М. И. Анохин, Группы автоморфизмов некоторых кодов, *Дискрет. матем.*, 2012, том 24, выпуск 1, 48–59

DOI: 10.4213/dm1171

Дискретная математика

том 24 выпуск 1 * 2012

УДК 519.725

Группы автоморфизмов некоторых кодов

© 2012 г. М. И. Анохин

В работе даются некоторые описания группы автоморфизмов, группы мономиальных автоморфизмов и группы перестановочных автоморфизмов произвольного кода вида $\{\rho\lambda \mid \lambda \in V^*\}$, где ρ есть отображение из конечного множества X в векторное пространство V, порожденное множеством $X\rho$, а V^* есть сопряженное пространство для V. Полученные общие результаты применяются к некоторым важным частным случаям.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 07–01–00154.

1. Введение

Группы автоморфизмов кодов являются классическими объектами изучения в теории кодирования. Автоморфизмы кода могут быть использованы, в частности, для построения алгоритмов декодирования (см., например, §8 в [1]). В [1] можно также найти обзор результатов, относящихся к группам автоморфизмов кодов.

Пусть F — поле и X — конечное множество. В настоящей работе под кодами мы понимаем подпространства векторного пространства F^X всех отображений из X в F. Обычно в теории кодирования (линейными) кодами считают подпространства векторного пространства всех последовательностей некоторой конечной длины n с элементами из поля F. Такие последовательности естественно отождествляются с отображениями из $\{1, \ldots, n\}$ в F. Наоборот, если $x_1, \ldots, x_n$ (где $n = |X|$) — все элементы множества X, перечисленные в каком-либо порядке, то отображение $\varphi\colon X \to F$ может быть отождествлено с последовательностью $(x_1\varphi, \ldots, x_n\varphi)$. В частности, длина кода, содержащегося в F^X, равна $|X|$. Указанные отождествления сохраняют операции векторных пространств и расстояние Хемминга. Поэтому наш подход эквивалентен традиционному. Кроме того, использование отображений из неупорядоченного множества X в F вместо последовательностей над F позволяет абстрагироваться от порядка перечисления координат кодовых векторов. Этот порядок не имеет значения для теории кодирования, так как перестановка координат кодовых векторов приводит к эквивалентному коду.

Наиболее общие результаты работы собраны в разделе 3 и заключаются в следующем. Пусть C есть код вида $\{\rho\lambda \mid \lambda \in V^*\}$, где ρ есть отображение из X в некоторое векторное пространство V над F, а ${}^*V$ есть сопряженное пространство для V. Мы предполагаем, что множество $X\rho$ порождает пространство V. Теорема 1 дает некоторые описания группы автоморфизмов $\mathrm{Aut}(C)$, группы мономиальных автоморфизмов $\mathrm{MAut}(C)$ и группы перестановочных автоморфизмов $\mathrm{PAut}(C)$ кода C. Для видов групп автоморфизмов мы используем терминологию и обозначения из [1]. Эти три вида групп автоморфизмов выбраны для описания также по аналогии с [1] (очевидно, что из описания $\mathrm{Aut}(C)$ вытекает

описание $\mathrm{MAut}(C)$, а из описания $\mathrm{MAut}(C)$ — описание $\mathrm{PAut}(C)$). Теорема 2, доказательство которой существенно основано на теореме 1, утверждает, что если прообразы всех элементов из $X\rho$ относительно ρ равномощны, то t-группа $(X, \mathrm{PAut}(C))$ подобна сплетению некоторых t- групп.

В последующих разделах результаты раздела 3 применяются к некоторым важным частным случаям. Раздел 4 посвящен кодам, являющимся циклическими GF-подмодулями F^G, где G — конечная группа, а GF — ее групповая алгебра над F. По существу, такие коды (без условия модульной цикличности и над конечным полем F) впервые рассматривались С. Д. Берманом [2, 3] под названием GF-кодов. В разделе 5 рассматриваются классы кодов, содержащие важные частные случаи кодов из раздела 4 (когда G — циклическая группа конечного порядка, не делящегося на характеристику поля F), расширенные циклические коды в смысле [1], подраздел 3.1], и коды, рассматриваемые О. А. Логачевым, А. А. Сальниковым и В. В. Ященко. Наконец, в разделе 6 найдены пересечения групп перестановочных автоморфизмов некоторых из кодов, рассматриваемых в разделе 5. Этим доказывается одно предположение, высказанное В. В. Ященко (подробнее см. раздел 6).

Автор благодарит В. В. Ященко, который направил его усилия на изучение объектов настоящей работы. Автор признателен О. А. Логачеву, А. А. Сальникову и В. В. Ященко, а также руководителям и участникам семинара “Кольца и модули” кафедры высшей алгебры механико-математического факультета МГУ за полезные обсуждения данной работы.

2. Определения, обозначения и необходимые факты

Пусть X, Y и Z — некоторые множества. Через Y^X будет обозначаться множество всех отображений из X в Y. Для отображений в работе используется правосторонняя запись, то есть значение отображения $\varphi \in Y^X$ на элементе $x \in X$ записывается в виде $x\varphi$, а не $\varphi(x)$. Композицию отображений $\varphi \in Y^X$ и $\psi \in Z^Y$ (в этом порядке) мы будем обозначать через $\varphi\psi$ (то есть $x(\varphi\psi) = (x\varphi)\psi$ для любого $x \in X$). Символ id_X обозначает тождественное отображение множества X. Через $\mathcal{S}_X$ обозначается симметрическая группа на множестве X (то есть группа всех перестановок этого множества); мы считаем, что $\mathcal{S}_X$ действует на X справа. Если X_0 — подмножество X и P — подгруппа $\mathcal{S}_X$, то через $P|_{X_0}$ мы будем обозначать подгруппу группы $\mathcal{S}_{X_0}$, состоящую из всех перестановок вида $\pi|_{X_0}$, где π пробегает всевозможные перестановки из P такие, что $X_0\pi = X_0$.

