2008 Теоретические основы прикладной дискретной математики № 1(1)

DOI 10.17223/20710410/1/5

УДК 519.7

ЛИНЕЙНЫЕ СТРУКТУРЫ ГРУПП ПОДСТАНОВОК НАД КОНЕЧНЫМ МОДУЛЕМ[1]

М.А. Пудовкина

Московский инженерно-физический институт (*государственный университет*)

E-mail: maricap@rambler.ru

Описание отображений с линейными структурами важно для синтеза и анализа шифрсистем, поскольку нетривиальная линейная структура является слабостью криптографического отображения. В частности, позволяет применить дифференциальный метод криптоанализа или метод гомоморфизмов. В данной работе на групповом языке описаны все биективные отображения над конечным модулем с линейной структурой.

Ключевые слова: *линейная структура*, *модуль*, *группа подстановок*, *импримитивная группа*, *сплетение групп.*

Линейная структура отображений (блочных шифрсистем) рассматривалась в работах [1 – 4] и др. Некоторые свойства отображений с линейными структурами приведены, например, в работе [5]. Наличие нетривиальной линейной структуры является слабостью криптографического отображения, в частности позволяет применять метод дифференциального криптоанализа или строить фактор-системы для данной криптографической системы, используя метод гомоморфизмов в явном виде [2] . Таким образом, описание отображений, обладающих линейными структурами, важно для синтеза и анализа шифрсистем.

В данной работе на групповом языке описаны все биективные отображения над конечным модулем с линейной структурой.

Будем придерживаться следующих обозначений: N_0 – множество натуральных чисел с нулем, $m \in N_0$, $m \geq 2$; R – конечное ассоциативное кольцо с единицей; p – простое число; $H \in \{GF(p^m), V_m(p), Z_{p^m}, R\text{-модуль}\}$; $\overline{a,b} = a, a+1, \ldots, b$, $a < b$; $S(X)$ – симметрическая группа подстановок на множестве X; $\pi, \sigma \in S(H)$; 0 – нулевой элемент H; $d(\pi, \sigma) = |\{\alpha \in H | \alpha^\pi \neq \alpha^\sigma\}|$; $<\alpha>$ – группа, порожденная элементом $\alpha \in H \backslash 0$. Отметим, что поле $GF(p^m)$ рассматривается как m-мерное векторное пространство над $GF(p)$.

Напомним (см., например, [5]), что отображение $\pi \in S(H)$ обладает линейной структурой, если в H существует ненулевой элемент α, такой, что $(\beta+\alpha)^\pi = \beta^\pi + \gamma_\alpha$ для любого $\beta \in H$, где $\gamma_\alpha \in H \backslash 0$ – некоторый фиксированный элемент. Элемент α называется линейным транслятором отображения π.

Пусть

$$\Pi_{\alpha,\gamma} = \left\{\pi \in S(H) \,|\, (\beta+\alpha)^\pi - \beta^\pi = \gamma,\ \forall \beta \in H\right\},\ \alpha, \gamma \in H \backslash 0,$$

$$\Pi_{W,W} = \left\{\pi \in S(H) \,|\, (\beta+\alpha)^\pi - \beta^\pi \in W,\ \forall \beta \in F, \forall \alpha \in W\right\},$$

где W – произвольный нетривиальный подмодуль R-модуля H. В частности, $\Pi_{W,W} = \Pi_{\alpha,\alpha}$, где $W = <\alpha>$. Существование у отображения подмодуля W, для которого $\Pi_{W,W} \neq e$, можно рассматривать как обобщение понятия линейной структуры. Его наличие может привести, например, к применению метода гомоморфизмов.

Для $H \in \{GF(2^m), V_m(2)\}$ множества $\Pi_{\alpha,\gamma}$, $\Pi_{W,W}$ описаны автором в работе [4].

1. Описание множества $\Pi_{W,W}$

Для произвольного подмодуля W R-модуля H приведем характеризацию множества $\Pi_{W,W}$ на групповом языке.

