b \in G$ – некоторый фиксированный элемент. Развитие аффинных генераторов рассматривалось в работах [12, 13, 14], где изучались группы, допускающие транзитивные преобразования вида

$$x \mapsto a\varphi_1(x)^{n_1}\varphi_2(x)^{n_2} \dots \varphi_k(x)^{n_k}.$$

Так как для любого автоморфизма $f(e) = e$, где e – единица группы G , то максимальный период, равный $|G| - 1$, достигается только в том случае, когда группа $F = \langle f \rangle$ транзитивна на $G \setminus \{e\}$. Полное описание групп, обладающих такими автоморфизмами, дается следующей теоремой. При этом мы будем отождествлять автоморфизм f с соответствующей подстановкой на множестве G .

Теорема 1. *Конечная группа G обладает автоморфизмом f , порождающим транзитивную на $G \setminus \{e\}$ группу подстановок, тогда и только тогда, когда G – элементарная абелева p -группа.*

Доказательство. Если G – элементарная абелева p -группа, то она изоморфна аддитивной группе поля $\mathbb{F}_{p^n}$ при некотором n . Если теперь a – примитивный элемент поля, то отображение $f: x \mapsto ax$ порождает транзитивную на $G \setminus \{e\}$ группу подстановок.

Обратно, пусть у группы G существует автоморфизм f , указанный в теореме. Так как любой автоморфизм сохраняет порядки элементов, то группа $F = \langle f \rangle$ транзитивна на $G \setminus \{e\}$ тогда и только тогда, когда порядок любого неединичного элемента группы G является некоторым простым числом p . В случае $p = 2$ группа G , очевидно, является абелевой. Пусть $p > 2$; обозначим через n такое целое число, что $f^n(a) = a^{-1}$ для некоторого неединичного элемента $a \in G$. Тогда если $b \in G$ – любой другой неединичный элемент и $b = f^k(a)$, то

$$f^n(b) = f^k(f^n(a)) = f^k(a^{-1}) = b^{-1}.$$

Рассмотрим теперь произведение ab . Если $ab = e$, то $b = a^{-1}$ и тогда $ab = ba$. Если же $ab \neq e$, то порядок элемента ab равен p и, следовательно, $f^n(ab) = (ab)^{-1}$. Отсюда получаем

$$b^{-1}a^{-1} = (ab)^{-1} = f^n(ab) = f^n(a)f^n(b) = a^{-1}b^{-1},$$

то есть $ab = ba$. В обоих случаях (как при $p = 2$, так и при $p > 2$) группа G является элементарной абелевой p -группой.

Как видно из теоремы 1, класс групп, обладающих таким автоморфизмом, довольно узок. Поэтому имеет смысл несколько ослабить требования, предъявляемые к цикловой структуре автоморфизма. А именно, автоморфизм $f \in \text{Aut } G$ будем называть автоморфизмом максимального периода, если для любых двух элементов a и b группы G одного порядка существует целое число k такое, что $f^k(a) = b$. Автоморфизмы максимального периода, хотя и не транзитивны на группе G , но, в отличие от, например, аффинных, имеют более простую реализацию. Поэтому они могут быть интересны для различных приложений.

Отметим, что любой автоморфизм максимального периода не имеет неподвижных элементов, за исключением единицы группы, то есть такой автоморфизм является регулярным. Регулярные и близкие к регулярным автоморфизмы достаточно широко изучаются, как пример, можно привести работы [2, 10], но в основном все исследования направлены на определение групп, допускающих регулярный автоморфизм некоторого фиксированного порядка, как правило, простого. В частности, показано, что такие группы являются нильпотентными. Целью данной статьи является описание всех абелевых групп и всех групп нечетного порядка, допускающих автоморфизм максимального периода. Кроме того, доказываются некоторые результаты о строении групп четного порядка.

В дальнейшем порядок элемента a группы G будем обозначать символом $|a|$.

2. Конечные абелевы группы

Начнем с изучения строения конечных абелевых групп, обладающих автоморфизмами максимального периода. При этом будем использовать аддитивную запись операции.

Так как любая абелева группа разлагается в прямую сумму p -групп, то сначала рассмотрим строение конечных абелевых p -групп. Начнем со следующего предложения.

Предложение 1. *В любом разложении p -группы A в прямую сумму циклических групп все прямые слагаемые изоморфны.*

Доказательство. Действительно, пусть $A = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \dots \oplus \langle a_n \rangle$ – разложение p -группы A в прямую сумму циклических групп. Докажем, что порядки образующих $a_1, a_2, \dots, a_n$ равны.