Напомним некоторые определения, касающиеся t-групп. Если X — множество и P — подгруппа $\mathcal{S}_X$, то пара (X, P) называется t-группой. Две t-группы (X, P) и (Y, Q) подобны, если существует биективное отображение $\delta \in Y^X$, удовлетворяющее равенству $\{\delta^{-1}\pi\delta \mid \pi \in P\} = Q$. Под сплетением $(X, P) \wr (Y, Q)$ t-групп (X, P) и (Y, Q) понимается t- группа $(X \times Y, T)$, где T состоит из всех перестановок вида $(x, y) \mapsto (x\pi_y, y\sigma)$, $x \in X$, $y \in Y$, в которых $\{\pi_y \mid y \in Y\}$ — семейство перестановок из P и σ — перестановка из Q.

Если R — ассоциативное кольцо с 1, то $R^\times$ обозначает группу обратимых элементов кольца R, а нуль кольца R в нулевой степени считается равным 1. Для целого положительного числа n через $\mathbf{Z}_n$ мы будем обозначать множество $\{0, \ldots, n-1\}$. Это множество будет иногда рассматриваться как кольцо относительно операций сложения и умножения по модулю n. Через $m \bmod n$ обозначается остаток от деления целого числа m на целое положительное число n.

На протяжении всей работы через F будет обозначаться некоторое поле. Все объекты и понятия линейной алгебры рассматриваются над основным полем F, если не оговорено противное. Пусть V и W — векторные пространства. Напомним, что отображение $\xi \in W^V$

называется α-полулинейным (где α — автоморфизм поля F), если $(v_1 + v_2)\xi = v_1\xi + v_2\xi$ и $(vf)\xi = (v\xi)(f\alpha)$ для всех $v_1, v_2, v \in V$ и $f \in F$. Отображение $\xi \in W^V$ называется полулинейным, если оно α-полулинейно для некоторого автоморфизма α поля F. Сопряженное пространство для V (то есть векторное пространство всех линейных отображений из V в F) мы обозначаем, как обычно, через V^*. Если U — подмножество V, то $< U >$ обозначает подпространство, порожденное множеством U. Через $GL(V)$ будет обозначаться полная линейная группа пространства V, то есть группа всех биективных линейных отображений из V^V. Для $\varphi \in F^X$ ($\varphi \in V^X$) и $\psi \in F^X$, где X — некоторое множество, через $\varphi \cdot \psi$ мы обозначаем отображение из F^X (соответственно, V^X), заданное равенством $x(\varphi \cdot \psi) = (x\varphi)(x\psi)$ для произвольного $x \in X$. Другими словами, $\varphi \cdot \psi$ является поточечным произведением φ и ψ. Если K — поле, являющееся конечным расширением поля F, то $\mathrm{Tr}_K(z)$ обозначает след элемента $z \in K$ относительно подполя F. Хорошо известно, что если F конечно, $|F| = q$ и $|K| = q^n$, то

$$\mathrm{Tr}_K(z) = \sum_{i=0}^{n-1} z^{q^i}$$

для всех $z \in K$. Через GF будет обозначаться групповая алгебра группы G над полем F.

Пусть X — конечное множество. Тогда F^X является конечномерным векторным пространством относительно поточечных операций сложения и умножения на элементы из F, а также метрическим пространством относительно расстояния Хемминга (напомним, что расстояние Хемминга между отображениями φ и ψ из F^X равно $|\{x \in X \mid x\varphi \neq x\psi\}|$). Хорошо известно, что если α — автоморфизм поля F, то α-полулинейные изометрические отображения F^X на себя — это в точности отображения вида

$$\varphi \mapsto \sigma(\varphi \cdot \mu)\alpha, \tag{1}$$

где $\mu \in (F^\times)^X$ и $\sigma \in \mathcal{S}_X$. Отображение (1) мы будем обозначать через $[\mu\sigma\alpha]$. В частности, линейные изометрические отображения F^X на себя — это в точности отображения вида $[\mu\sigma\mathrm{id}_F]$. Такие отображения называются мономиальными. Вместо $[\mu\sigma\mathrm{id}_F]$ мы будем писать $[\mu\sigma]$. Очевидно, что если X непусто, то μ, σ и α определяются отображением $[\mu\sigma\alpha]$ однозначно.

Кодом называется всякое подпространство пространства F^X. Пусть C — некоторый такой код. Тогда полулинейное изометрическое (и, следовательно, биективное) отображение $\beta\colon F^X \to F^X$ называется автоморфизмом кода C, если $C\beta = C$ (или, что эквивалентно, $C\beta \subseteq C$). Множество всех линейных автоморфизмов кода C совпадает с множеством всех мономиальных автоморфизмов этого кода. Перестановочный автоморфизм кода C — это произвольная перестановка $\sigma \in \mathcal{S}_X$ такая, что $\sigma\varphi \in C$ для всех $\varphi \in C$. Множества всех автоморфизмов, мономиальных автоморфизмов и перестановочных автоморфизмов кода C обозначаются через $\mathrm{Aut}(C)$, $\mathrm{MAut}(C)$ и $\mathrm{PAut}(C)$ соответственно. Очевидно, что эти множества являются группами относительно операции композиции.

Иногда под автоморфизмом кода C понимается произвольное полулинейное изометрическое отображение этого кода на себя. Однако если поле F конечно (именно этот случай наиболее важен для теории кодирования), то автоморфизмы кода C в смысле второго определения — это в точности ограничения на C автоморфизмов этого кода в смысле первого определения. Действительно, ограничение на C всякого автоморфизма этого кода в смысле первого определения, очевидно, является автоморфизмом кода C в смысле второго определения. Обратное утверждение является частным случаем следующего предложения, которое обобщает известную теорему Маквильямс о продолжении [4]

на полулинейные изометрические отображения. Возможно, что это предложение известно в теории кодирования, но автору не удалось найти ссылок на него.

