О кратной транзитивности произведения множеств подстановок*

В. В. МИЗЕРОВ
e-mail: luomiana@rambler.ru

УДК 519.7

Ключевые слова: группы подстановок, кратная транзитивность, отношение эквивалентности, ρ-отмеченное множество, (ρ, η)-блочная матрица, редуцированная матрица.

Аннотация

Описан подход, позволяющий в ряде случаев свести изучение кратной транзитивности произведения множеств подстановок на множестве Ω к изучению произведения матриц небольших размеров. Эффективное применение такого подхода требует знания ряда свойств отношений эквивалентности, заданных на декартовой степени множества Ω. С точки зрения этих свойств изучены отношения, построенные с помощью различных групп.

Abstract

V. V. Mizerov, On multiple transitivity for products of sets of permutations, Fundamentalnaya i prikladnaya matematika, vol. 12 (2006), no. 2, pp. 119—141.

The study of multiple transitivity of products of sets of permutations on a set Ω is reduced to the study of products of matrices of small dimensions. For effective application of this approach we need some information about properties of equivalence relations defined on the Cartesian degree of the set Ω. These properties are studied for relations induced by various groups.

В ряде криптографических алгоритмов требуется построить множества подстановок большой мощности, обладающих определённым набором специальных качеств. Один из использующихся способов заключается в итеративном применении преобразований из нескольких относительно небольших по мощности и эффективно реализуемых классов подстановок (см., например, [7]). В математической постановке задачи речь идёт об изучении множества подстановок $A = B_1 \cdot B_2 \cdot \ldots \cdot B_k$. При этом одним из важнейших свойств множества A является его кратная транзитивность (см. [1—3]). В данной работе описан подход, позволяющий свести изучение этого свойства к изучению произведения матриц небольших размеров.

Итак, пусть Ω — непустое конечное множество, $S(\Omega)$ — симметрическая группа подстановок на множестве Ω, l — натуральное число. Через $\Omega^{[l]}$ обозначим

*Работа выполнена при поддержке гранта Президента России НШ 8564.2006.10.

Фундаментальная и прикладная математика, 2006, том 12, № 2, с. 119—141.

множество всех векторов-строк длины l с координатами из Ω, состоящих из попарно различных элементов. Для множества $A \subseteq S(\Omega)$ определим $(0,1)$-матрицу $P_l(A)$, строки и столбцы которой занумерованы в одинаковом порядке элементами множества $\Omega^{[l]}$ и на пересечении строки с номером $\bar{a} = (a_1, a_2, \ldots, a_l)$ и столбца с номером $\bar{b} = (b_1, b_2, \ldots, b_l)$ стоит единица, если существует подстановка $h \in A$ со свойством $h(\bar{a}) = \bar{b}$, и нуль в противном случае. Здесь и далее $h(\bar{a}) = (h(a_1), h(a_2), \ldots, h(a_l))$. Отметим, что множество подстановок A l-транзитивно тогда и только тогда, когда матрица $P_l(A)$ не содержит нулевых элементов.

Если ρ — отношение эквивалентности на множестве $\Omega^{[l]}$, то через $\tilde{\rho}$ обозначим множество номеров классов эквивалентных элементов, на которые множество $\Omega^{[l]}$ разбивается отношением ρ, а через $\tilde{\rho}(u)$ — класс с номером $u \in \tilde{\rho}$. Через $S(\Omega, \rho)$ обозначим множество всех подстановок h из $S(\Omega)$, таких что для любого элемента $\bar{a} \in \Omega^{[l]}$ справедливо соотношение $\bar{a}\ \rho\ h(\bar{a})$. Очевидно, что $S(\Omega, \rho)$ — группа. Множество $K \subseteq S(\Omega, \rho)$ назовём ρ-отмеченным, если для любых ρ-эквивалентных векторов $\bar{a}, \bar{b} \in \Omega^{[l]}$ найдётся такая подстановка $h \in K$, что $h(\bar{a}) = \bar{b}$. Из этого определения вытекает, что если K — ρ-отмеченное множество и множество H удовлетворяет условию $K \subseteq H \subseteq S(\Omega, \rho)$, то H — ρ-отмеченное множество.

Пусть ρ и η — отношения эквивалентности на множестве $\Omega^{[l]}$. Матрицу $P_l(A) = (p_A(\bar{a}, \bar{b}))$ назовём (ρ, η)-блочной, если для любых ρ-эквивалентных элементов $\bar{a}, \bar{c} \in \Omega^{[l]}$ и η-эквивалентных элементов $\bar{b}, \bar{d} \in \Omega^{[l]}$ равенство $p_A(\bar{a}, \bar{b}) = 1$ имеет место тогда и только тогда, когда верно равенство $p_A(\bar{c}, \bar{d}) = 1$. Любой (ρ, η)-блочной матрице $P_l(A)$ поставим в соответствие редуцированную матрицу $\overline{P_l(A)} = (p_{uv})$, строки которой занумерованы элементами множества $\tilde{\rho}$, столбцы — элементами множества $\tilde{\eta}$, положив $p_{uv} = p_A(\bar{a}, \bar{b})$ для любых $u \in \tilde{\rho}$, $v \in \tilde{\eta}$, $\bar{a} \in \tilde{\rho}(u)$, $\bar{b} \in \tilde{\eta}(v)$.

Сформулируем эквивалентные определения ρ-отмеченного множества.

Утверждение 1. *Пусть ρ — отношение эквивалентности на множестве $\Omega^{[l]}$ и $K \subseteq S(\Omega)$. Тогда следующие утверждения эквивалентны*:

1) *множество K является ρ-отмеченным*;
2) *произвольные векторы $\bar{a}, \bar{b} \in \Omega^{[l]}$ ρ-эквивалентны тогда и только тогда, когда найдётся подстановка $h \in K$ со свойством $h(\bar{a}) = \bar{b}$*;
3) *матрица $P_l(K)$ является (ρ, ρ)-блочной и редуцированная матрица $\overline{P_l(K)}$ является единичной.*

Доказательство. Импликация $1 \implies 2$ непосредственно следует из определения ρ-отмеченного мультимножества.

Пусть справедлив п. 2 утверждения 1. Ввиду определения матрицы $P_l(K)$ её элемент $p_K(\bar{a}, \bar{b})$ будет равен единице тогда и только тогда, когда найдётся подстановка $h \in K$ со свойством $h(\bar{a}) = \bar{b}$, т. е. когда векторы $\bar{a}, \bar{b} \in \Omega^{[l]}$ ρ-эквивалентны. Если $\bar{a}', \bar{b}' \in \Omega^{[l]}$, $\bar{a}'\ \rho\ \bar{a}$ и $\bar{b}'\ \rho\ \bar{b}$, то $\bar{a}'\ \rho\ \bar{b}'$ и, следовательно, $p(\bar{a}', \bar{b}') = 1$. Это доказывает (ρ, ρ)-блочность матрицы $P_l(K)$. Кроме того, так

как $p(\bar{a},\bar{b})=1$ только в случае принадлежности $\bar{a}$ и $\bar{b}$ одному классу ρ-эквивалентных элементов, матрица $\overline{P_l(K)}$ единичная.

Импликация $3 \implies 1$ очевидна. □

Утверждение 2. *Пусть ρ и η — отношения эквивалентности на множестве $\Omega^{[l]}$, множество A ρ-отмеченное, множество C η-отмеченное и $B \subseteq S(\Omega)$. Тогда матрица $P_l(ABC)$ будет (ρ,η)-блочной.*

Доказательство. Пусть векторы $\bar{a},\bar{c} \in \Omega^{[l]}$ ρ-эквивалентны, векторы $\bar{b},\bar{d} \in \in \Omega^{[l]}$ η-эквивалентны и справедливо равенство $p_{ABC}(\bar{a},\bar{b})=1$. Тогда по определению матрицы $P_l(ABC)$ найдутся такие подстановки $h_1 \in A$, $h_2 \in B$, $h_3 \in C$, что $h_1h_2h_3(\bar{a})=\bar{b}$. Ввиду п. 2 утверждения 1 справедливы соотношения $\bar{a}\ \rho\ h_1(\bar{a})$ и $h_3^{-1}(\bar{b})\ \eta\ \bar{b}$. Следовательно, $\bar{c}\ \rho\ h_1(\bar{a})$, $h_3^{-1}(\bar{b})\ \eta\ \bar{d}$ и по п. 2 утверждения 1 существуют подстановки $h_1' \in A$, $h_3' \in C$ со свойствами $h_1'(\bar{c})=h_1(\bar{a})$ и $h_3^{-1}h_3'(\bar{b})=\bar{d}$. Отсюда имеем $h_1'h_2h_3'(\bar{c})=\bar{d}$ и $p_{ABC}(\bar{c},\bar{d})=1$. Утверждение доказано. □

Рассмотрим случай, когда ρ-отмеченное множество является группой. По данной подгруппе G группы $S(\Omega)$ определим на множестве $\Omega^{[l]}$ отношение эквивалентности $\rho(l,G)$ следующим образом: будем считать, что векторы $\bar{a},\bar{b} \in \Omega^{[l]}$ находятся в этом отношении тогда и только тогда, когда существует такая подстановка $h \in G$, что $h(\bar{a})=\bar{b}$.

Утверждение 3.

1. *Если ρ — отношение эквивалентности на множестве $\Omega^{[l]}$, то подгруппа G группы $S(\Omega)$ является ρ-отмеченной тогда и только тогда, когда $\rho=\rho(l,G)$.*
2. *Если G — подгруппа группы $S(\Omega)$ и среди классов, на которые отношение $\rho(l,G)$ разбивает множество $\Omega^{[l]}$, существует класс мощности $|G|$, то никакое собственное подмножество группы G не является $\rho(l,G)$-отмеченным.*

Доказательство. Достаточно воспользоваться п. 2 утверждения 1 и определением отношения $\rho(l,G)$. □

Для произвольных отношений эквивалентности ρ и η на множестве $\Omega^{[l]}$ и множества B подстановок из $S(\Omega)$ определим $(0,1)$-матрицу $F_\rho^\eta(B)=(f_{uv}(B))$, строки которой занумерованы элементами множества $\tilde{\rho}$, а столбцы элементами множества $\tilde{\eta}$. Здесь $f_{uv}(B)=1$ тогда и только тогда, когда найдутся такие вектор $\bar{a} \in \tilde{\rho}(u)$ и подстановка $g \in B$, что $g(\bar{a}) \in \tilde{\eta}(v)$.