Теорема 1. Пусть W – произвольный нетривиальный подмодуль R-модуля H, $|H| = b$, $|W| = d$. Тогда множество $\Pi_{W,W}$ является импримитивной группой из $S(H)$ с системой импримитивности $\{\beta+W | \beta \in H\}$. Группа $\Pi_{W,W}$ подобна группе $S_d \int S_{d^{-1}b}$.

Доказательство. Покажем, что $\Pi_{W,W}$ является группой. Если $\pi_1, \pi_2 \in \Pi_{W,W}$, то для любого $\alpha \in W$ из равенств

$$(\beta+\alpha)^{\pi_1\pi_2} - \beta^{\pi_1\pi_2} = (\beta^{\pi_1}+\alpha)^{\pi_2} - (\beta^{\pi_1})^{\pi_2} = \beta^{\pi_1\pi_2} + \alpha' - \beta^{\pi_1\pi_2} = \alpha' \in W$$

[1] Работа выполнена при поддержке гранта Президента РФ НШ №4.2008.10.

следует, что $\pi_1\pi_2 \in \Pi_{W,W}$. Очевидно, что $e \in \Pi_{W,W}$. Осталось доказать, что $\pi^{-1} \in \Pi_{W,W}$ для любой $\pi \in \Pi_{W,W}$. Если это не так, то существуют $\gamma \in H$, $\alpha \in W$ и подстановка $\pi \in \Pi_{W,W}$ такие, что $(\gamma+\alpha)^{\pi^{-1}} - \gamma^{\pi^{-1}} \notin W$. Положим $\beta = \gamma^{\pi^{-1}}$. Тогда из равенства

$$(\gamma+\alpha)^{\pi^{-1}} - \gamma^{\pi^{-1}} = (\beta^{\pi}+\alpha)^{\pi^{-1}} - (\beta^{\pi})^{\pi^{-1}} = (\beta+\alpha')^{\pi\pi^{-1}} - (\beta^{\pi})^{\pi^{-1}} = \alpha' \in W$$

получаем противоречие с предположением, что $(\gamma+\alpha)^{\pi^{-1}} - \gamma^{\pi^{-1}} \notin W$. Значит, $\Pi_{W,W}$ – группа.

Для любой подстановки $\pi \in \Pi_{W,W}$ равенство $(\beta+W)^{\pi} = \beta^{\pi} + W$ эквивалентно тому, что π: $\beta+W \to \beta^{\pi}+W$ для каждого $\beta \in H$. Группа, порождаемая всеми такими подстановками, является импримитивной с системой импримитивности $\{\beta+W | \beta \in H\}$ и совпадает с группой $S_d \int S_{d^{-1}b}$. Теорема доказана.

В шифраторах обычно используются операции и преобразования над векторным пространством $V_m(p)$, полем Галуа $GF(p^m)$ и кольцом вычетов Z_{p^m}. В качестве следствий теоремы 1 приведем группу $\Pi_{W,W}$ для этих случаев.

Следствие 1. Пусть $H \in \{GF(p^m), V_m(p)\}$. Для любого подпространства $W<H$, $\dim W = t \in \{\overline{1, m-1}\}$, множество $\Pi_{W,W}$ является импримитивной группой из $S(H)$ с системой импримитивности $\{\beta+W | \beta \in H\}$. Группа $\Pi_{W,W}$ подобна группе $S_{p^t} \int S_{p^{m-t}}$.

Следствие 2. Пусть W – идеал кольца вычетов Z_{p^m}, $|W| = p^t$, $t \in \{\overline{1, m-1}\}$. Тогда множество $\Pi_{W,W}$ является импримитивной группой из $S(Z_{p^m})$ с системой импримитивности $\left\{\beta+W \mid \beta \in Z_{p^m}\right\}$. Группа $\Pi_{W,W}$ подобна группе $S_{p^t} \int S_{p^{m-t}}$.

2. Описание множества $\Pi_{\alpha,\gamma}$

Для произвольного модуля H над кольцом вычетов приведем описание множества $\Pi_{\alpha,\alpha}$.