Предложение 1. *Предположим, что поле F конечно. Пусть $\beta: V \to F^X$ есть α-полулинейная изометрия, где V есть подпространство векторного пространства F^X, а α есть автоморфизм поля F. Тогда β продолжается до α-полулинейной изометрии F^X на себя.*

Доказательство. Определим отображение из $(F^X)^V$ формулой $\varphi \mapsto (\varphi\beta)\alpha^{-1}$, $\varphi \in V$. Ясно, что это отображение линейно и изометрично. Поэтому ввиду теоремы Маквильямс о продолжении [4] оно продолжается до линейной изометрии $\gamma: F^X \to F^X$. Тогда $\varphi \mapsto (\varphi\gamma)\alpha$ ($\varphi \in F^X$) — искомое продолжение отображения β до α-полулинейной изометрии F^X на себя.

3. Общие результаты

В настоящем разделе через X будет обозначаться некоторое конечное множество, через V — векторное пространство, а через ρ — такое отображение из V^X, что $\langle X\rho\rangle = V$. В частности, V конечномерно. Мы будем пользоваться тем, что

$$v_1\lambda = v_2\lambda \text{ для всех } \lambda \in V^* \implies v_1 = v_2 \quad (v_1, v_2 \in V). \tag{2}$$

Обозначим также через C код $\{\rho\lambda \mid \lambda \in V^*\}$.

Теорема 1. *Пусть $\mu \in (F^\times)^X$, $\sigma \in \mathcal{S}_X$ и α — автоморфизм поля F. Тогда*

(i) $[\mu;\sigma,\alpha] \in \mathrm{Aut}(C)$*, если и только если существует α^{-1}-полулинейное отображение $\xi \in V^V$, удовлетворяющее равенству*

$$\rho\xi = \sigma(\rho \cdot \mu); \tag{3}$$

(ii) $[\mu;\sigma] \in \mathrm{MAut}(C)$*, если и только если существует линейное отображение $\xi \in V^V$, удовлетворяющее равенству* (3)*;*

(iii) $\sigma \in \mathrm{PAut}(C)$*, если и только если существует линейное отображение $\xi \in V^V$, удовлетворяющее равенству*

$$\rho\xi = \sigma\rho.$$

Кроме того, если такое отображение ξ существует, то оно единственно и биективно.

Доказательство. Достаточно доказать только часть (i), так как часть (ii) является частным случаем части (i) (если положить $\alpha = \mathrm{id}_F$), а часть (iii) — частным случаем части (ii) (если положить $x\mu = 1$ для всех $x \in X$). Пусть сначала $[\mu;\sigma,\alpha] \in \mathrm{Aut}(C)$. Поставим в соответствие каждому отображению $\lambda \in V^*$ отображение $\lambda' \in V^*$, удовлетворяющее равенству $(\rho\lambda)[\mu;\sigma,\alpha] = \rho\lambda'$ (очевидно, что такое отображение λ' существует и единственно). Тогда

$$\sigma(\rho \cdot \mu)\lambda\alpha = \sigma((\rho\lambda) \cdot \mu)\alpha = (\rho\lambda)[\mu;\sigma,\alpha] = \rho\lambda' \tag{4}$$

для всех $\lambda \in V^*$, так как любое отображение $\lambda \in V^*$ линейно. Из равенства (4) и импликации (2) вытекает импликация

$$x_1\rho = x_2\rho \implies x_1\sigma(\rho\cdot\mu) = x_2\sigma(\rho\cdot\mu)$$

для произвольных $x_1, x_2 \in X$. Поэтому существует отображение $\xi_0 \in V^{X\rho}$, удовлетворяющее равенству

$$\rho\xi_0 = \sigma(\rho\cdot\mu). \tag{5}$$

Из равенств (5) и (4) следует, что

$$u\xi_0\lambda\alpha = u\lambda'$$

для всех $u \in X\rho$ и $\lambda \in V^*$. Последнее равенство и импликация (2) дают импликацию

$$\sum_{u\in X\rho} u(u\psi_1) = \sum_{u\in X\rho} u(u\psi_2) \implies \sum_{u\in X\rho} (u\xi_0)(u\psi_1\alpha^{-1}) = \sum_{u\in X\rho} (u\xi_0)(u\psi_2\alpha^{-1})$$

для любых $\psi_1, \psi_2 \in F^{X\rho}$. Из этой импликации следует, что отображение ξ, заданное формулой

$$\left(\sum_{u\in X\rho} u(u\psi)\right)\xi = \sum_{u\in X\rho} (u\xi_0)(u\psi\alpha^{-1}), \qquad \psi \in F^{X\rho},$$

корректно определено на $\langle X\rho\rangle = V$. Легко видеть, что ξ является α^{-1}- полулинейным и $\xi|_{X\rho} = \xi_0$. Из последнего равенства и равенства (5) вытекает равенство (3). Таким образом, ξ удовлетворяет условиям утверждения (i).