Для любого неотрицательного действительного числа a положим

$$\operatorname{sgn}(a)=\begin{cases}1, & \text{если } a>0,\\ 0, & \text{если } a=0.\end{cases}$$

По произвольной матрице $P=(p_{ij})$ с неотрицательными действительными элементами определим матрицу $\operatorname{sgn}(P)$ тех же размеров, в которой на пересечении строки с номером i и столбца с номером j стоит элемент $\operatorname{sgn}(p_{ij})$. Через $P^\top$ обозначим матрицу, транспонированную к матрице P.

Утверждение 4. *Пусть ρ и η — отношения эквивалентности на множестве $\Omega^{[l]}$, A, B и C — непустые множества подстановок на Ω, такие что $A \subseteq S(\Omega, \rho)$, $C \subseteq S(\Omega, \eta)$. Тогда справедливы следующие соотношения*:

1) $F_\rho^\eta(B) = \operatorname{sgn}\Big(\sum\limits_{h\in B} F_\rho^\eta(h)\Big)$;
2) $F_\eta^\rho(B^{-1}) = F_\rho^\eta(B)^\top$;
3) $F_\rho^\eta(ABC) = F_\rho^\eta(B)$.

Доказательство. Первый пункт утверждения 4 очевиден.

В силу определений матрицы $F_\rho^\eta(B)$ и мультимножества B^{-1} для любых $u \in \tilde{\rho}$, $v \in \tilde{\eta}$ справедлива цепочка равенств

$$f_{uv}(B) = \operatorname{sgn}\Big(\sum_{h\in B} f_{uv}(h)\Big) = \operatorname{sgn}\Big(\sum_{h\in B} \operatorname{sgn}|\{\bar{a} \in \tilde{\rho}(u) \mid h(\bar{a}) \in \tilde{\eta}(v)\}|\Big) =$$
$$= \operatorname{sgn}\Big(\sum_{h\in B} \operatorname{sgn}|\{\bar{b} \in \tilde{\eta}(v) \mid h^{-1}(\bar{b}) \in \tilde{\rho}(u)\}|\Big) =$$
$$= \operatorname{sgn}\Big(\sum_{g\in B^{-1}} \operatorname{sgn}|\{\bar{b} \in \tilde{\eta}(v) \mid g(\bar{b}) \in \tilde{\rho}(u)\}|\Big) = \operatorname{sgn}\Big(\sum_{g\in B^{-1}} f_{vu}(g)\Big) = f_{vu}(B^{-1}),$$

и второй пункт доказан.

Воспользуемся определениями матрицы $F_\rho^\eta(B)$ и групп $S(\Omega, \rho)$ и $S(\Omega, \eta)$. Для любых $u \in \tilde{\rho}$, $v \in \tilde{\eta}$ имеем

$$f_{uv}(ABC) = \operatorname{sgn}\Big(\sum_{h\in ABC} f_{uv}(h)\Big) = \operatorname{sgn}\Big(\sum_{h_1\in A,\, h_2\in B,\, h_3\in C} f_{uv}(h_1h_2h_3)\Big) =$$
$$= \operatorname{sgn}\Big(\sum_{h_1\in A,\, h_2\in B,\, h_3\in C} \operatorname{sgn}|\{\bar{a} \in \tilde{\rho}(u) \mid h_1h_2h_3(\bar{a}) \in \tilde{\eta}(v)\}|\Big) =$$
$$= \operatorname{sgn}\Big(\sum_{h_1\in A,\, h_2\in B,\, h_3\in C} \operatorname{sgn}|\{\bar{a} \in \tilde{\rho}(u) \mid h_2(\bar{a}) \in \tilde{\eta}(v)\}|\Big) =$$
$$= \operatorname{sgn}\Big(\sum_{h_2\in B} \operatorname{sgn}|\{\bar{a} \in \tilde{\rho}(u) \mid h_2(\bar{a}) \in \tilde{\eta}(v)\}|\Big) = \operatorname{sgn}\Big(\sum_{h_2\in B} f_{uv}(h_2)\Big) = f_{uv}(B),$$

что доказывает третий пункт. □

Непосредственно из пунктов 1 и 3 утверждения 3 вытекает следствие.

Следствие 5. *Пусть $B = \{h_1, h_2, \ldots, h_m\} \subseteq S(\Omega)$, $A_i \subseteq S(\Omega, \rho)$, $C_i \subseteq S(\Omega, \eta)$, $i \in \overline{1,m}$ и $D = \bigcup\limits_{i=1}^{m} A_ih_iC_i$. Тогда справедливо равенство $F_\rho^\eta(D) = F_\rho^\eta(B)$.* □

Путь $\rho_1, \rho_2, \ldots, \rho_{k+1}$ — отношения эквивалентности на множестве $\Omega^{[l]}$ и $B_1, B_2, \ldots, B_k$ — подмножества в $S(\Omega)$. Рассмотрим следующее множество подстановок:

$$\Re(B_1, B_2, \ldots, B_k) = A_1C_1A_2C_2 \ldots A_kC_kA_{k+1}.$$

Здесь для любого $i \in \overline{1,k+1}$ A_i — ρ_i-отмеченное множество и для каждого $j \in \overline{1,k}$ множество C_j определяется следующим образом: если

$$B_j = \{h_1^{(j)}, h_2^{(j)}, \ldots, h_{m_j}^{(j)}\},$$

то

$$C_j = \bigcup_{s=1}^{m_j} U_s^{(j)} h_s^{(j)} V_s^{(j)},$$

где $U_1^{(j)}, \ldots, U_{m_j}^{(j)}$ — некоторые непустые подмножества в $S(\Omega, \rho_j)$, а $V_1^{(j)}, \ldots, V_{m_j}^{(j)}$ — непустые подмножества в $S(\Omega, \rho_{j+1})$.

Оказывается, что l-транзитивность множества $\Re(B_1, B_2, \ldots, B_k)$ зависит только от множеств $B_1, B_2, \ldots, B_k$ и может быть установлена с помощью изучения произведения матриц существенно меньших размеров, чем мощность множества $\Omega^{[l]}$.

Теорема 6. *Пусть $\Re(B_1, B_2, \ldots, B_k)$ — определённое выше множество подстановок, тогда матрица $P_l(\Re(B_1, B_2, \ldots, B_k))$ является (ρ_1, ρ_{k+1})-блочной и справедливо равенство*

$$\overline{P_l(\Re(B_1, B_2, \ldots, B_k))} = \operatorname{sgn}(F_{\rho_1}^{\rho_2}(B_1) \cdot F_{\rho_2}^{\rho_3}(B_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(B_k)).$$

Доказательство. Матрица $P_l(\Re(B_1, B_2, \ldots, B_k))$ будет (ρ_1, ρ_{k+1})-блочной ввиду утверждения 2.

Заметим, что по следствию 5 справедливо равенство

$$F_{\rho_1}^{\rho_2}(C_1) \cdot F_{\rho_2}^{\rho_3}(C_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(C_k) = F_{\rho_1}^{\rho_2}(B_1) \cdot F_{\rho_2}^{\rho_3}(B_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(B_k).$$

Пусть $u_1 \in \tilde{\rho}_1$ и $u_{k+1} \in \tilde{\rho}_{k+1}$. Покажем, что элемент матрицы

$$\overline{P_l(\Re(B_1, B_2, \ldots, B_k))},$$

стоящий на пересечении строки с номером u_1 и столбца с номером u_{k+1}, равен единице тогда и только тогда, когда положителен аналогичный элемент матрицы

$$F_{\rho_1}^{\rho_2}(C_1) \cdot F_{\rho_2}^{\rho_3}(C_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(C_k).$$

Если элемент матрицы

$$\overline{P_l(\Re(B_1, B_2, \ldots, B_k))},$$

стоящий на пересечении строки с номером u_1 и столбца с номером u_{k+1}, равен единице, то для любых векторов $\bar{a}_1 \in \tilde{\rho}_1(u_1)$ и $\bar{b}_{k+1} \in \tilde{\rho}_{k+1}(u_{k+1})$ справедливо равенство $p_{\Re(B_1, B_2, \ldots, B_k)}(\bar{a}_1, \bar{b}_{k+1}) = 1$. Тогда по определению матрицы $P_l(\Re(B_1, B_2, \ldots, B_k))$ найдутся подстановки $g_i \in A_i$, $i \in \overline{1,k+1}$, и $h_j \in C_j$, $j \in \overline{1,k}$, удовлетворяющие равенству $g_1 h_1 \ldots g_k h_k g_{k+1}(\bar{a}_1) = \bar{b}_{k+1}$. Положим $g_1 h_1 \ldots g_{i-1} h_{i-1} g_i(\bar{a}_1) = \bar{b}_i$ и $g_1 h_1 \ldots g_i h_i(\bar{a}_1) = \bar{a}_{i+1}$ при всех $i \in \overline{1,k}$. Так как для любого $i \in \overline{1,k+1}$ множество A_i является ρ_i-отмеченным, то $\bar{a}_i \ \rho_i \ \bar{b}_i$ и $\bar{a}_i, \bar{b}_i \in \tilde{\rho}_i(u_i)$. Следовательно, для каждого $j \in \overline{1,k}$ элемент $f_{u_j, u_{j+1}}(C_j)$ матрицы $F_{\rho_j}^{\rho_{j+1}}(C_j)$ равен единице. Поэтому элемент матрицы

$$F_{\rho_1}^{\rho_2}(C_1) \cdot F_{\rho_2}^{\rho_3}(C_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(C_k),$$

стоящий на пересечении строки с номером u_1 и столбца с номером u_{k+1}, положителен.