Теорема 2. Пусть α – произвольный ненулевой элемент Z_l-модуля H, $|H| = b$, $l \geq 2$ – произвольное натуральное число, $d = |<\alpha>|$. Тогда множество $\Pi_{\alpha,\alpha}$ является импримитивной группой из $S(H)$ с системой импримитивности $\{\beta+<\alpha> | \beta \in H\}$. Группа $\Pi_{\alpha,\alpha}$ подобна группе $Z_d \int S_{d^{-1}b}$.

Доказательство. Аналогично теореме 1 показывается, что множество $\Pi_{\alpha,\alpha}$ является группой.

Поскольку $(\alpha+\beta)^{\pi} = \alpha+\beta^{\pi}$ для любого элемента $\beta \in H$, то справедливо равенство $(\alpha c+\beta)^{\pi} = \alpha c+\beta^{\pi}$ для любого элемента $\alpha c \in <\alpha>$, $c \in Z_l$, и любого элемента $\beta \in H$. Значит, $(\beta+<\alpha>)^{\pi} = \beta^{\pi}+<\alpha>$ для любого элемента $\beta \in H$. Следовательно, группа $\Pi_{\alpha,\alpha}$ имеет систему импримитивности $\{\beta+<\alpha> | \beta \in H\}$.

Рассмотрим действие группы $\Pi_{\alpha,\alpha}$ на произвольном блоке импримитивности $<\alpha>+\beta$. В этом случае $\beta^{\pi} \in \beta+<\alpha>$. Пусть $\beta^{\pi} = \alpha r+\beta$ для некоторого элемента $\alpha r \in <\alpha>$. Тогда справедливо равенство $(\alpha c+\beta)^{\pi} = \beta+\alpha(c+r)$ для любого элемента $\alpha c \in <\alpha>$. Таким образом, группа $\Pi_{\alpha,\alpha}$ подобна аддитивной группе кольца вычетов Z_d по сложению. Теорема доказана.

В качестве следствий теоремы 2 приведем множество $\Pi_{\alpha,\alpha}$ для $H \in \{GF(p^m), V_m(p), Z_{p^m}\}$.

Следствие 1. Пусть $H \in \{GF(p^m), V_m(p)\}$. Для любого ненулевого $\alpha \in H$ множество $\Pi_{\alpha,\alpha}$ является импримитивной группой из $S(H)$ с системой импримитивности $\{\beta+<\alpha> | \beta \in H\}$. Группа $\Pi_{\alpha,\alpha}$ подобна группе $Z_p \int S_{p^{m-1}}$.

Следствие 2. Для любого ненулевого $\alpha \in Z_{p^m}$, $|<\alpha>| = p^t$, $t \in \{\overline{1, m-1}\}$, множество $\Pi_{\alpha,\alpha}$ является импримитивной группой из $S(Z_{p^m})$ с системой импримитивности $\left\{\beta+<\alpha> \mid \beta \in Z_{p^m}\right\}$. Группа $\Pi_{\alpha,\alpha}$ подобна группе $Z_{p^t} \int S_{p^{m-t}}$.

Для произвольного модуля H над кольцом вычетов покажем, что множество $\Pi_{\alpha,\gamma}$ является правым смежным классом группы $S(H)$ по подгруппе $\Pi_{\alpha,\alpha}$.

Утверждение 1. Пусть α, γ – произвольные ненулевые элементы Z_l-модуля H, $\alpha \neq \gamma$, $d = |<\alpha>|$, $|H| = b$, $l \geq 2$ – произвольное натуральное число. Тогда

$$\Pi_{\alpha,\gamma} = \begin{cases} \left(\Pi_{\alpha,\alpha}\right)h = \left(Z_d \int S_{d^{-1}b}\right)h, \text{ если } |<\alpha>| = |<\gamma>|, \\ \varnothing, \text{ если } |<\alpha>| \neq |<\gamma>|, \end{cases}$$

где h – произвольное линейное отображение из $\Pi_{\alpha,\gamma}$, $\alpha^h = \gamma$.