Предположим, что для некоторых i и j , $|a_i| = p^t$, $|a_j| = p^s$ и пусть $s < t$. Тогда элемент $p^{t-s}a_i$ имеет тот же порядок, что и a_j , и, следовательно, существует такое n , что $a_j = f^n(p^{t-s}a_i)$. Обозначив $b = f^n(a_i)$ мы получим, что a_j лежит в циклической группе $\langle b \rangle$ порядка p^t . Но тогда группа $\langle a_j \rangle$ не может выделяться прямым слагаемым. Полученное противоречие доказывает предложение.

Из предложения 1 следует, что класс абелевых p -групп, обладающих автоморфизмами максимального периода, с точностью до изоморфизма состоит из абелевых групп типа $C_{p^n}^m$, где n, m – некоторые натуральные числа, а через C_k обозначена циклическая группа порядка k . Приведем теперь полное описание всех конечных абелевых p -групп, обладающих автоморфизмами максимального периода.

Теорема 2. *Конечная p -группа G обладает автоморфизмами максимального периода тогда и только тогда, когда она изоморфна одной из следующих групп:*

- 1) C_p^m ,
- 2) C_{p^n} , $p \neq 2$,
- 3) C_4 .

Доказательство. В соответствии с предложением 1 группа G изоморфна группе $C_{p^n}^m$ при некоторых натуральных n и m . Так как при $n = 1$ группа C_p^m является элементарной абелевой группой, то, по теореме 1, она обладает автоморфизмами максимального периода. Осталось рассмотреть случай, когда $n > 1$.

Для начала пусть $G \simeq C_{p^2}^m$ и $m > 1$. В соответствии с [7], любой автоморфизм группы G , в частности, и автоморфизм f , можно представить в виде невырожденной матрицы $F = (f_{ij})$, где $f_{ij} \in \mathbb{Z}_{p^2}$. Так как группа G содержит $p^m - 1$ элементов порядка p , то для матрицы F автоморфизма максимального периода f должно выполняться равенство

$$F^{p^m-1} \equiv E \pmod{p},$$

то есть $F^{p^m-1} = E + p(g_{ij})$, где $g_{ij} \in \mathbb{Z}_{p^2}$. Отсюда следует, что $F^{p(p^m-1)} = E$, то есть порядок автоморфизма f является делителем числа $p(p^m - 1)$.

Подсчитаем теперь число N элементов порядка p^2 в группе $C_{p^2}^m$. Из равенства

$$p^{2m} = 1 + (p^m - 1) + N$$

следует, что

$$N = p^{2m} - p^m = p^m(p^m - 1) > p(p^m - 1).$$

Случай $n > 2$ легко сводится к рассмотренному. Действительно, если $G \simeq C_{p^n}^m$ и $n > 2$, то все элементы порядка не выше p^2 образуют подгруппу, изоморфную группе $C_{p^2}^m$. Но тогда, как доказано выше, у группы G не может существовать автоморфизмов максимального периода.

Осталось показать, что на группе C_{p^n} существуют автоморфизмы максимального периода только в том случае, когда $p \neq 2$ при любом n , $p = 2$ и $n = 1$ или $n = 2$.

Действительно, группа C_{p^n} изоморфна аддитивной группе кольца $\mathbb{Z}_{p^n}$. Любой автоморфизм этой аддитивной группы имеет вид $x \mapsto ax$ для некоторого $a \in \mathbb{Z}_{p^n}$, взаимно простого с p . Следовательно, автоморфизмы максимального периода существуют тогда и только тогда, когда мультипликативная группа $\mathbb{Z}_{p^n}^*$ циклическая. Как известно [1], группа $\mathbb{Z}_{p^n}^*$ – циклическая только в следующих случаях: $p > 2$ при любом n , $p = 2$ и $n = 1$ или $n = 2$. Отсюда получаем утверждение теоремы.

Теперь мы можем дать описание всех абелевых групп, обладающих автоморфизмами максимального периода.

Теорема 3. *Абелева группа G обладает автоморфизмами максимального периода тогда и только тогда, когда она изоморфна одной из следующих групп:*

- 1) C_p^n , p – простое число,

- 2) C_4 ,
- 3) C_{p^n} , p – простое число, $p \neq 2$,
- 4) $C_2^n \oplus C_p^m$, p – простое число, $p \neq 2$ и $(2^n - 1, p^m - 1) = 1$,
- 5) $C_2^n \oplus C_{p^m}$, p – простое число, $p \neq 2$ и $(2^n - 1, p^{m-1}(p - 1)) = 1$.

Доказательство. Пусть G – абелева группа и пусть

$$G = \sum_p G_p \quad (1)$$

– разложение группы G в прямую сумму p -групп, где сумма берется по всем простым числам p , делящим порядок группы G . Если f – автоморфизм группы G , то он на каждом прямом слагаемом G_p индуцирует автоморфизм f_p , причем, если f – автоморфизм максимального периода, то и каждый автоморфизм f_p также является автоморфизмом максимального периода на группе G_p . Описание всех абелевых p -групп, обладающих автоморфизмами максимального периода, получено в теореме 2.