Предположим теперь, что отображение ξ удовлетворяет условиям утверждения (i). Пусть $\rho\lambda$, где $\lambda \in V^*$, — произвольное отображение из кода C. Тогда

$$(\rho\lambda)[\mu;\sigma,\alpha] = \sigma((\rho\lambda)\cdot\mu)\alpha = \sigma(\rho\cdot\mu)\lambda\alpha = \rho\xi\lambda\alpha$$

ввиду линейности отображения λ и равенства (3). Здесь $\xi\lambda\alpha \in V^*$, так как ξ α^{-1}-полулинейно, а λ линейно. Поэтому $C[\mu;\sigma,\alpha] \subseteq C$ и $[\mu;\sigma,\alpha] \in \mathrm{Aut}(C)$. Из α^{-1}-полулинейности ξ и равенства (3) вытекает равенство

$$\begin{aligned}\left(\sum_{x\in X} x\rho\left(\left(\frac{x\sigma\varphi}{x\sigma\mu}\right)\alpha\right)\right)\xi &= \sum_{x\in X} x\rho\xi\frac{x\sigma\varphi}{x\sigma\mu} = \sum_{x\in X}(x\sigma\rho)(x\sigma\varphi)\\ &= \sum_{x\in X}(x\rho)(x\varphi), \qquad \varphi \in F^X.\end{aligned}$$

которое вместе с равенством $\langle X\rho\rangle = V$ показывает, что отображение ξ сюръективно и, следовательно, биективно. Очевидно, что значения ξ на $X\rho$ однозначно определяются из равенства (3), а значения ξ на V однозначно определяются его значениями на $X\rho$ ввиду полулинейности ξ и равенства $\langle X\rho\rangle = V$. Поэтому отображение ξ единственно.

Теорема 2. *Пусть $|\{x \in X \mid x\rho = u\}| = m$ для каждого $u \in X\rho$, где число m не зависит от u, а Y — какое-либо множество из m элементов. Тогда t-группы $(X, \mathrm{PAut}(C))$ и $(Y, \mathcal{S}_Y) \wr (X\rho, GL(V)|_{X\rho})$ подобны.*

Доказательство. Выберем какое-либо отображение $\tau \in Y^X$ такое, что отображение δ, переводящее произвольный элемент $x \in X$ в $(x\tau, x\rho)$, является биекцией X на $Y \times X\rho$. Легко видеть, что

$$(y, z)\delta^{-1}\rho = z \tag{6}$$

для любых $y \in Y$ и $z \in X\rho$. Обозначим через T множество всех перестановок (множества $Y \times X\rho$) вида $(y, z) \mapsto (y\pi_z, z\xi|_{X\rho})$, $y \in Y$, $z \in X\rho$, где $\{\pi_z \mid z \in X\rho\}$ — семейство перестановок из $\mathcal{S}_Y$, а ξ — такое отображение из $GL(V)$, что $X\rho\xi = X\rho$. Докажем, что $\{\delta^{-1}\sigma\delta \mid \sigma \in \mathrm{PAut}(C)\} = T$.

Пусть $\sigma \in \mathrm{PAut}(C)$. Обозначим через ξ отображение из $GL(V)$, удовлетворяющее равенству

$$\rho\xi = \sigma\rho \tag{7}$$

(согласно части (iii) теоремы 1, такое отображение ξ существует и единственно). Из равенства (7) вытекает, что $X\rho\xi = X\rho$. Для каждого $z \in X\rho$ определим отображение $\pi_z \in Y^Y$ равенством

$$y\pi_z = (y, z)\delta^{-1}\sigma\tau, \qquad y \in Y.$$

Если $y_1\pi_z = y_2\pi_z$ для некоторых $y_1, y_2 \in Y$ и $z \in X\rho$, то

$$\begin{aligned}&(y_1, z)\delta^{-1}\sigma\tau = (y_2, z)\delta^{-1}\sigma\tau,\\ &(y_1, z)\delta^{-1}\sigma\rho = (y_1, z)\delta^{-1}\rho\xi = z\xi = (y_2, z)\delta^{-1}\rho\xi = (y_2, z)\delta^{-1}\sigma\rho\end{aligned}$$

ввиду равенства (7) и формулы (6). Поэтому

$$(y_1, z)\delta^{-1}\sigma\delta = (y_2, z)\delta^{-1}\sigma\delta,$$

и $y_1 = y_2$. Это показывает, что отображение π_z инъективно и, следовательно, $\pi_z \in \mathcal{S}_Y$ для любого $z \in X\rho$. Кроме того,

$$\begin{aligned}(y, z)\delta^{-1}\sigma\delta &= ((y, z)\delta^{-1}\sigma\tau, (y, z)\delta^{-1}\sigma\rho)\\ &= (y\pi_z, (y, z)\delta^{-1}\rho\xi) = (y\pi_z, z\xi) = (y\pi_z, z\xi|_{X\rho})\end{aligned}$$

для любых $y \in Y$ и $z \in X\rho$ ввиду равенства (7) и формулы (6). Таким образом, справедливо включение $\{\delta^{-1}\sigma\delta \mid \sigma \in \mathrm{PAut}(C)\} \subseteq T$.

Предположим теперь, что $\{\pi_z \mid z \in X\rho\}$ — семейство перестановок из $\mathcal{S}_Y$, а ξ — такое отображение из $GL(V)$, что $X\rho\xi = X\rho$. Определим перестановку $\sigma \in \mathcal{S}_X$ равенством

$$x\sigma = (y\pi_z, z\xi)\delta^{-1}, \quad x \in X, \quad (y, z) = x\delta.$$

Тогда

$$x\sigma\rho = (y\pi_z, z\xi)\delta^{-1}\rho = z\xi = x\rho\xi$$

для любого $x \in X$, где $(y, z) = x\delta$, ввиду формулы (6). Поэтому $\sigma \in \mathrm{PAut}(C)$ согласно части (iii) теоремы 1. Очевидно также, что

$$(y, z)\delta^{-1}\sigma\delta = (y\pi_z, z\xi) = (y\pi_z, z\xi|_{X\rho})$$

для любых $y \in Y$ и $z \in X\rho$.

Таким образом, справедливо включение $T \subseteq \{\delta^{-1}\sigma\delta \mid \sigma \in \mathrm{PAut}(C)\}$.