Доказательство. Для всех $\beta \in H$, $r \in Z_l$ справедливо равенство $(\alpha r + \beta)^\pi = \beta^\pi + \gamma r$. Если $\Pi_{\alpha,\gamma} \neq \varnothing$ при $|<\alpha>| \neq |<\gamma>|$, то $\beta^\pi = \beta^\pi + \gamma d$ и $\gamma d \neq 0$ при $r = d$, что невозможно. Значит, $\Pi_{\alpha,\gamma} = \varnothing$ при $|<\alpha>| \neq |<\gamma>|$.

Если $|<\alpha>| = |<\gamma>|$, то всегда существует линейное отображение $h \in H$, такое, что $\alpha^h = \gamma$, и $h \in \Pi_{\alpha,\gamma}$. Следовательно, $\Pi_{\alpha,\gamma} \neq \varnothing$.

Рассмотрим теперь случай, когда $|<\alpha>| = |<\gamma>|$, т.е. $\Pi_{\alpha,\gamma} \neq \varnothing$. Очевидно, что $\Pi_{\alpha,\gamma} \cap \Pi_{\alpha,\alpha} = \varnothing$ при $\alpha \neq \gamma$. Если $s \in \Pi_{\alpha,\gamma}$ и $g \in (\Pi_{\alpha,\alpha})s$, то выполняется равенство $(\beta + \alpha)^g = (\beta + \alpha)^{\pi s} = (\beta^\pi + \alpha)^s = \beta^{\pi s} + \gamma$, где $g = \pi s$ для некоторой подстановки $\pi \in \Pi_{\alpha,\alpha}$.

Кроме того, если $s \in \Pi_{\alpha,\gamma}$, то $s^{-1} \in \Pi_{\gamma,\alpha}$, так как равенство $(\beta + \alpha)^s = \beta^s + \gamma$ влечет $(\theta + \gamma)^{s^{-1}} = \theta^{s^{-1}} + \alpha$, где $\theta = \beta^s$.

Для любых подстановок $s_1, s_2 \in \Pi_{\alpha,\gamma}$ из справедливости равенства $(\beta + \alpha)^{s_1 s_2^{-1}} = (\beta^{s_1} + \gamma)^{s_2^{-1}} = \beta^{s_1 s_2^{-1}} + \alpha$ следует, что $s_1 s_2^{-1} \in \Pi_{\alpha,\alpha}$. Таким образом, $\Pi_{\alpha,\gamma} = \Pi_{\alpha,\alpha} h$.

Из теоремы 2 следует, что $\Pi_{\alpha,\alpha} = Z_d \int S_{d^{-1}b}$. Значит, $\Pi_{\alpha,\gamma} = \left(Z_d \int S_{d^{-1}b}\right)h$. Утверждение доказано.

Следствие 1. Пусть α, γ – произвольные ненулевые элементы Z_l-модуля H, $\alpha \neq \gamma$, $|<\gamma>| = d$, $|H| = b$, $l \geq 2$ – произвольное натуральное число, $d = |<\alpha>|$. Тогда

$$\Pi_{\alpha,\gamma} = \begin{cases} h\left(\Pi_{\gamma,\gamma}\right) = h\left(Z_d \int S_{d^{-1}b}\right), \text{ если } |<\alpha>| = |<\gamma>|, \\ \varnothing, \text{ если } |<\alpha>| \neq |<\gamma>|, \end{cases}$$

где h – произвольное линейное отображение из $\Pi_{\alpha,\gamma}$, $\alpha^h = \gamma$.

Доказательство аналогично доказательству утверждения 1.

Следствие 2. Пусть выполнены условия утверждения 1. Тогда $\left|\Pi_{\alpha,\gamma}\right| = (b/d)! \cdot d^{b/d}$, если $|<\alpha>| = |<\gamma>|$, и $|\Pi_{\alpha,\gamma}| = 0$, если $|<\alpha>| \neq |<\gamma>|$.