Если элемент матрицы

$$F_{\rho_1}^{\rho_2}(C_1) \cdot F_{\rho_2}^{\rho_3}(C_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(C_k),$$

стоящий на пересечении строки с номером u_1 и столбца с номером u_{k+1}, положителен, то найдутся $u_i \in \tilde{\rho}_i$, $i \in \overline{2,k}$, со свойствами $f_{u_j,u_{j+1}}(C_j) > 0$ для всех $j \in \overline{1,k}$. Тогда существуют векторы $\bar{a}_2, \bar{a}_3, \ldots, \bar{a}_{k+1}, \bar{b}_1, \bar{b}_2, \ldots, \bar{b}_k \in \Omega^{[l]}$ и подстановки $h_j \in C_j$, $j \in \overline{1,k}$, такие что

$$\bar{b}_1 \in \tilde{\rho}_1(u_1); \quad \bar{a}_i, \bar{b}_i \in \tilde{\rho}_i(u_i), \quad i \in \overline{2,k};$$
$$\bar{a}_{k+1} \in \tilde{\rho}_{k+1}(u_{k+1}); \quad h_j(\bar{b}_j) = \bar{a}_{j+1}, \quad j \in \overline{1,k}.$$

Так как для каждого $i \in \overline{2,k}$ выполняется $\bar{a}_i \ \rho_i \ \bar{b}_i$ и A_i — ρ_i-отмеченное множество, найдётся подстановка $g_i \in A_i$ со свойством $g_i(\bar{a}_i) = \bar{b}_i$. Суммируя сказанное выше, получаем $h_1 g_2 h_2 \ldots g_k h_k(\bar{b}_1) = \bar{a}_{k+1}$, причём $\bar{b}_1 \in \tilde{\rho}_1(u_1)$, $\bar{a}_{k+1} \in \in \tilde{\rho}_{k+1}(u_{k+1})$. Это означает, что элемент матрицы

$$\overline{(P_l(\Re(B_1, B_2, \ldots, B_k)))},$$

стоящий на пересечении строки с номером u_1 и столбца с номером u_{k+1}, равен единице. □

Следствие 7. *В условиях теоремы множество $\Re(B_1, B_2, \ldots, B_k)$ l-транзитивно тогда и только тогда, когда матрица $F_{\rho_1}^{\rho_2}(B_1) \cdot F_{\rho_2}^{\rho_3}(B_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(B_k)$ не содержит нулевых элементов.*

Доказательство. l-транзитивность множества $\Re(B_1, B_2, \ldots, B_k)$ равносильна отсутствию нулей в матрице $P_l(\Re(B_1, B_2, \ldots, B_k))$, т. е. отсутствию нулевых элементов в матрице $F_{\rho_1}^{\rho_2}(B_1) \cdot F_{\rho_2}^{\rho_3}(B_2) \cdot \ldots \cdot F_{\rho_k}^{\rho_{k+1}}(B_k)$. □

Эффективное применение способа обоснования кратной транзитивности произведения множеств подстановок, предложенного в теореме 6, требует знания ряда свойств используемых отношений эквивалентности.

1. Число классов, на которые множество $\Omega^{[l]}$ разбивается отношением эквивалентности, характеризует размеры редуцированных матриц, а следовательно, и сложность их умножения.
2. «Удобная» нумерация классов и «легко проверяемый» критерий принадлежности вектора классу эквивалентности с данным номером весьма полезны при построении матриц $F_{\rho}^{\eta}(B)$.
3. Описание (для используемого отношения эквивалентности ρ) максимального ρ-отмеченного множества — группы $S(\Omega, \rho)$ — позволяет получить информацию о строении любого ρ-отмеченного мультимножества.

Рассмотрим с точки зрения упомянутых свойств отношения эквивалентности $\rho(l, G)$, построенные для различных натуральных чисел l и групп G, допускающих эффективную реализацию на современной элементной базе.

1. Точно кратно транзитивные группы

Пусть m — натуральное число. Напомним, что группа подстановок G на множестве Ω называется точно m-транзитивной [9], если для любых $\bar{a}, \bar{b} \in \Omega^{[m]}$ существует единственная подстановка $h \in G$ со свойством $h(\bar{a}) = \bar{b}$.

Утверждение 8. *Пусть G — точно m-транзитивная подгруппа группы $S(\Omega)$, $l > m$, $\rho = \rho(l, G)$. Тогда*

1) *мощность любого класса ρ-эквивалентных элементов равна*

$$|\Omega|(|\Omega| - 1) \dots (|\Omega| - m + 1);$$

2) *множество $\Omega^{[l]}$ разбивается на*

$$(|\Omega| - m)(|\Omega| - m - 1) \dots (|\Omega| - l + 1)$$

классов ρ-эквивалентных элементов;

3) $S(\Omega, \rho) = G$.

Доказательство. 1. Из определения точной m-транзитивности следует, что мощность класса ρ-эквивалентных элементов, содержащего вектор $\bar{a} \in \Omega^{[l]}$, равна $|\{g(\bar{a}) \mid g \in G\}| = |G|$. Осталось заметить, что $|G| = |\Omega|(|\Omega|-1) \dots (|\Omega|-m+1)$ (см. [9]).

2. Так как все классы ρ-эквивалентных элементов равномощны, то их число равно

$$\frac{|\Omega^{[l]}|}{|\Omega|(|\Omega| - 1) \dots (|\Omega| - m + 1)} = (|\Omega| - m)(|\Omega| - m - 1) \dots (|\Omega| - l + 1).$$

3. Включение $G \subseteq S(\Omega, \rho)$ очевидно. Пусть $h \in S(\Omega, \rho)$ и

$$\bar{a} = (a_1, \dots, a_m, a_{m+1}, \dots, a_{l-1}, a_l) \in \Omega^{[l]}.$$

Тогда $\bar{a}\ \rho\ h(\bar{a})$ и существует подстановка $g \in G$, такая что $g(\bar{a}) = h(\bar{a})$. Покажем, что $g = h$. Это будет означать, что $S(\Omega, \rho) \subseteq G$. Иными словами, покажем, что для любого элемента $c \in \Omega$ справедливо равенство $g(c) = h(c)$. Если $c \in \{a_1, \dots, a_l\}$, то этот факт очевиден. В противном случае рассмотрим l-грамму $\bar{a}' = (a_1, \dots, a_m, a_{m+1}, \dots, a_{l-1}, c)$. Как и ранее, существует подстановка $g' \in G$ со свойством $g'(\bar{a}') = h(\bar{a}')$. Тогда

$$g'(a_1, \dots, a_m) = h(a_1, \dots, a_m) = g(a_1, \dots, a_m)$$

и из точной m-транзитивности группы G следует равенство $g' = g$, откуда имеем $g(c) = h(c)$. □

Пусть G — точно 1-транзитивная (регулярная) группа. Зафиксируем элемент $e \in \Omega$ и зададим на множестве Ω операцию $\circ$ равенством $a \circ b = g_b(a)$, где g_b — единственная подстановка группы G, удовлетворяющая условию $g_b(e) = b$. Тогда $(\Omega; \circ)$ — группа с единицей e и G — правое регулярное представление группы $(\Omega; \circ)$. Хорошо известно следующее утверждение.

Утверждение 9. *Пусть G — правое регулярное представление группы $(\Omega;\circ)$. Тогда векторы $\bar a=(a_1,a_2,\dots,a_l)$ и $\bar b=(b_1,b_2,\dots,b_l)$ из $\Omega^{[l]}$ $\rho(l,G)$-эквивалентны в том и только в том случае, когда для любого $i\in\overline{1,l-1}$ справедливо равенство $a_i\circ a_l^{-1}=b_i\circ b_l^{-1}$.*

Доказательство. По определению отношения $\rho(l,G)$ эквивалентность векторов $\bar a$ и $\bar b$ равносильна существованию такого элемента $c\in\Omega$, что $a_i\circ c=b_i$ для всех $i\in\overline{1,l}$. Следовательно, $c=a_l^{-1}\circ b_l$ и соотношение $\bar a\rho(l,G)\bar b$ имеет место тогда и только тогда, когда $a_i\circ a_l^{-1}\circ b_l=b_i$, $i\in\overline{1,l-1}$, т. е. когда $a_i\circ a_l^{-1}=b_i\circ b_l^{-1}$, $i\in\overline{1,l-1}$. □

Утверждение 9 позволяет эффективно занумеровать классы $\rho(l,G)$-эквивалентных векторов элементами множества $(\Omega\setminus\{e\})^{[l-1]}$ и считать, что вектор $\bar a=(a_1,a_2,\dots,a_l)$ лежит в классе с номером $(c_1,c_2,\dots,c_{l-1})$ тогда и только тогда, когда $a_i\circ a_l^{-1}=c_i$ для всех $i\in\overline{1,l-1}$.

Точно 2-транзитивные группы, отличные от симметрической и знакопеременной, имеют примарную степень. Их можно рассматривать как группы аффинных преобразований конечного поля (см. [9]). Итак, пусть на множестве Ω задана структура конечного поля $P=(\Omega;+,\cdot)$ и

$$\mathrm{AGL}(P)=\left\{\begin{pmatrix}x\\ux+v\end{pmatrix}\;\middle|\;u,v\in P,\ u\neq0\right\}.$$

Утверждение 10. *Пусть на множестве Ω задана структура конечного поля $P=(\Omega;+,\cdot)$, $\rho=\rho(3,\mathrm{AGL}(P))$. Тогда векторы $\bar a=(a_1,a_2,a_3)$ и $\bar b=(b_1,b_2,b_3)$ из $\Omega^{[3]}$ ρ-эквивалентны в том и только в том случае, когда*

$$(a_1-a_2)\cdot(a_1-a_3)^{-1}=(b_1-b_2)\cdot(b_1-b_3)^{-1}.$$

Доказательство. Если $\bar a\,\rho\,\bar b$, то найдутся такие $u,v\in P$, $u\neq0$, что

$$\begin{cases}ua_1+v=b_1,\\ua_2+v=b_2,\\ua_3+v=b_3.\end{cases}$$

Тогда

$$u=(a_1-a_2)^{-1}\cdot(b_1-b_2)=(a_1-a_3)^{-1}\cdot(b_1-b_3)$$

и, следовательно,

$$(a_1-a_2)\cdot(a_1-a_3)^{-1}=(b_1-b_2)\cdot(b_1-b_3)^{-1}.$$

С другой стороны, если $(a_1-a_2)\cdot(a_1-a_3)^{-1}=(b_1-b_2)\cdot(b_1-b_3)^{-1}$, то, положив $u=(a_1-a_2)^{-1}\cdot(b_1-b_2)$ и $v=b_1-ua_1$, имеем $u\neq0$ и

$$\begin{cases}ua_1+v=b_1,\\ua_2+v=b_2,\\ua_3+v=b_3,\end{cases}$$

т. е. триграммы $\bar a\,\rho\,\bar b$. □

Утверждение 10 даёт возможность занумеровать классы $\rho(3, \mathrm{AGL}(P))$-эквивалентных векторов элементами множества $\Omega \setminus \{0, e\}$ и считать, что вектор $\bar{a} = (a_1, a_2, a_3)$ лежит в классе с номером d тогда и только тогда, когда $(a_1 - a_2) \cdot (a_1 - a_3)^{-1} = d$.