4. Коды, являющиеся циклическими подмодулями F^G, где G — конечная группа

В настоящем разделе роль множества X из раздела 3 будет играть некоторая конечная группа G. Мы рассматриваем векторное пространство F^G как правый GF-модуль, в котором $x(\varphi g) = (xg^{-1})\varphi$ для всех $x, g \in G$ и $\varphi \in F^G$. Очевидно, что отображение

$$\varphi \mapsto \widehat{\varphi} = \sum_{x \in G} x(x\varphi), \qquad \varphi \in F^G, \tag{8}$$

является изоморфизмом F^G на GF как правых GF-модулей. Целью настоящего раздела является применение результатов раздела 3 к кодам, являющимся циклическими GF-подмодулями F^G. Этим кодам при изоморфизме (8) соответствуют главные правые идеалы алгебры GF. Очевидно, что если характеристика поля F не делит $|G|$, то любой GF-подмодуль F^G является циклическим, так как любой правый идеал GF является главным.

Пусть $\omega \in F^G$. Применим результаты раздела 3 к коду $\omega(GF)$. В качестве V из раздела 3 мы выбираем левый идеал $(GF)\widehat{\omega}$ алгебры GF, а в качестве ρ — отображение $x \mapsto x^{-1}\widehat{\omega}$ $(x \in G)$. Очевидно, что $\langle G\rho \rangle = (GF)\widehat{\omega}$. Положим $C = \{\rho\lambda \mid \lambda \in ((GF)\widehat{\omega})^*\}$ и покажем, что $C = \omega(GF)$. Для каждого $g \in G$ обозначим δ_g отображение из $(GF)^*$, переводящее $\sum_{x \in G} x(x\varphi) \in GF$, где $\varphi \in F^G$, в $g\varphi$. Тогда $(GF)^* = \langle \delta_g \mid g \in G \rangle$. Кроме того, $((GF)\widehat{\omega})^*$ совпадает с множеством всевозможных ограничений на $(GF)\widehat{\omega}$ отображений из $(GF)^*$. Следовательно, $C = \langle \rho\delta_g \mid g \in G \rangle$. Непосредственно проверяется, что $\rho\delta_g = \omega g^{-1}$ для любого $g \in G$. Поэтому $C = \langle \omega g^{-1} \mid g \in G \rangle = \omega(GF)$. Таким образом, к коду $\omega(GF)$ применима теорема 1, из которой вытекает следующее утверждение.

Следствие 1. *Пусть $\mu \in (F^\times)^G$, $\sigma \in \mathcal{S}_G$ и α — автоморфизм поля F. Тогда*

(i) $[\mu; \sigma, \alpha] \in \mathrm{Aut}(\omega(GF))$, *если и только если существует α^{-1}-полулинейное отображение $\xi\colon (GF)\widehat{\omega} \to (GF)\widehat{\omega}$, удовлетворяющее равенству*

$$(x^{-1}\widehat{\omega})\xi = (x\sigma)^{-1}\widehat{\omega}(x\sigma\mu) \tag{9}$$

для всех $x \in G$;

(ii) $[\mu\sigma] \in \mathrm{MAut}(\omega(GF))$, *если и только если существует линейное отображение $\xi\colon (GF)\widehat{\omega} \to (GF)\widehat{\omega}$, удовлетворяющее равенству* (9)*;*

(iii) $\sigma \in \mathrm{PAut}(\omega(GF))$, *если и только если существует линейное отображение $\xi\colon (GF)\widehat{\omega} \to (GF)\widehat{\omega}$, которое удовлетворяет равенству*

$$(x^{-1}\widehat{\omega})\xi = (x\sigma)^{-1}\widehat{\omega}$$

для всех $x \in G$.

Кроме того, если такое отображение ξ существует, то оно единственно и биективно.

Определим подгруппу H группы G следующим образом:

$$H = \{x \in G \mid x\widehat{\omega} = \widehat{\omega}\}. \tag{10}$$

Тогда очевидно, что

$$|\{x \in G \mid x^{-1}\widehat{\omega} = g^{-1}\widehat{\omega}\}| = |Hg| = |H|$$

для любого $g \in G$. Поэтому следующее утверждение является следствием из теоремы 2.

Следствие 2. *Если H определяется равенством* (10)*, то t-группы $(G, \mathrm{PAut}(\omega(GF)))$, $(H, \mathcal{S}_H) \wr (G\widehat{\omega}, GL((GF)\widehat{\omega})|_{G\widehat{\omega}})$ подобны.*

5. Коды $E_s(X)$ и $D_{\mathfrak{S}}(X)$

В настоящем разделе мы предполагаем, что поле F конечно и $|F| = q$. Пусть также K есть поле, являющееся расширением поля F и G есть некоторая конечная подгруппа $K^\times$. Тогда G циклична и ее порядок не делится на характеристику поля F. Роль множества X из раздела 3 будет играть либо G, либо $G \cup \{0\}$; эти два случая рассматриваются параллельно. Мы рассматриваем векторное пространство F^X как GF-модуль, в котором $x(\varphi g) = (xg^{-1})\varphi$ для всех $x \in X$, $g \in G$ и $\varphi \in F^X$. Обозначим через $\mathfrak{C}$ множество всех q-циклотомических классов по модулю $|G|$, то есть множеств вида $\{lq^i \bmod |G|,\ i = 0, 1, \dots\}$, где $l \in \mathbf{Z}_{|G|}$, если $X = G$, и это множество, объединенное с $\{\{|G|\}\}$, если $X = G \cup \{0\}$.

Пусть $s \in \mathbf{Z}_{|X|}$. Положим

$$L_s = \langle x^s \mid x \in X\rangle = \langle x^s \mid x \in G\rangle.$$

Очевидно, что L_s есть конечное подполе K, причем $F \subseteq L_s$. Мы будем рассматривать L_s как GF-модуль, в котором действие элемента $g \in G$ переводит $v \in L_s$ в vg^{-s}. Обозначим через $E_s(X)$ множество всех отображений вида

$$x \mapsto \mathrm{Tr}_{L_s}(vx^s), \quad x \in X, \quad v \in L_s. \tag{11}$$

Очевидно, что $E_s(X)$ есть GF-подмодуль F^X. Кроме того, отображение, переводящее $v \in L_s$ в отображение (11), является изоморфизмом L_s на $E_s(X)$ как GF-модулей.