Итак, предположим сначала, что в прямую сумму (1) входят две группы G_p и G_q , где p и q – нечетные простые числа. Рассмотрим четыре варианта

- 1) $G_p \simeq C_p^n$, $G_q \simeq C_q^m$, $|f_p| = p^n - 1$, $|f_q| = p^m - 1$,
- 2) $G_p \simeq C_p^n$, $G_q \simeq C_q^m$, $|f_p| = p^n - 1$, $|f_q| = q^{m-1}(q - 1)$,
- 3) $G_p \simeq C_{p^n}$, $G_q \simeq C_q^m$, $|f_p| = p^{n-1}(p - 1)$, $|f_q| = q^m - 1$,
- 4) $G_p \simeq C_{p^n}$, $G_q \simeq C_q^m$, $|f_p| = p^{n-1}(p - 1)$, $|f_q| = q^{m-1}(q - 1)$.

Во всех возможных вариантах порядки автоморфизмов f_p и f_q не являются взаимно простыми, следовательно, автоморфизм f не может быть автоморфизмом максимального периода. Нам осталось рассмотреть следующие четыре случая:

- 1) $C_2^n \oplus C_p^m$, $|f_2| = 2^n - 1$, $|f_p| = p^m - 1$,
- 2) $C_2^n \oplus C_{p^m}$, $|f_2| = 2^n - 1$, $|f_p| = p^{m-1}(p - 1)$,
- 3) $C_4 \oplus C_p^m$, $|f_2| = 2$, $|f_p| = p^m - 1$,
- 4) $C_4 \oplus C_{p^m}$, $|f_2| = 2$, $|f_p| = p^{m-1}(p - 1)$.

Как и выше, в последних двух случаях порядки автоморфизмов f_2 и f_p имеют общий делитель, следовательно, эти два случая невозможны. Первые же два варианта возможны только в том случае, когда $(2^n - 1, p^m - 1) = 1$ и $(2^n - 1, p^{m-1}(p - 1)) = 1$ соответственно. Это завершает доказательство теоремы.

3. Неабелевы группы

Перейдем теперь к некоммутативным группам, причем сначала рассмотрим группы нечетного порядка. Здесь имеет место следующая теорема.

Теорема 4. *Если G – конечная группа нечетного порядка с автоморфизмом максимального периода, то она абелева.*

Доказательство. Пусть a и b – любые два элемента группы G , f – автоморфизм максимального периода. Справедливо равенство $|a| = |a^{-1}|$. Пусть n и m – такие целые числа, что

$$f^n(a) = a^{-1}, \quad f^m(b) = b^{-1}.$$

Положим $d = [n, m]$ – наименьшее общее кратное чисел n и m . Тогда, положив

$$d = nd_1 = md_2,$$

получим

$$\begin{aligned} f^d(a) &= f^{nd_1}(a) = a^{(-1)^{d_1}}, \\ f^d(b) &= f^{md_2}(b) = b^{(-1)^{d_2}}. \end{aligned}$$

Так как d – наименьшее общее кратное, то числа d_1 и d_2 не могут быть четными одновременно. Без ограничения общности предположим, что d_1 нечетное и, заметив, что $|b| = |aba^{-1}|$, рассмотрим два случая:

1) $f^d(a) = a^{-1}$, $f^d(b) = b^{-1}$. При этом имеем

$$ab^{-1}a^{-1} = (aba^{-1})^{-1} = f^d(aba^{-1}) = a^{-1}b^{-1}a,$$

откуда следует, что $a^2b^{-1} = b^{-1}a^2$ и, так как a – элемент нечетного порядка, то $\langle a \rangle = \langle a^2 \rangle$ и, следовательно, $ab = ba$.

2) $f^d(a) = a^{-1}$, $f^d(b) = b$. В этом случае имеем

$$aba^{-1} = f^d(aba^{-1}) = a^{-1}ba,$$

откуда следует, что $a^2b = ba^2$ и, как и ранее, $ab = ba$.

Отметим, что aba^{-1} и b имеют один и тот же порядок и, следовательно, лежат на одном цикле автоморфизма f .

Итак, во всех случаях оказалось, что $ab = ba$, то есть группа действительно G является абелевой.

Как показывает теорема 4, любая группа нечетного порядка, обладающая автоморфизмом максимального периода, является абелевой. Все такие группы описаны в теореме 3 и являются группами типа C_p^n или C_{p^n} для некоторого простого $p > 2$ и натурального n .

Рассмотрим теперь группы четного порядка. Сначала докажем следующее утверждение.

Предложение 2. Пусть G – конечная группа четного порядка, f – автоморфизм группы G максимального периода. Тогда множество H всех элементов нечетного порядка группы G является абелевой нормальной подгруппой, допустимой относительно автоморфизма f .