Следствие 3. Пусть $H \in \{GF(p^m), V_m(p)\}$. Для любых ненулевых элементов $\alpha, \gamma \in H$ множество $\Pi_{\alpha,\gamma} = \Pi_{\alpha,\alpha} h = \left(Z_p \int S_{p^{m-1}}\right)h$, где h – произвольное линейное отображение из $\Pi_{\alpha,\gamma}$. Число подстановок из $S(H)$, обладающих линейным транслятором α, равно $(p^m - 1) \cdot p^{p^{m-1}} \cdot (p^{m-1}!)$.

Доказательство следует из утверждения 1, следствия 2 из него и того, что $|<\alpha>| = |<\gamma>| = p$ для любых ненулевых элементов $\alpha, \gamma \in H \setminus 0$.

Следствие 4. Пусть α, γ – произвольные ненулевые элементы кольца Z_{p^m}, $\alpha \neq \gamma$, $|<\alpha>| = p^t$, $t \in \{\overline{1, m-1}\}$. Тогда

$$\Pi_{\alpha,\gamma} = \begin{cases} \left(\Pi_{\alpha,\alpha}\right)h = \left(Z_{p^t} \int S_{p^{m-1}}\right)h, \text{ если } |<\alpha>| = |<\gamma>|, \\ \varnothing, \text{ если } |<\alpha>| \neq |<\gamma>|, \end{cases}$$

где h – произвольное линейное отображение из $\Pi_{\alpha,\gamma}$, $\alpha^h = \gamma$.

Число подстановок из $S(Z_{p^m})$, обладающих линейным транслятором α, равно

$$(p^{m-t} - p^{m-t-1}) \cdot p^{t \cdot p^{m-t}} \cdot (p^{m-t}!).$$

Доказательство следует из утверждения 1, следствия 2 из него и того, что число элементов $\gamma \in Z_{p^m}$, удовлетворяющих равенству $|<\gamma>| = p^t$ в Z_{p^m}, равно $\varphi(p^{m-t}) = p^{m-t} - p^{m-t-1}$.

Для $H \in \{GF(p^m), V_m(p)\}$ покажем, что множества $\bigcap_{i=1}^{k} \Pi_{<\alpha_i>,<\alpha_i>}$, где $\{\alpha_1, \ldots, \alpha_k\} \subseteq H \setminus 0$, $k \geq 1$, также являются сплетениями групп подстановок. Кроме того, подобные группы возникают при описании силовских p-подгрупп группы $S(H)$.

Теорема 3. Пусть $H \in \{GF(p^m),\ V_m(p)\}$. Для любого подмножества $\{\alpha_1, \ldots, \alpha_k\} \subseteq H$, $k \in \overline{\{1, p^m\}}$, $\dim<\alpha_1, \ldots, \alpha_k> = t \geq 1$, имеет место равенство $\bigcap_{i=1}^{k} \Pi_{<\alpha_i>,<\alpha_i>} = \underbrace{S_p \int \ldots \int S_p}_{t} \int S_{p^{m-t}}$.

Доказательство. Обозначим $G^{(1)} = \bigcap_{i=1}^{k} \Pi_{<\alpha_i>,<\alpha_i>}$. Аналогично доказательству теоремы 1 показывается, что $G^{(1)}$ является группой.

Предположим, что элементы $\alpha_1, \ldots, \alpha_t \in H$ линейно независимы. Пусть $\gamma \in H \backslash 0$. Для произвольного множества $X = \{x_1, \ldots, x_r\}$, $r \geq 1$, обозначим $X+\gamma = \{x_1+\gamma, \ldots, x_r+\gamma\}$.

Положим $X_\gamma^{(0)} = \gamma$, $X_\gamma^{(1)} = \gamma + <\alpha_1, \ldots, \alpha_t>$ для $\gamma \in H$, $[X^{(1)}] = \{X_\gamma^{(1)} \mid \gamma \in H\}$, $X_\gamma^{(2)} = \gamma + <\alpha_2, \ldots, \alpha_t>$ для $\gamma \in X_0^{(1)}$, $[X^{(2)}] = \{X_\gamma^{(2)} \mid \gamma \in X_0^{(1)}\}$, $\ldots$, $X_\gamma^{(t-1)} = \gamma + <\alpha_t>$ для $\gamma \in X_0^{(t-2)}$, $[X^{(t-1)}] = \{X_\gamma^{(t-1)} \mid \gamma \in X_0^{(t-2)}\}$, $X_\gamma^{(t)} = \gamma$ для $\gamma \in X_0^{(t-1)}$.