2. Группы аффинных и линейных преобразований конечного коммутативного кольца с единицей

Пусть на множестве Ω задана структура конечного коммутативного кольца $R = (\Omega; +, \cdot)$ с единицей, R^* — мультипликативная группа этого кольца. Через

$$\mathrm{AGL}(R) = \left\{ \begin{pmatrix} x \\ ux + v \end{pmatrix} \;\middle|\; u \in R^*,\ v \in R \right\}, \quad \mathrm{GL}(R) = \left\{ \begin{pmatrix} x \\ ux \end{pmatrix} \;\middle|\; u \in R^* \right\}$$

обозначим группы аффинных и линейных преобразований кольца R.

Утверждение 11. *Пусть на множестве Ω задана структура конечного коммутативного кольца R с единицей, $\rho = \rho(2, \mathrm{AGL}(R))$. Тогда*

1) *векторы $\bar{a} = (a_1, a_2)$ и $\bar{b} = (b_1, b_2)$ из $\Omega^{[2]}$ ρ-эквивалентны тогда и только тогда, когда главные идеалы кольца R, порождённые $a_1 - a_2$ и $b_1 - b_2$, совпадают*;
2) *число классов, на которые множество $\Omega^{[2]}$ разбивается отношением ρ, равно числу ненулевых главных идеалов кольца R.*

Доказательство. Если $\bar{a}\ \rho\ \bar{b}$, то существуют такие $u \in R^*$, $v \in R$, что

$$\begin{cases} ua_1 + v = b_1, \\ ua_2 + v = b_2. \end{cases}$$

Тогда $u(a_1 - a_2) = b_1 - b_2$ и, следовательно, $(a_1 - a_2)R = (b_1 - b_2)R$.

С другой стороны, если $(a_1 - a_2)R = (b_1 - b_2)R$, то существует такой элемент $w \in R$, что $w(a_1 - a_2) = b_1 - b_2$. Покажем, что w можно выбрать обратимым. Тогда, положив $v = b_1 - wa_1 = b_2 - wa_2$, имеем

$$\begin{cases} wa_1 + v = b_1, \\ wa_2 + v = b_2, \end{cases}$$

т. е. $\bar{a}\ \rho\ \bar{b}$.

Так как R — конечное коммутативное кольцо с единицей, то оно либо локальное, либо раскладывается в прямую сумму локальных коммутативных колец с единицей (см., например, [4]).

Пусть R — локальное кольцо. Из равенства $(a_1 - a_2)R = (b_1 - b_2)R$ вытекает существование элемента $w_1 \in R$ со свойством $a_1 - a_2 = w_1(b_1 - b_2)$. Тогда $(e - ww_1)(a_1 - a_2) = 0$, где e — единица кольца R. Так как $a_1 - a_2 \neq 0$, то $e - ww_1$ — делитель нуля или $e - ww_1 = 0$. Поэтому $ww_1 \in R^*$ (см. [4]) и, следовательно, $w \in R^*$.

Пусть

$$R = R_1 \dot{+} \ldots \dot{+} R_m -$$

прямая сумма локальных колец и

$$e = e^{(1)} + \ldots + e^{(m)},$$

где $e^{(i)} \in R_i$, $i \in \overline{1,m}$. Тогда для всех $i \in \overline{1,m}$ $e^{(i)}$ — единица кольца R_i. Если $a_1 - a_2 = a^{(1)} + \ldots + a^{(m)}$ и $b_1 - b_2 = b^{(1)} + \ldots + b^{(m)}$, где $a^{(i)}, b^{(i)} \in R_i$, $i \in \overline{1,m}$, то условие $(a_1 - a_2)R = (b_1 - b_2)R$ равносильно системе равенств $a^{(i)}R_i = b^{(i)}R_i$, $i \in \overline{1,m}$. Для каждого $i \in \overline{1,m}$ выберем в кольце R_i элемент $w^{(i)}$ следующим образом. Если $a^{(i)} = 0$, то $b^{(i)} = 0$ и положим $w^{(i)} = e^{(i)}$. Если $a^{(i)} \neq 0$, то воспользуемся тем, что R_i — локальное конечное коммутативное кольцо с единицей. По доказанному выше из равенства $a^{(i)}R_i = b^{(i)}R_i$ вытекает существование элемента $w^{(i)} \in R_i^*$ со свойством $w^{(i)}a^{(i)} = b^{(i)}$. Тогда, положив $w = w^{(1)} + \ldots + w^{(m)}$, имеем $w \in R^*$ и $w(a_1 - a_2) = b_1 - b_2$.

Второй пункт очевиден. □

Утверждение 12. *Пусть на множестве Ω задана структура конечного коммутативного кольца R с единицей, $\rho = \rho(1, \mathrm{GL}(R))$. Тогда*

1) *элементы a и b множества Ω ρ-эквивалентны тогда и только тогда, когда $aR = bR$;*
2) *число классов, на которые множество Ω разбивается отношением ρ, равно числу главных идеалов кольца R.*

Доказательство. Если $a = 0$, то элементы a и b ρ-эквивалентны тогда и только тогда, когда $b = 0$, т. е. когда $aR = bR = \{0\}$.

Пусть $a \neq 0$. Тогда $b \neq 0$ и элементы a и b ρ-эквивалентны тогда и только тогда, когда векторы $\bar{a} = (a, 0)$ и $\bar{b} = (b, 0)$ $\rho(2, \mathrm{AGL}(R))$-эквивалентны. Последнее ввиду п. 1 утверждения 11 равносильно равенству $aR = bR$.

Второй пункт очевиден. □

3. Группы аффинных и линейных преобразований кольца Галуа

Следуя [4, 8], под кольцом Галуа будем понимать конечное коммутативное кольцо R с единицей, множество делителей нуля которого имеет вид pR, где p — простое число. В таком случае R — локальное кольцо главных идеалов, характеристика которого равна p^n (n — натуральное число), а мощность q^n, где q — число элементов в поле вычетов $\bar{R} = R/pR$. Множество идеалов кольца R образует цепь

$$R \supset pR \supset p^2R \supset \ldots \supset p^{n-1}R \supset p^nR = \{0\}.$$

Кольцо Галуа однозначно с точностью до изоморфизма определяется числом элементов и характеристикой и обозначается $\mathrm{GR}(q^n, p^n)$. Важными примерами колец Галуа являются конечные поля $\mathrm{GF}(q) = \mathrm{GR}(q, p)$ и кольца вычетов

по примарному модулю $\mathbb{Z}/p^n\mathbb{Z} = \mathrm{GR}(p^n, p^n)$. Фактор-кольцо кольца Галуа по любому его идеалу также является кольцом Галуа, в частности $R/p^{n-1}R = \mathrm{GR}(q^{n-1}, p^{n-1})$.

Норму $\|a\|$ элемента $a \in R$ определим равенством

$$\|a\| = \max\{i \mid a \in p^i R,\ 0 \leqslant i \leqslant n\}.$$

Пусть $\ddot{R}$ — подмножество кольца R, удовлетворяющее условиям $|\ddot{R}| = q$ и $\tau(\ddot{R}) = \bar{R}$, где τ — естественный эпиморфизм R на $\bar{R}$. Согласно [5] эти условия равносильны тому, что любой элемент $a \in R$ однозначно представи́м в виде

$$a = p^{n-1}\delta_{n-1}(a) + \ldots + p\delta_1(a) + \delta_0(a),$$

где $\delta_i(a) \in \ddot{R}$, $i \in \overline{0, n-1}$.

Утверждение 13. *Пусть на множестве Ω задана структура кольца Галуа $R = \mathrm{GR}(q^n, p^n)$, $\rho = \rho(2, \mathrm{AGL}(R))$. Тогда*

1) *векторы $\bar{a} = (a_1, a_2)$ и $\bar{b} = (b_1, b_2)$ из $\Omega^{[2]}$ ρ-эквивалентны тогда и только тогда, когда $\|a_1 - a_2\| = \|b_1 - b_2\|$;*
2) *множество $\Omega^{[2]}$ разбивается отношением ρ на n классов эквивалентности;*
3) $|S(\Omega, \rho)| = (q!)^{\frac{q^n-1}{q-1}}$;
4) *если $q = 2$, то $S(\Omega, \rho)$ — силовская 2-подгруппа группы $S(\Omega)$.*

Доказательство. Для доказательства пунктов 1, 2 заметим, что если $\|a\| = i$, то a порождает главный идеал $p^i R$. Осталось воспользоваться утверждением 11 и свойствами кольца Галуа.

Доказательство п. 3 проведём индукцией по n.

Если $n = 1$, то $R = \mathrm{GR}(q, p)$ — поле, которое не имеет собственных идеалов. Тогда $S(\Omega, \rho) = S(\Omega)$ и $|S(\Omega, \rho)| = q!$.

Пусть формула верна для любого кольца Галуа характеристики p^n, где p — произвольное простое число и $1 \leqslant n \leqslant m$, и пусть $n = m + 1$. Наряду с кольцом R и отношением ρ рассмотрим кольцо Галуа $R' = R/p^m R = \mathrm{GR}(q^m, p^m)$, структура которого задана на множестве Ω', и отношение $\rho' = \rho(2, \mathrm{AGL}(R'))$.

Пусть $h \in S(\Omega, \rho)$. Из определения группы $S(\Omega, \rho)$ и п. 1 следует, что для любых элементов $a, b \in \Omega$ принадлежность $b - a \in p^m R$ всегда влечёт принадлежность $h(b) - h(a) \in p^m R$. Иными словами, если $b \in a + p^m R$, то $h(b) \in h(a) + p^m R$. Поэтому для любого элемента $a \in \Omega$ справедливо равенство $h(a + p^m R) = h(a) + p^m R$. Теперь можно корректно определить отображение $\psi\colon S(\Omega, \rho) \to S(\Omega', \rho')$. Для любого смежного класса $a + p^m R \in R/p^m R$ положим $\psi(h)(a + p^m R) = h(a) + p^m R$. Воспользовавшись свойствами отношений ρ и ρ', несложно проверить, что $\psi(h)$ — подстановка из $S(\Omega', \rho')$.