Легко видеть, что если s_1 и s_2 принадлежат одному и тому же множеству из $\mathfrak{C}$, то $E_{s_1}(X) = E_{s_2}(X)$. Поэтому для каждого $\mathfrak{c} \in \mathfrak{C}$ мы можем положить

$$D_{\mathfrak{c}}(X) = E_s(X),$$

где s — произвольный элемент $\mathfrak{c}$. Положим также

$$D_{\mathfrak{S}}(X) = \sum_{\mathfrak{c}\in\mathfrak{S}} D_{\mathfrak{c}}(X)$$

для всякого $\mathfrak{S} \subseteq \mathfrak{C}$. Как будет отмечено ниже, эта сумма является прямой. Целью настоящего раздела является применение результатов раздела 3 к кодам $D_{\mathfrak{S}}(X)$.

Приведем описание GF-подмодулей модуля F^X. Рассмотрим сначала случай, когда $X = G$. В этом случае такое описание вытекает из описания идеалов алгебры GF (см. [3]). Именно, F^G является прямой суммой семейства $\{D_{\mathfrak{c}}(G) \mid \mathfrak{c} \in \mathfrak{C}\}$ своих попарно неизоморфных простых GF-подмодулей. Поэтому отображение $\mathfrak{S} \mapsto D_{\mathfrak{S}}(G)$, $\mathfrak{S} \subseteq \mathfrak{C}$, является изоморфизмом решетки всех подмножеств $\mathfrak{C}$ (относительно операций объединения и пересечения) на решетку всех GF-подмодулей модуля F^G. Как отмечалось в разделе 4, все GF-подмодули F^G являются циклическими, так как характеристика поля F не делит $|G|$. Таким образом, эта ситуация является частным случаем ситуации раздела 4.

Пусть теперь $X = G \cup \{0\}$. В этом случае GF-модуль F^X содержит подмодуль $M = \{\varphi \in F^X \mid 0\varphi = 0\}$ такой, что F^X является прямой суммой M и $D_{\{0\}}(X)$. Отображение $\varphi \mapsto \varphi|_G$ ($\varphi \in M$) является изоморфизмом M на F^G как GF-модулей. Следовательно, F^X является прямой суммой семейства $\{D_{\mathfrak{c}}(X) \mid \mathfrak{c} \in \mathfrak{C}\}$ своих простых GF-подмодулей. Среди этих простых подмодулей $D_{\mathfrak{c}}(X)$ при $\mathfrak{c} \in \mathfrak{C} \setminus \{\{|G|\}\}$ попарно неизоморфны, а $D_{\{|G|\}}(X)$ изоморфен $D_{\{0\}}(X)$ (оба они являются одномерными пространствами с тривиальным действием группы G). Поэтому произвольный GF-подмодуль F^X является

прямой суммой $D_{\mathfrak{T}}(X)$ при некотором множестве $\mathfrak{T} \subseteq \mathfrak{C} \setminus \{\{0\}, \{|G|\}\}$ и некоторого подпространства прямой суммы $D_{\{0\}}(X) = E_0(X)$ и $D_{\{|G|\}}(X) = E_{|G|}(X)$. Мы ограничимся рассмотрением GF-подмодулей вида $D_{\mathfrak{S}}(X)$ при $\mathfrak{S} \subseteq \mathfrak{C}$ (для остальных GF-подмодулей F^X рассуждения проводятся аналогично). Отметим, что если X — конечное подполе K, то коды $D_{\mathfrak{S}}(X)$ при $\mathfrak{S} \subseteq \mathfrak{C} \setminus \{\{|G|\}\}$ назывались в подразделе 3.1 в [1] расширенными циклическими кодами над F длины $|X|$. Кроме того, если q есть простое число и X есть конечное подполе K, то коды $D_{\mathfrak{S}}(X)$ при $\mathfrak{S} \subseteq \mathfrak{C}$ рассматривались О. А. Логачевым, А. А. Сальниковым и В. В. Ященко.

Предположим снова, что X равно либо G, либо $G \cup \{0\}$. Фиксируем произвольное множество $\mathfrak{S} \subseteq \mathfrak{C}$. Выберем какое-либо множество S представителей всех множеств из $\mathfrak{S}$ и обозначим через L_S внешнюю прямую сумму семейства $\{L_s \mid s \in S\}$. Мы будем рассматривать L_S и как GF-модуль, и как линейную алгебру. Из сказанного выше следует, что $D_{\mathfrak{S}}(X)$ состоит из всех отображений вида

$$x \mapsto \sum_{s \in S} \mathrm{Tr}_{L_s}(v_s x^s), \qquad x \in X, \tag{12}$$

где $v_s \in L_s$. Применим к коду $D_{\mathfrak{S}}(X)$ результаты раздела 3, выбрав в качестве V пространство L_S, а в качестве ρ отображение $x \mapsto (x^s \mid s \in S)$, $x \in X$. Очевидно, что $\langle X\rho \rangle$ является подмодулем GF-модуля L_S, причем проекция $\langle X\rho \rangle$ на L_s отлична от $\{0\}$ для любого $s \in S$. Если $\{0, |G|\} \not\subseteq S$ (в частности, если $X = G$), то из сказанного выше вытекает, что $\{L_s \mid s \in S\}$ является семейством попарно неизоморфных простых GF-модулей. Следовательно, в этом случае $\langle X\rho \rangle = L_S$. Предположим теперь, что $\{0, |G|\} \subseteq S$ (это возможно лишь при $X = G \cup \{0\}$). Тогда

$$W = \{(v_s \mid s \in S) \in L_S \mid v_0 = v_{|G|} = 0\} \subseteq \langle X\rho \rangle.$$