Непересекающиеся множества вида $X_\gamma^{(1)}$, $\gamma \in H \backslash 0$, образуют максимальную систему импримитивности группы $G^{(1)}$, а $X_\gamma^{(j)}$, $\gamma \in X_0^{(j-1)}$ – максимальную систему импримитивности группы $G^{(1)}$ при ограничении ее действия на множество $X_0^{(j-1)}$, $j = \overline{2, t-1}$.

Для $j = \overline{1, t-1}$ рассмотрим естественный гомоморфизм $\varphi_j : G^{(j)} \to \overline{G}^{(j)}$ импримитивной группы $G^{(j)}$ с блоками импримитивности $X_\gamma^{(j)}$ с $\operatorname{Ker}\varphi_j = G^{(j+1)}$. Нетрудно убедиться, что $\operatorname{Im}\varphi_j = S([X^{(j)}])$ и $G^{(j)} = G^{(j+1)} \int \overline{G}^{(j)}$. Кроме того, $S([X^{(j)}]) = S_{p^{m-t}}$ при $j = 1$ и $S([X^{(j)}]) = S_p$ при $j \geq 2$, $G^{(t)} = S_p$. Значит, $G^{(1)} = G^{(2)} \int S_{p^{m-t}} = G^{(3)} \int S_p \int S_{p^{m-t}} = \ldots = S_p \int \ldots \int S_p \int S_{p^{m-t}}$. Теорема доказана.

Теорема 4. Пусть $H \in \{GF(p^m),\ V_m(p)\}$. Для любого подмножества $\{\alpha_1, \ldots, \alpha_k\} \subseteq H$, $k \in \overline{\{1, p^m\}}$, $\dim <\alpha_1, \ldots, \alpha_k> = t \geq 1$, имеет место равенство $\bigcap_{i=1}^{k} \Pi_{\alpha_i,\alpha_i} = \underbrace{Z_p \int \ldots \int Z_p}_{t} \int S_{p^{m-t}}$.

Доказательство аналогично доказательству теоремы 3.

Утверждение 2. Пусть W_1 – произвольный нетривиальный подмодуль R-модуля H, $W_1 = <\alpha_1, \ldots, \alpha_t>$, $t \geq 1$, $I = W_1 + \alpha$, $\alpha \in H \backslash W_1$, $|H| = b$, $|W_1| = d_1$. Пусть также $W_2 = <\alpha_1, \ldots, \alpha_t, \alpha>$, $|W_2| = d_2$. Тогда множество $\Pi_{I,I}$ является импримитивной группой из $S(H)$ с системой импримитивности $\{\beta + W_2 \mid \beta \in H\}$. Группа $\Pi_{I,I}$ подобна группе $S_{d_1} \int S_{d_1^{-1}d_2} \int S_{d_2^{-1}b}$.

Доказательство следует из теоремы 1.

ЛИТЕРАТУРА

1. *Evertse J.H.* Linear structures in block ciphers // EUROCRYPT '87. Springer Verlag,1987.
2. *Chaum D.*, *Evertse J.H.* Cryptanalysis of DES with a reduced number of rounds sequences of linear factors in block ciphers // Crypto '85. Springer Verlag, 1985.
3. *Meier W.*, *Staffelbach O.* Nonlinearity criteria for cryptographic functions // EUROCRYPT'89. Springer Verlag, 1989.
4. *Погорелов Б.А.*, *Пудовкина М.А.* Линейные структуры групп подстановок векторных пространств // Труды 3-й Междунар. конф. «Проблемы безопасности и противодействия терроризму, 2007». М.: МЦНМО, 2008.
5. *Логачев О.А.*, *Сальников А.А.*, *Ященко В.В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.