Отображение ψ сюръективно, так как для любой подстановки $g' \in S(\Omega', \rho')$ существует прообраз $g \in \psi^{-1}(g')$, определяемый следующим образом. Для каждого класса $a + p^m R \in R/p^m R$ зафиксируем элемент $b \in g'(a + p^m R)$ и, если $c \in a + p^m R$, положим $g(c) = b + p^m \delta_m(c)$. Нетрудно видеть, что g — подстановка из $S(\Omega, \rho)$ и $\psi(g) = g'$.

Кроме того, ψ — гомоморфизм, так как для любых подстановок $g, h \in S(\Omega, \rho)$ и любого элемента $a \in \Omega$ справедлива цепочка равенств

$$\psi(gh)(a + p^m R) = h(g(a)) + p^m R = \psi(h)(g(a) + p^m R) = \\ = \psi(h)(\psi(g)(a + p^m R)) = (\psi(g)\psi(h))(a + p^m R).$$

Таким образом, ψ — эпиморфизм. Его ядро $\operatorname{Ker}\psi$ состоит из всех подстановок $h \in S(\Omega, \rho)$, таких что для любого элемента $a \in \Omega$ справедливо равенство $h(a + p^m R) = a + p^m R$. Так как $|p^m R| = q$, то указанных подстановок ровно $|\operatorname{Ker}\psi| = (q!)^{q^m}$, и по теореме об эпиморфизме групп имеем

$$|S(\Omega, \rho)| = |S(\Omega', \rho')| \cdot |\operatorname{Ker}\psi| = (q!)^{\frac{q^m - 1}{q-1}} \cdot (q!)^{q^m} = (q!)^{\frac{q^{m+1}-1}{q-1}}.$$

Докажем пункт 4. Если $q = 2$, то $|S(\Omega, \rho)| = 2^{2^n - 1}$ — максимальная степень числа 2, делящая $|S(\Omega)| = (2^n)!$. Следовательно, $S(\Omega, \rho) = G$ — силовская 2-подгруппа группы $S(\Omega)$. □

Для любого ненулевого элемента $a \in \Omega$ положим

$$\vartheta(a) = \delta_{\|a\|}(a) + p\delta_{\|a\|+1}(a) + \ldots + p^{n-1-\|a\|}\delta_{n-1}(a).$$

Утверждение 14. *Пусть на множестве Ω задана структура кольца Галуа $R = \mathrm{GR}(q^n, p^n)$ с единицей e, $\rho = \rho(3, \mathrm{AGL}(R))$. Тогда*

1) *векторы $\bar{a} = (a_1, a_2, a_3)$ и $\bar{b} = (b_1, b_2, b_3)$ из $\Omega^{[3]}$ ρ-эквивалентны тогда и только тогда, когда $\|a_1 - a_3\| = \|b_1 - b_3\|$, $\|a_2 - a_3\| = \|b_2 - b_3\|$ и*

$$\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} - \vartheta(b_1 - b_3)\vartheta(b_2 - b_3)^{-1} \in p^m R,$$

где $m = n - \max\{\|a_1 - a_3\|, \|a_2 - a_3\|\}$;

2) *для любых $i, j \in \overline{0, n-1}$ и $d \in \Omega$ вектор $\bar{a} = (a_1, a_2, a_3) \in \Omega^{[3]}$, удовлетворяющий условиям*

$$\|a_1 - a_3\| = i, \quad \|a_2 - a_3\| = j, \quad p^{\max\{i,j\}}\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} = d,$$

существует тогда и только тогда, когда $\|d\| = \max\{i, j\}$ и либо $i \neq j$, либо $i = j$ и $d \neq p^{\max\{i,j\}} \cdot e$.

Доказательство. 1. Если $\bar{a}\ \rho\ \bar{b}$, то существуют элементы $u \in R^*$, $v \in R$, такие что

$$\begin{cases} ua_1 + v = b_1, \\ ua_2 + v = b_2, \\ ua_3 + v = b_3. \end{cases}$$

Тогда

$$\begin{cases} u(a_1 - a_3) = (b_1 - b_3), \\ u(a_2 - a_3) = (b_2 - b_3). \end{cases} \qquad (*)$$

Так как $u \in R^*$, то $\|a_1 - a_3\| = \|b_1 - b_3\|$, $\|a_2 - a_3\| = \|b_2 - b_3\|$ и равенства $(*)$ можно переписать в виде

$$\begin{cases} p^{\|a_1-a_3\|}u \cdot \vartheta(a_1 - a_3) = p^{\|a_1-a_3\|}\vartheta(b_1 - b_3), \\ p^{\|a_2-a_3\|}u \cdot \vartheta(a_2 - a_3) = p^{\|a_2-a_3\|}\vartheta(b_2 - b_3). \end{cases}$$

Поэтому

$$\begin{cases} p^{\|a_1-a_3\|}u = p^{\|a_1-a_3\|}\vartheta(b_1 - b_3) \cdot \vartheta(a_1 - a_3)^{-1}, \\ p^{\|a_2-a_3\|}u = p^{\|a_2-a_3\|}\vartheta(b_2 - b_3) \cdot \vartheta(a_2 - a_3)^{-1}. \end{cases}$$

Отсюда вытекает, что

$$p^{n-m}(\vartheta(b_2 - b_3)\vartheta(a_2 - a_3)^{-1} - \vartheta(b_1 - b_3)\vartheta(a_1 - a_3)^{-1}) = 0.$$

Следовательно,

$$p^{n-m}(\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} - \vartheta(b_1 - b_3)\vartheta(b_2 - b_3)^{-1}) = 0,$$

т. е.

$$\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} - \vartheta(b_1 - b_3)\vartheta(b_2 - b_3)^{-1} \in p^m R.$$

С другой стороны, если $\|a_1 - a_3\| = \|b_1 - b_3\|$, $\|a_2 - a_3\| = \|b_2 - b_3\|$ и $\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} - \vartheta(b_1 - b_3)\vartheta(b_2 - b_3)^{-1} \in p^m R$, то, положив

$$u = \begin{cases} \vartheta(b_1 - b_3) \cdot \vartheta(a_1 - a_3)^{-1}, & \text{если } \|a_1 - a_3\| \leqslant \|a_2 - a_3\|, \\ \vartheta(b_2 - b_3) \cdot \vartheta(a_2 - a_3)^{-1}, & \text{если } \|a_1 - a_3\| > \|a_2 - a_3\| \end{cases}$$

и $v = b_1 - ua_1$, имеем $u \in R^*$ и справедливы равенства $(*)$, т. е. $\bar{a}\ \rho\ \bar{b}$.

2. Пусть вектор $\bar{a} \in \Omega^{[3]}$ удовлетворяет условиям $\|a_1 - a_3\| = i$, $\|a_2 - a_3\| = j$ и $p^{\max\{i,j\}}\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} = d$. Так как

$$\|\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1}\| = 0,$$

то $\|d\| = \max\{i, j\}$.

Если $i = j$, то предположим противное, а именно пусть $d = p^i \cdot e$. Тогда $\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} \in e + p^{n-i}R$, или, иначе, $\vartheta(a_1 - a_3) \in \vartheta(a_2 - a_3) + p^{n-i}R$. Отсюда следует, что $p^i\vartheta(a_1 - a_3) = p^i\vartheta(a_2 - a_3)$, т. е. $a_1 - a_3 = a_2 - a_3$, и $a_1 = a_2$. Получаем противоречие.

Докажем обратное утверждение. Пусть $j \leqslant i$, $\|d\| = i$ и $d \neq p^i \cdot e$ в случае $i = j$. Равенства $\|a_2 - a_3\| = j$ и $p^i\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} = d$ равносильны системе соотношений

$$\begin{cases} \delta_0(a_2) = \delta_0(a_3), \\ \quad \vdots \\ \delta_{j-1}(a_2) = \delta_{j-1}(a_3), \\ \delta_j(a_2) \neq \delta_j(a_3), \\ a_1 - a_3 = d \cdot \vartheta(a_2 - a_3). \end{cases}$$

При этом любой вектор $\bar{a} = (a_1, a_2, a_3)$, удовлетворяющий этим соотношениям, лежит в $\Omega^{[3]}$. Кроме того, так как $\|d\| = i$, то $\|a_1 - a_3\| = i$. Поэтому количество таких векторов из $\Omega^{[3]}$ равно $(q-1)q^{2n-j-1} > 0$. Случай $i < j$ рассматривается аналогично. □

Утверждение 14 позволяет эффективно занумеровать классы $\rho(3,\mathrm{AGL}(R))$-эквивалентных векторов элементами множества

$$\big\{(i,j,d) \mid i,j \in \overline{0,n-1},\ d \in \Omega,\ \|d\| = \max\{i,j\}\big\} \setminus \big\{(i,i,p^i \cdot e) \mid i \in \overline{0,n-1}\,\big\}$$

и считать, что вектор $\bar{a} = (a_1, a_2, a_3)$ лежит в классе с номером (i,j,d) тогда и только тогда, когда

$$\|a_1 - a_3\| = i, \quad \|a_2 - a_3\| = j, \quad p^{\max\{i,j\}}\vartheta(a_1 - a_3)\vartheta(a_2 - a_3)^{-1} = d.$$

Следствие 15. *В условиях утверждения*14 *множество* $\Omega^{[3]}$ *разбивается отношением* $\rho(3, \mathrm{AGL}(R))$ *на* $\frac{1}{q-1}(q^{n+1} + q^n - q(3n+1) + 3n - 1)$ *классов эквивалентности.* □

Из определения ρ-отмеченного множества следует, что максимальным таким множеством является группа $S(\Omega, \rho)$. Для случая $\rho = \rho(2, \mathrm{AGL}(R))$ изучим свойства отношения $\rho(l, S(\Omega, \rho))$.