Кроме того, 0ρ и 1ρ линейно независимы по модулю W, поэтому они порождают пространство L_S по модулю W, так как размерность L_S / W равна 2. Следовательно, и в этом случае $\langle X\rho \rangle = L_S$. Очевидно также, что отображение

$$((v_s \mid s \in S), (w_s \mid s \in S)) \mapsto \sum_{s \in S} \mathrm{Tr}_{L_s}(v_s w_s) \quad v_s, w_s \in L_s, \quad s \in S,$$

является невырожденной симметричной билинейной формой на пространстве L_S. Из этого, ввиду (12), следует, что код $D_{\mathfrak{S}}(X)$ имеет вид, рассматриваемый в разделе 3. Таким образом, к этому коду применима теорема 1, из которой вытекает следующее утверждение.

Следствие 3. *Пусть $\mu \in (F^\times)^X$, $\sigma \in \mathcal{S}_X$ и α — автоморфизм поля F. Тогда*

(i) *$[\mu\sigma\alpha] \in \mathrm{Aut}(D_{\mathfrak{S}}(X))$, если и только если существует α^{-1}-полулинейное отображение $\xi\colon L_S \to L_S$, удовлетворяющее равенству*

$$(x^s \mid s \in S)\xi = ((x\sigma)^s (x\sigma\mu) \mid s \in S) \tag{13}$$

для всех $x \in X$;

(ii) *$[\mu\sigma] \in \mathrm{MAut}(D_{\mathfrak{S}}(X))$, если и только если существует линейное отображение $\xi\colon L_S \to L_S$, удовлетворяющее равенству* (13)*;*

(iii) $\sigma \in \mathrm{PAut}(D_{\mathfrak{S}}(X))$, *если и только если существует линейное отображение* $\xi\colon L_S \to L_S$, *удовлетворяющее равенству*

$$(x^s \mid s \in S)\xi = ((x\sigma)^s \mid s \in S)$$

для всех $x \in X$.

Кроме того, если такое отображение ξ *существует, то оно единственно и биективно.*

Если $X = G$, то ρ есть гомоморфизм из G в $L_S^\times$. Его ядром является подгруппа

$$H = \bigcap_{s\in S}\{x \in G \mid x^s = 1\} \tag{14}$$

группы G. Другими словами, H — единственная подгруппа G такая, что $|H|$ равен наибольшему общему делителю $|G|$ и всех элементов S. В этом случае

$$|\{x \in G \mid x\rho = g\rho\} = |Hg| = ||H||$$

для любого $g \in G$. Поэтому из теоремы 2 вытекает следующее утверждение.

Следствие 4. *Предположим, что* $X = G$. *Пусть* H *определяется равенством* (14), *а*

$$Z = G\rho = \{(x^s \mid s \in S) \mid x \in G\}.$$

Тогда t*-группы* $(G, \mathrm{PAut}(D_{\mathfrak{S}}(G)))$, $(H, \mathcal{S}_H) \wr (Z, GL(L_S)|_Z)$ *подобны.*

6. Пересечения групп $\mathrm{PAut}(E_s(K))$, где $|K = q^n|$

В настоящем разделе будут использоваться обозначения и соглашения раздела 5. При этом мы дополнительно предполагаем, что $|K| = q^n$ (где n — целое положительное число) и $X = K$. Обозначим также через Π группу всех перестановок из $\mathcal{S}_K$ вида $x \mapsto cx^{q^i}$, где $c \in K^\times$ и $i \in \mathbf{Z}_n$. Непосредственно проверяется (а также вытекает из части (iii) следствия 3), что

$$\Pi \subseteq \bigcap_{\mathfrak{S}\subseteq\mathfrak{C}} \mathrm{PAut}(D_{\mathfrak{S}}(K)).$$

В частности,

$$\Pi \subseteq \bigcap_{s=0}^{q^n-1} \mathrm{PAut}(E_s(K)). \tag{15}$$

В. В. Ященко высказал предположение о том, что знак включения в формуле (15) можно заменить на знак равенства. Целью настоящего раздела является доказательство этого предположения (см. теоремы 3 и 4 ниже).

Замечание 1. Хорошо известно, что любое отображение из K^K единственным образом представимо в виде многочлена над K степени не более $|K| - 1 = q^n - 1$ (нулевому многочлену мы приписываем отрицательную степень). Кроме того, отображение из K^K линейно тогда и только тогда, когда его представление в виде такого многочлена имеет вид $x \mapsto \sum_{i=0}^{n-1} a_i x^{q^i}$, где $a_i \in K$ для всех $i \in \mathbf{Z}_n$.

Замечание 2. Пусть $s \in \mathbf{Z}_{q^n}$ и $\sigma \in \mathrm{PAut}(E_s(K))$. Тогда из пункта (iii) следствия 3 и замечания 1 вытекает, что существуют $a_0, \ldots, a_{n-1} \in K$, удовлетворяющие равенству

$$(x\sigma)^s = \sum_{i=0}^{n-1} a_i x^{sq^i}$$

для всех $x \in K$.

Теорема 3. *Справедливо равенство*

$$\Pi = \mathrm{PAut}(E_1(K)) \cap \bigcap_{l=1}^{n-1} \mathrm{PAut}(E_{q^l+1}(K)). \tag{16}$$

Доказательство. Ввиду формулы (15), достаточно доказать только включение $\supseteq$ в равенстве (16). Пусть $\sigma \in \mathcal{S}_K$ принадлежит правой части равенства (16). Тогда, ввиду замечания 2,

$$x\sigma = \sum_{i=0}^{n-1} a_i x^{q^i} \quad (x \in K) \tag{17}$$

для некоторых $a_i \in K$, так как $\sigma \in \mathrm{PAut}(E_1(K))$.