Доказательство. Доказательство того, что H является абелевой подгруппой, практически дословно повторяет рассуждения, приведенные в доказательстве теоремы 4. Действительно, рассматривая любые два элемента из множества H мы можем показать, что они перестановочны. Но это и означает, что H – абелева подгруппа.

Так как при сопряжении порядки элементов не меняются, то подгруппа H является нормальной. Наконец, то, что H допустима относительно автоморфизма f , следует из того, что автоморфизм f также сохраняет порядки элементов.

Следствие 1. Порядок группы четного порядка, обладающей автоморфизмами максимального периода, равен $2^n p^m$, где $p > 2$ – простое число, n и m – некоторые натуральные числа, а ее силовская p -подгруппа нормальна.

В заключение, используя предложение 2, докажем следующее утверждение.

Предложение 3. Пусть G – группа с автоморфизмом максимального периода, $|G| = 2p^t$ и силовская p -подгруппа группы G циклическая. Тогда $G \simeq C_2 \oplus C_{p^t}$.

Доказательство. Обозначим силовскую p -подгруппу через G_p . Пусть $a \in G$ – элемент порядка 2, $b \in G_p$ – произвольный порождающий элемент. Тогда либо $ab = ba$ и группа G абелева, либо $aba^{-1} = b^{-1}$. Покажем, что второй случай невозможен, откуда и будет следовать справедливость леммы.

Предположим, что f – автоморфизм максимального периода. Заметим, что для любого натурального n выполняется равенство $(ab^n)^2 = e$, то есть группа G содержит p^t элементов второго порядка. Пусть $f(a) = ab^r$ и $f(b) = b^s$ для некоторых натуральных r и s . Так как f – автоморфизм, то b^s также является порождающим группы G_p , то есть s является порождающим мультипликативной группы $\mathbb{Z}_{p^t}^*$, откуда следует, что $s^{\varphi(p^t)} \equiv 1 \pmod{p^t}$ и $(s-1, p) = 1$. Легко проверить, что

$$f^n(a) = ab^{r(1+s+\dots+s^{n-1})} = ab^{r \frac{s^n-1}{s-1}}.$$

В частности, при $n = \varphi(p^t)$ мы получим $f^n(a) = a$, то есть не все элементы порядка 2 лежат на одном цикле автоморфизма f . Это противоречит тому, что f является автоморфизмом максимального периода.

Список литературы

1. Виноградов М.И., *Основы теории чисел*. Лань, Санкт-Петербург, 2006.
2. Глухов М.М., Ларин С.В., Абелевы и метабе́левы группы с регулярными автоморфизмами и полуавтоморфизмами. *Матем. заметки* (1972) **12**, №6, 727–738.
3. Кнут Д., *Искусство программирования. Том 2. Получисленные алгоритмы*. "Вильямс", Москва, 2001.
4. Кузьмин А.С., Нечаев А.А., Линейные рекуррентные последовательности над кольцами Галуа. *Успехи матем. наук* (1993) **48**, №1, 167–168.
5. Кузьмин А.С., Куракин В.Л., Нечаев А.А., Псевдослучайные и полилинейные последовательности. *Труды по дискретной математике* (1997) **1**, 139–202.
6. Кузьмин А.С., Маршалко Г.Б., Нечаев А.А., Восстановление линейной рекурренты над примарным кольцом вычетов по ее усложнению. *Математические вопросы криптографии* (2010) **1**, №2, 31–56.
7. Курош А.Г., *Теория групп*. Лань, Санкт-Петербург, 2005.
8. Ларин М.В., Транзитивные полиномиальные преобразования колец вычетов. *Дискретная математика* (2002) **14**, №2, 20–32.
9. Лидл Р., Нидеррайтер Г., *Конечные поля*, **1**, **2**. Мир, Москва, 1988.
10. Макаренко М.Ю., Хухро Е.И., Конечные группы с почти регулярным автоморфизмом порядка четыре. *Алгебра и логика* (2006) **45**, №5, 575–602.
11. Нечаев А.А., Линейные рекуррентные последовательности над коммутативными кольцами. *Дискретная математика* (1991) **3**, №4, 105–127.
12. Anashin V.S., Uniformly distributed sequences in computer algebra, or how to construct program generators of random numbers. *J. Math. Sci.* (1998) **89**, №4, 1355–1390.
13. Anashin V.S., Noncommutative algebraic dynamics: ergodic theory for profinite groups. *Труды МИАН* (2009) **256**, 36–65.
14. Anashin V., Khrennikov A., Applied Algebraic Dynamics. *de Gruyter Expositions in Mathematics* (2009) **49**.
15. Jonah D., Schreiber B.M., Transitive affine transformations on groups. *Pacific J. Math* (1975) **58**, №2, 483–509.