Утверждение 16. *Пусть на множестве* Ω *задана структура кольца Галуа* $R = \mathrm{GR}(q^n, p^n)$, $\rho = \rho(2, \mathrm{AGL}(R))$, $G = S(\Omega, \rho)$. *Тогда*

1) *векторы* $\bar{a} = (a_1, a_2, \ldots, a_l)$ *и* $\bar{b} = (b_1, b_2, \ldots, b_l)$ *из* $\Omega^{[l]}$ $\rho(l, G)$*-эквивалентны в том и только в том случае, когда для любых* $i, j \in \overline{1,l}$ *справедливо равенство* $\|a_i - a_j\| = \|b_i - b_j\|$;
2) *для любых* $i_1, i_2, i_3 \in \overline{0,n-1}$ *вектор* $\bar{a} = (a_1, a_2, a_3) \in \Omega^{[3]}$, *удовлетворяющий условиям* $\|a_1 - a_2\| = i_1$, $\|a_1 - a_3\| = i_2$ *и* $\|a_2 - a_3\| = i_3$, *существует тогда и только тогда, когда*

$$|\{j \mid i_j = \min\{i_1, i_2, i_3\}\}| = \begin{cases} 2 \text{ или } 3, & \text{если } q > 2, \\ 2, & \text{если } q = 2. \end{cases}$$

Доказательство. 1. Пусть $\bar{a}\ \rho(l,G)\ \bar{b}$, т. е. существует подстановка $h \in G$ со свойством $h(\bar{a}) = \bar{b}$, и пусть $i, j \in \overline{1,l}$. Если $i = j$, то равенство $\|a_i - a_j\| = \|b_i - b_j\|$ очевидно. Если $i \neq j$, то $h(a_i, a_j) = (b_i, b_j)$ и по определению группы $S(\Omega, \rho)$ векторы (a_i, a_j) и (b_i, b_j) ρ-эквивалентны. Следовательно, по утверждению 13 $\|a_i - a_j\| = \|b_i - b_j\|$.

Проведём доказательство в обратную сторону. Докажем следующее более общее утверждение: для любых векторов $\bar{a} = (a_1, a_2, \ldots, a_l)$ и $\bar{b} = (b_1, b_2, \ldots, b_l)$ с координатами из Ω, таких что для всех $i, j \in \overline{1,l}$ справедливо равенство $\|a_i - a_j\| = \|b_i - b_j\|$, найдётся подстановка $g \in G$ со свойством $g(\bar{a}) = \bar{b}$. Проведём индукцию по n.

Если $n = 1$, то $S(\Omega, \rho) = S(\Omega)$ и существование нужной подстановки очевидно.

Пусть для любого кольца Галуа характеристики p^n, где p — произвольное простое число и $1 \leqslant n \leqslant m$, и для любых векторов $\bar{a} = (a_1, a_2, \ldots, a_l)$ и $\bar{b} = (b_1, b_2, \ldots, b_l)$ со свойством $\|a_i - a_j\| = \|b_i - b_j\|$, $i, j \in \overline{1,l}$, найдётся такая подстановка $g \in G$, что $g(\bar{a}) = \bar{b}$.

Пусть $n = m + 1$. Как и в доказательстве утверждения 13, положим $R' = R/p^m R = \mathrm{GR}(q^m, p^m)$, $\rho' = \rho(2, \mathrm{AGL}(R'))$, Ω' — множество элементов кольца R'. Наряду с векторами $\bar{a} = (a_1, a_2, \ldots, a_l)$ и $\bar{b} = (b_1, b_2, \ldots, b_l)$ (с координатами из Ω), удовлетворяющими условию доказываемого утверждения, рассмотрим векторы

$$\bar{a}' = (a_1 + p^m R, a_2 + p^m R, \ldots, a_l + p^m R),$$
$$\bar{b}' = (b_1 + p^m R, b_2 + p^m R, \ldots, b_l + p^m R)$$

с координатами из Ω'. Очевидно, что в кольце R' для любых $i, j \in \overline{1,l}$ справедливо равенство

$$\|(a_i + p^m R) - (a_j + p^m R)\| = \|(b_i + p^m R) - (b_j + p^m R)\|.$$

Тогда по предположению индукции существует такая подстановка $h' \in S(\Omega', \rho')$, что $h'(\bar{a}') = \bar{b}'$. Пусть, как и в доказательстве утверждения 13,

$$\psi\colon S(\Omega, \rho) \to S(\Omega', \rho') -$$

эпиморфизм групп, определяемый равенством $\psi(h)(a + p^m R) = h(a) + p^m R$, и пусть $h \in \psi^{-1}(h')$. Тогда по определению отображения ψ вектор $\bar{c} = h(\bar{a}) = (c_1, c_2, \ldots, c_l)$ удовлетворяет условиям $c_i \in b_i + p^m R$, $i \in \overline{1,l}$. Так как h — подстановка, то равенство $a_i = a_j$ равносильно равенству $c_i = c_j$. Из описания ядра отображения ψ в доказательстве утверждения 13 следует, что найдётся подстановка $h_1 \in \mathrm{Ker}\,\psi$ со свойством $h_1(\bar{c}) = \bar{b}$. Тогда, положив $g = h \cdot h_1$, имеем $g(\bar{a}) = \bar{b}$.

2. Пусть вектор $\bar{a} = (a_1, a_2, a_3) \in \Omega^{[3]}$ удовлетворяет условиям

$$\|a_1 - a_2\| = i_1, \quad \|a_1 - a_3\| = i_2, \quad \|a_2 - a_3\| = i_3.$$

Если $i_1 > i_2$, то из равенств $\|a_1 - a_2\| = i_1$ и $\|a_1 - a_3\| = i_2$ вытекает система соотношений

$$\begin{cases} \delta_0(a_1) = \delta_0(a_2) = \delta_0(a_3), \\ \quad \vdots \\ \delta_{i_2-1}(a_1) = \delta_{i_2-1}(a_2) = \delta_{i_2-1}(a_3), \\ \delta_{i_2}(a_1) = \delta_{i_2}(a_2) \neq \delta_{i_2}(a_3), \end{cases}$$

а тогда $\|a_2 - a_3\| = i_2 = i_3$.

В случае $i_1 = i_2$ условия $\|a_1 - a_2\| = i_1$ и $\|a_1 - a_3\| = i_2$ равносильны тому, что

$$\begin{cases} \delta_0(a_1) = \delta_0(a_2) = \delta_0(a_3), \\ \quad \vdots \\ \delta_{i_2-1}(a_1) = \delta_{i_2-1}(a_2) = \delta_{i_2-1}(a_3), \\ \delta_{i_2}(a_1) \neq \delta_{i_2}(a_2), \\ \delta_{i_2}(a_1) \neq \delta_{i_2}(a_3), \end{cases}$$

т. е. $i_3 \geqslant i_2$. Если при этом $q = 2$, то $\delta_{i_2}(a_2) = \delta_{i_2}(a_3)$.

Случай $i_1 < i_2$ рассматривается аналогично случаю $i_1 > i_2$.

Докажем обратное утверждение. Пусть $|\{j \mid i_j = \min\{i_1, i_2, i_3\}\}| = 2$. Без ограничения общности можно считать, что $i_1 = i_2 < i_3$. Тогда в качестве искомого вектора достаточно взять $\bar{a} = (p^{i_1}e, p^{i_3}e, 0)$, где e — единица кольца R. Если $q > 2$ и $i_1 = i_2 = i_3$, положим $\bar{a} = (p^{i_1}e, p^{i_1}b, 0)$, где b — обратимый элемент кольца R, удовлетворяющий условию $\delta_0(b) \neq \delta_0(e)$. □

Теперь ясно, что классы $\rho(3, G)$-эквивалентных векторов можно в случае $q = 2$ занумеровать элементами множества

$$\big\{(i_1, i_2, i_3) \mid i_1, i_2, i_3 \in \overline{0, n-1},\ \big|\{j \mid i_j = \min\{i_1, i_2, i_3\}\}\big| = 2\big\},$$

а в случае $q > 2$ — элементами множества

$$\big\{(i_1, i_2, i_3) \mid i_1, i_2, i_3 \in \overline{0, n-1},\ \big|\{j \mid i_j = \min\{i_1, i_2, i_3\}\}\big| \geqslant 2\big\}.$$

При этом вектор $\bar{a} = (a_1, a_2, a_3)$ лежит в классе с номером (i_1, i_2, i_3) тогда и только тогда, когда $\|a_1 - a_2\| = i_1$, $\|a_1 - a_3\| = i_2$ и $\|a_2 - a_3\| = i_3$.

Следствие 17. *В условиях утверждения* 16 *множество* $\Omega^{[3]}$ *разбивается отношением* $\rho(3, G)$ *в случае* $q = 2$ *на* $\frac{3n(n-1)}{2}$ *классов эквивалентности, а в случае* $q > 2$ *на* $\frac{n(3n-1)}{2}$ *классов.* □

Из свойств кольца Галуа и утверждения 12 вытекает утверждение 18.

Утверждение 18. *Пусть на множестве* Ω *задана структура кольца Галуа* $R = \mathrm{GR}(q^n, p^n)$, $\rho = \rho(1, \mathrm{GL}(R))$. *Тогда*

1) *элементы* a *и* b *множества* Ω ρ*-эквивалентны тогда и только тогда, когда* $\|a\| = \|b\|$;
2) *число классов* ρ*-эквивалентных элементов равно* $n + 1$. □

Утверждение 19. *Пусть на множестве* Ω *задана структура кольца Галуа* $R = \mathrm{GR}(q^n, p^n)$ *с единицей* e, $\eta = \rho(2, \mathrm{GL}(R))$. *Тогда*

1) *векторы* $\bar{a} = (a_1, a_2)$ *и* $\bar{b} = (b_1, b_2)$ *из* $\Omega^{[2]}$ η*-эквивалентны тогда и только тогда, когда* $\|a_1\| = \|b_1\|$, $\|a_2\| = \|b_2\|$ *и либо* $a_1 = b_1 = 0$, *либо* $a_2 = b_2 = 0$, *либо* $\vartheta(a_1)\vartheta(a_2)^{-1} - \vartheta(b_1)\vartheta(b_2)^{-1} \in p^m R$, *где* $m = n - \max\{\|a_1\|, \|a_2\|\}$;
2) *для любых* $i, j \in \overline{0, n-1}$ *и* $d \in \Omega$ *вектор* $\bar{a} = (a_1, a_2) \in \Omega^{[2]}$, *такой что* $0 \notin \{a_1, a_2\}$, $\|a_1\| = i$, $\|a_2\| = j$ *и* $p^{\max\{i,j\}}\vartheta(a_1)\vartheta(a_2)^{-1} = d$, *существует тогда и только тогда, когда* $\|d\| = \max\{i, j\}$ *и либо* $i \neq j$, *либо* $i = j$ *и* $d \neq p^{\max\{i,j\}} \cdot e$.