Предположим, что существуют $k_1, k_2 \in \mathbf{Z}_n$ такие, что $k_1 < k_2$, $a_{k_1} \neq 0$ и $a_{k_2} \neq 0$. Пусть $l = k_2 - k_1$. Тогда из формулы (17) следует равенство

$$\begin{aligned}(x\sigma)^{q^l+1} = (x\sigma)^{q^l}(x\sigma) &= \sum_{i,j=0}^{n-1} a_i^{q^l} a_j x^{q^{(i+l) \bmod n} + q^j} \\ &= a_{n-1-l}^{q^l} a_{n-1} x^r + \sum_{\substack{i,j \in \{0,\ldots,n-1\} \\ (i,j) \neq (n-1-l,n-1)}} a_i^{q^l} a_j x^{q^{(i+l) \bmod n} + q^j}, \quad x \in K, \end{aligned} \tag{18}$$

где $r = 2q^{n-1}$, если $q \neq 2$, и $r = 1$ в противном случае. В то же время из замечания 2 следует, что

$$(x\sigma)^{q^l+1} = \sum_{i=0}^{n-1} b_i x^{(q^l+1)q^i} = \sum_{i=0}^{n-1} b_i x^{q^{(i+l) \bmod n} + q^i}, \qquad x \in K, \tag{19}$$

для некоторых $b_i \in K$, так как $1 \leqslant l \leqslant n-1$ и, следовательно, $\sigma \in \mathrm{PAut}(E_{q^l+1}(K))$.

Очевидно, что самые правые части равенств (18) и (19) представляют собой значения многочленов над K степени не более $|K| - 1 = q^n - 1$ на произвольном элементе $x \in K$. Следовательно, эти многочлены должны совпадать (см. замечание 1). С другой стороны, положим $t = 2q^{k_2}$, если $q \neq 2$ или $k_2 \neq n-1$, и $t = 1$ в противном случае. Тогда коэффициент при x^t в самой правой части равенства (18) равен $a_{k_1}^{q^l} a_{k_2} \neq 0$, а в самой правой части равенства (19) он равен 0. Это противоречие показывает, что множество $\{i \in \mathbf{Z}_n \mid a_i \neq 0\}$ содержит не более одного элемента. В то же время это множество непусто, так как $\sigma \in \mathcal{S}_K$. Таким образом, $\sigma \in \Pi$.

Теорема 4. *Пусть s — целое число, удовлетворяющее неравенствам $2 \leqslant s \leqslant q-1$ и взаимно простое с q. Тогда*

$$\Pi = \mathrm{PAut}(E_1(K)) \cap \mathrm{PAut}(E_s(K)). \tag{20}$$

Доказательство. Ввиду формулы (15), достаточно доказать только включение $\supseteq$ в равенстве (20). Пусть $\sigma \in \mathcal{S}_K$ принадлежит правой части равенства (20). Тогда, ввиду замечания 2,

$$x\sigma = \sum_{i=0}^{n-1} a_i x^{q^i}, \qquad x \in K,$$

для некоторых $a_i \in K$, так как $\sigma \in \mathrm{PAut}(E_1(K))$. Следовательно,

$$(x\sigma)^s = \sum_{\substack{i_0,\ldots,i_{n-1}\geqslant 0,\\ i_0+\ldots+i_{n-1}=s}} \frac{s!}{i_0!\cdots i_{n-1}!} a_0^{i_0}\cdots a_{n-1}^{i_{n-1}} x^{i_0+i_1q+\ldots+i_{n-1}q^{n-1}}, \qquad x \in K. \tag{21}$$

В то же время, из замечания 2 вытекает, что

$$(x\sigma)^s = \sum_{i=0}^{n-1} b_i x^{sq^i}, \qquad x \in K, \tag{22}$$

для некоторых $b_i \in K$, так как $\sigma \in \mathrm{PAut}(E_s(K))$.

Предположим, что существуют $k_1, k_2 \in \mathbf{Z}_n$ такие, что $k_1 \neq k_2$, $a_{k_1} \neq 0$ и $a_{k_2} \neq 0$. Очевидно, что правые части равенств (21) и (22) представляют собой значения многочленов над K степени не более $|K| - 1 = q^n - 1$ на произвольном элементе $x \in K$. Следовательно, эти многочлены должны совпадать (см. замечание 1). Однако коэффициент при $x^{q^{k_1}+(s-1)q^{k_2}}$ в правой части равенства (21) равен $sa_{k_1}a_{k_2}^{s-1} \neq 0$, а в правой части равенства (22) он равен 0. Это противоречие показывает, что множество $\{i \in \mathbf{Z}_n \mid a_i \neq 0\}$ содержит не более одного элемента. В то же время это множество непусто, так как $\sigma \in \mathcal{S}_K$. Таким образом, $\sigma \in \Pi$.

Очевидно, что целые числа s, удовлетворяющие условиям теоремы 4, существуют тогда и только тогда, когда $q \neq 2$. Действительно, в качестве такого числа s можно взять 2 (если q нечетно) или 3 (если $q = 2^j$, где j — целое число, удовлетворяющее неравенству $j \geqslant 2$).

Список литературы

1. Huffman W. C., Codes and groups. In: *Handbook of coding theory*, **II** (Pless V. S., Huffman W. C., Brualdi R. A., eds.). Elsevier, Amsterdam, 1998, pp. 1345–1440.
2. Берман С. Д., К теории групповых кодов. *Кибернетика* (1967) №1, 31–39.
3. Берман С. Д., Полупростые циклические и абелевы коды. II. *Кибернетика* (1967) №3, 21–30.
4. MacWilliams F. J., *Combinatorial problems of elementary group theory*, PhD Thesis, Dept. Math., Harvard Univ., 1962.

Статья поступила 30.01.2009.