Доказательство. 1. Если $\bar{a}\ \eta\ \bar{b}$, то существует такой элемент $u \in R^*$, что

$$\begin{cases} ua_1 = b_1, \\ ua_2 = b_2. \end{cases}$$

Так как $u \in R^*$, то $\|a_1\| = \|b_1\|$ и $\|a_2\| = \|b_2\|$. Если $0 \in \{a_1, a_2\}$, то либо $a_1 = b_1 = 0$, либо $a_2 = b_2 = 0$. Если $0 \notin \{a_1, a_2\}$, то $0 \notin \{b_1, b_2\}$. Тогда векторы $\bar{a}' = (a_1, a_2, 0)$ и $\bar{b}' = (b_1, b_2, 0)$ $\rho(3, \mathrm{AGL}(R))$-эквивалентны и по утверждению 14 справедливо $\vartheta(a_1)\vartheta(a_2)^{-1} - \vartheta(b_1)\vartheta(b_2)^{-1} \in p^m R$, где $m = n - \max\{\|a_1\|, \|a_2\|\}$.

С другой стороны, если $a_1 = b_1 = 0$ или $a_2 = b_2 = 0$, то по утверждению 13 $\bar{a}\ \rho(2, \mathrm{AGL}(R))\ \bar{b}$, т. е. найдутся такие $u \in R^*$, $v \in R$, что

$$\begin{cases} ua_1 + v = b_1, \\ ua_2 + v = b_2. \end{cases}$$

Так как $a_1 = b_1 = 0$ или $a_2 = b_2 = 0$, то $v = 0$ и, следовательно, $\bar{a}\ \eta\ \bar{b}$.

Если $\|a_1\| = \|b_1\|$, $\|a_2\| = \|b_2\|$ и $0 \notin \{a_1, a_2\}$, то $\bar{a}' = (a_1, a_2, 0)$ и $\bar{b}' = (b_1, b_2, 0)$ — векторы из $\Omega^{[3]}$. Так как $\vartheta(a_1)\vartheta(a_2)^{-1} - \vartheta(b_1)\vartheta(b_2)^{-1} \in p^m R$, то по утверждению 14 $\bar{a}'\ \rho(3, \mathrm{AGL}(R))\ \bar{b}'$, т. е. существуют $u \in R^*$, $v \in R$ со свойством

$$\begin{cases} ua_1 + v = b_1, \\ ua_2 + v = b_2, \\ u \cdot 0 + v = 0. \end{cases}$$

Тогда $v = 0$ и $\bar{a}\ \eta\ \bar{b}$.

2. Вектор $\bar{a} = (a_1, a_2) \in \Omega^{[2]}$ с указанными свойствами существует тогда и только тогда, когда существует вектор $\bar{a}' = (a_1, a_2, 0) \in \Omega^{[3]}$ со свойствами $\|a_1 - 0\| = i$, $\|a_2 - 0\| = j$ и $p^{\max\{i,j\}}\vartheta(a_1 - 0)\vartheta(a_2 - 0)^{-1} = d$. Осталось воспользоваться утверждением 14. □

Следствие 20. *В условиях утверждения* 19 *множество* $\Omega^{[2]}$ *разбивается отношением* η *на* $\frac{1}{q-1}(q^{n+1} + q^n - q(n+1) + n - 1)$ *классов эквивалентности.* □

4. Группы аффинных и линейных преобразований кольца вычетов

Рассмотрим кольцо вычетов $\mathbb{Z}/N$. Пусть $N = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_m^{n_m}$ — каноническое разложение натурального числа N. Норму $\|a\|$ элемента $a \in \mathbb{Z}/N$ определим следующим образом. Если неотрицательный наибольший общий делитель чисел a и N равен $\mathrm{НОД}\{a, N\} = p_1^{i_1} \cdot p_2^{i_2} \cdot \ldots \cdot p_m^{i_m}$, положим

$$\|a\| = (i_1, i_2, \ldots, i_m).$$

Утверждение 21. *Пусть на множестве* Ω *задана структура кольца вычетов* $R = \mathbb{Z}/N$, $\rho = \rho(2, \mathrm{AGL}(R))$. *Тогда*

1) *векторы* $\bar{a} = (a_1, a_2)$ *и* $\bar{b} = (b_1, b_2)$ *из* $\Omega^{[2]}$ ρ*-эквивалентны тогда и только тогда, когда* $\|a_1 - a_2\| = \|b_1 - b_2\|$;

2) *число классов, на которые множество* $\Omega^{[2]}$ *разбивается отношением* ρ, *равно* $\prod\limits_{s=1}^{m}(n_s+1)-1$.

Доказательство. 1. Хорошо известно, что главные идеалы aR и bR совпадают тогда и только тогда, когда $\text{НОД}\{a,N\}=\text{НОД}\{b,N\}$, т. е. тогда и только тогда, когда $\|a\|=\|b\|$. Теперь для доказательства первого пункта осталось воспользоваться утверждением 11.

2. Согласно утверждению 11 число классов, на которые множество $\Omega^{[2]}$ разбивается отношением ρ, равно числу ненулевых главных идеалов кольца R, т. е. числу отличных от N натуральных делителей числа N. Число таких делителей есть $\prod\limits_{s=1}^{m}(n_s+1)-1$. □

Утверждение 22. *Пусть на множестве* Ω *задана структура кольца вычетов* $R=\mathbb{Z}/N$, $\rho=\rho(1,\mathrm{GL}(R))$. *Тогда*

1) *элементы* a *и* b *множества* Ω ρ*-эквивалентны тогда и только тогда, когда* $\|a\|=\|b\|$;
2) *число классов* ρ*-эквивалентных элементов равно* $\prod\limits_{s=1}^{m}(n_s+1)$.

Доказательство. 1. Если $a=0$, то $a\ \rho\ b$ тогда и только тогда, когда $b=0$, т. е. когда $\|a\|=\|b\|=(n_1,n_2,\ldots,n_m)$.

Пусть $a\neq 0$. В этом случае $b\neq 0$ и $a\ \rho\ b$ тогда и только тогда, когда $(a,0)\ \rho(2,\mathrm{AGL}(R))\ (b,0)$. Последнее ввиду утверждения 21 равносильно равенству $\|a\|=\|b\|$.

2. Число классов, на которые множество Ω разбивается отношением ρ, равно числу натуральных делителей N, т. е. $\prod\limits_{s=1}^{m}(n_s+1)$. □

5. Внешние прямые произведения групп

Пусть $\Omega=\Omega(1)\times\Omega(2)\times\ldots\times\Omega(m)$, G_j — группа подстановок на множестве $\Omega(j)$, $j\in\overline{1,m}$. Через $G=G_1\otimes G_2\otimes\ldots\otimes G_m$ обозначим внешнее прямое произведение групп $G_1,G_2,\ldots,G_m$. Задав естественным образом действие группы G на множестве Ω, G можно рассматривать как подгруппу группы $S(\Omega)$.

Рассмотрим векторы $\bar a=(a_1,a_2,\ldots,a_l)$ и $\bar b=(b_1,b_2,\ldots,b_l)$ из $\Omega^{[l]}$, и пусть

$$a_i=\big(a_i^{(1)},a_i^{(2)},\ldots,a_i^{(m)}\big),\quad b_i=\big(b_i^{(1)},b_i^{(2)},\ldots,b_i^{(m)}\big),\quad i\in\overline{1,l}.$$

Для каждого $j\in\overline{1,m}$ естественным образом определим векторы

$$\bar a^{(j)}=\big(a_1^{(j)},a_2^{(j)},\ldots,a_l^{(j)}\big),\quad \bar b^{(j)}=\big(b_1^{(j)},b_2^{(j)},\ldots,b_l^{(j)}\big)$$

с координатами из $\Omega(j)$.

Зададимся целью свести $\rho(l,G)$-эквивалентность векторов $\bar a$ и $\bar b$ к эквивалентности при каждом $j\in\overline{1,m}$ векторов $\bar a^{(j)}$ и $\bar b^{(j)}$. Заметим, что $\bar a^{(j)}$ и

$\bar{b}^{(j)}$ могут не лежать в множестве $\Omega(j)^{[l]}$. Поэтому по произвольному вектору $\bar{a} = (a_1, a_2, \ldots, a_l)$ с координатами из некоторого множества построим соответствующий ему вектор с попарно различными координатами следующим образом. Сначала в векторе $\bar{a}$ вычеркнем все стоящие за первым элементом равные ему элементы, затем в полученном векторе вычеркнем все стоящие за вторым элементом равные ему элементы, и т. д. В результате получим вектор $\mathrm{red}(\bar{a}) = (a_{i_1}, a_{i_2}, \ldots, a_{i_t})$ с попарно различными координатами, однозначно определяемый следующими условиями: $i_1 = 1 < i_2 < \ldots < i_t$ и для любого $s \in \overline{1,l}$ найдётся единственное $u \in \overline{1,t}$, такое что $a_{i_u} = a_s$, $i_u \leqslant s$. Через $\mathrm{nred}(\bar{a})$ обозначим длину вектора $\mathrm{red}(\bar{a})$.

Утверждение 23. *Пусть*

$$G = G_1 \otimes G_2 \otimes \ldots \otimes G_m -$$

группа подстановок на множестве

$$\Omega = \Omega(1) \times \Omega(2) \times \ldots \times \Omega(m),$$

где для любого $j \in \overline{1,m}$ G_j — группа подстановок на множестве $\Omega(j)$, $\rho = \rho(l, G)$. Тогда векторы $\bar{a} = (a_1, a_2, \ldots, a_l)$ и $\bar{b} = (b_1, b_2, \ldots, b_l)$ из $\Omega^{[l]}$ $\rho(l, G)$-эквивалентны в том и только в том случае, когда для любого $j \in \overline{1,m}$ справедливы следующие утверждения:

1) *при всех $u, v \in \overline{1,l}$ равенство $a_u^{(j)} = a_v^{(j)}$ имеет место тогда и только тогда, когда имеет место равенство $b_u^{(j)} = b_v^{(j)}$;*
2) *векторы $\mathrm{red}(\bar{a}^{(j)})$ и $\mathrm{red}(\bar{b}^{(j)})$ $\rho(\mathrm{nred}(\bar{a}^{(j)}), G_j)$-эквивалентны.*

Доказательство. По определению отношения $\rho(l, G)$ имеем, что $\bar{a}$ $\rho(l, G)$ $\bar{b}$ тогда и только тогда, когда найдётся подстановка $g = \big(g^{(1)}, g^{(2)}, \ldots, g^{(m)}\big) \in G$ со свойством $g(\bar{a}) = \bar{b}$, т. е. когда для каждого $j \in \overline{1,m}$ существует такая подстановка $g^{(j)} \in G_j$, что $g^{(j)}\big(\bar{a}^{(j)}\big) = \bar{b}^{(j)}$.

Зафиксируем $j \in \overline{1,m}$. Если для некоторой подстановки $g^{(j)} \in G_j$ справедливо равенство $g^{(j)}\big(\bar{a}^{(j)}\big) = \bar{b}^{(j)}$, то для любых $u, v \in \overline{1,l}$ равенство $a_u^{(j)} = a_v^{(j)}$ равносильно равенству $b_u^{(j)} = b_v^{(j)}$. Поэтому $\mathrm{nred}\big(\bar{a}^{(j)}\big) = \mathrm{nred}\big(\bar{b}^{(j)}\big)$ и $g^{(j)}\big(\mathrm{red}(\bar{a}^{(j)})\big) = \mathrm{red}\big(\bar{b}^{(j)}\big)$. С другой стороны, если $g^{(j)}\big(\mathrm{red}(\bar{a}^{(j)})\big) = \mathrm{red}\big(\bar{b}^{(j)}\big)$, $g^{(j)} \in G_j$ и имеет место утверждение 1, то $g^{(j)}\big(\bar{a}^{(j)}\big) = \bar{b}^{(j)}$.

Таким образом, $\bar{a}$ $\rho(l, G)$ $\bar{b}$ тогда и только тогда, когда для любого $j \in \overline{1,m}$ справедливы пункты 1 и 2 из формулировки утверждения. □

Следствие 24. *Пусть в условиях утверждения 23 $\rho = \rho(1, G)$. Тогда*

1) *элементы $a = \big(a^{(1)}, a^{(2)}, \ldots, a^{(m)}\big)$ и $b = \big(b^{(1)}, b^{(2)}, \ldots, b^{(m)}\big)$ множества Ω ρ-эквивалентны тогда и только тогда, когда для любого $j \in \overline{1,m}$ элементы $a^{(j)}$ и $b^{(j)}$ множества $\Omega(j)$ $\rho(1, G_j)$-эквивалентны*;
2) *число классов ρ-эквивалентных элементов равно $\prod\limits_{j=1}^{m} k_j$, где k_j для каждого $j \in \overline{1,m}$ — это число классов, на которые множество $\Omega(j)$ разбивается отношением $\rho(1, G_j)$.* □

Следствие 25. *Пусть в условиях утверждения* 23 *группы* G_j, $j \in \overline{1,m}$, *транзитивны*, $\rho = \rho(2, G)$. *Тогда*

1) *векторы* $\bar{a} = (a_1, a_2)$ *и* $\bar{b} = (b_1, b_2)$ *из* $\Omega^{[2]}$ ρ*-эквивалентны тогда и только тогда, когда для любого* $j \in \overline{1,m}$ *либо* $a_1^{(j)} = a_2^{(j)}$ *и* $b_1^{(j)} = b_2^{(j)}$, *либо* $\bar{a}^{(j)}\ \rho(2, G_j)\ \bar{b}^{(j)}$;
2) *множество* $\Omega^{[2]}$ *разбивается отношением* ρ *на* $\prod\limits_{j=1}^{m}(k_j+1)-1$ *классов эквивалентных элементов, где* k_j *для каждого* $j \in \overline{1,m}$ *— это число классов, на которые множество* $\Omega(j)^{[2]}$ *разбивается отношением* $\rho(2, G_j)$. □

Опишем группу $S(\Omega, \rho(l, G))$.

Утверждение 26. *Пусть в условиях утверждения* 23 $l \geqslant 2$, $|\Omega(j)| \geqslant l$, $\rho_j = \rho(l, G_j)$, $j \in \overline{1,m}$. *Тогда*

$$S(\Omega, \rho) = S(\Omega(1), \rho_1) \otimes S(\Omega(2), \rho_2) \otimes \ldots \otimes S(\Omega(m), \rho_m).$$

Доказательство. Пусть $h \in S(\Omega, \rho)$. Тогда по определению группы $S(\Omega, \rho)$ для любого вектора $\bar{a} = (a_1, a_2, \ldots, a_l) \in \Omega^{[l]}$ найдётся подстановка $g = \big(g^{(1)}, g^{(2)}, \ldots, g^{(m)}\big) \in G$ со свойством

$$h(\bar{a}) = g(\bar{a}) = \big(\big(g^{(1)}\big(a_1^{(1)}\big), g^{(2)}\big(a_1^{(2)}\big), \ldots, g^{(m)}\big(a_1^{(m)}\big)\big), \ldots, \big(g^{(1)}\big(a_l^{(1)}\big), g^{(2)}\big(a_l^{(2)}\big), \ldots, g^{(m)}\big(a_l^{(m)}\big)\big)\big).$$

Рассмотрим различные элементы

$$a = \big(a^{(1)}, a^{(2)}, \ldots, a^{(m)}\big), \quad b = \big(b^{(1)}, b^{(2)}, \ldots, b^{(m)}\big)$$

из Ω и положим

$$h(a) = \big(c^{(1)}, c^{(2)}, \ldots, c^{(m)}\big), \quad h(b) = \big(d^{(1)}, d^{(2)}, \ldots, d^{(m)}\big).$$

Так как $l \geqslant 2$, то существует вектор из $\Omega^{[l]}$, элементами которого являются a и b. Тогда для любого $j \in \overline{1,m}$ равенство $a^{(j)} = b^{(j)}$ равносильно равенству $c^{(j)} = d^{(j)}$. Это означает, что

$$h \in S(\Omega(1)) \otimes S(\Omega(2)) \otimes \ldots \otimes S(\Omega(m)),$$

т. е. $h = \big(h^{(1)}, h^{(2)}, \ldots, h^{(m)}\big)$, где $h^{(j)} \in S(\Omega(j))$ для любого $j \in \overline{1,m}$.

Теперь равенство $h(\bar{a}) = g(\bar{a})$ можно переписать в виде системы соотношений

$$h^{(j)}\big(\bar{a}^{(j)}\big) = g^{(j)}\big(\bar{a}^{(j)}\big), \quad j \in \overline{1,m},$$

и в силу произвольности вектора $\bar{a}$ имеем $h^{(j)} \in S(\Omega(j), \rho_j)$, $j \in \overline{1,m}$.

Таким образом,

$$S(\Omega, \rho) \subseteq S(\Omega(1), \rho_1) \otimes S(\Omega(2), \rho_2) \otimes \ldots \otimes S(\Omega(m), \rho_m).$$

Обратное включение очевидно. □

Теперь с использованием полученных ранее результатов о свойствах отношений эквивалентности, порождаемых различными группами, нетрудно получать результаты о свойствах отношений, построенных с помощью внешних прямых произведений таких групп. Выделим два случая.

Утверждение 27. *Пусть в условиях следствия* 25 *для каждого* $j \in \overline{1,m}$ *на множестве* $\Omega(j)$ *задана структура кольца Галуа* $R_j = \mathrm{GR}(q_j^{n_j}, p_j^{n_j})$ *и* $G_j = \mathrm{AGL}(R_j)$. *Тогда*

1) *векторы* $\bar{a} = (a_1, a_2)$ *и* $\bar{b} = (b_1, b_2)$ *из* $\Omega^{[2]}$ ρ*-эквивалентны тогда и только тогда, когда для любого* $j \in \overline{1,m}$ *в кольце* R_j *справедливо равенство* $\|a_1^{(j)} - a_2^{(j)}\| = \|b_1^{(j)} - b_2^{(j)}\|$;
2) *множество* $\Omega^{[2]}$ *разбивается отношением* ρ *на* $\prod\limits_{j=1}^{m}(n_j+1)-1$ *классов эквивалентных элементов*;
3) $|S(\Omega,\rho)| = \prod\limits_{j=1}^{m}(q_j!)^{\frac{q_j^{n_j}-1}{q_j-1}}$.

Доказательство. Достаточно воспользоваться утверждениями 13, 26 и следствием 25. □

Утверждение 27 позволяет эффективно занумеровать классы ρ-эквивалентных векторов элементами множества

$$\left\{(i_1, i_2, \ldots, i_m) \mid i_j \in \overline{0, n_j},\ j \in \overline{1,m}\right\} \setminus \{(n_1, n_2, \ldots, n_m)\}$$

и считать, что вектор $\bar{a} = (a_1, a_2)$ лежит в классе с номером $(i_1, i_2, \ldots, i_m)$ тогда и только тогда, когда для любого $j \in \overline{1,m}$ справедливо равенство $\|a_1^{(j)} - a_2^{(j)}\| = i_j$.

Утверждение 28. *Пусть в условиях следствия* 25 $G_j = S(\Omega(j))$ *для каждого* $j \in \overline{1,m}$. *Тогда*

1) *векторы* $\bar{a} = (a_1, a_2)$ *и* $\bar{b} = (b_1, b_2)$ *из* $\Omega^{[2]}$ ρ*-эквивалентны тогда и только тогда, когда для любого* $j \in \overline{1,m}$ *либо* $a_1^{(j)} = a_2^{(j)}$ *и* $b_1^{(j)} = b_2^{(j)}$, *либо* $a_1^{(j)} \neq a_2^{(j)}$ *и* $b_1^{(j)} \neq b_2^{(j)}$;
2) *множество* $\Omega^{[2]}$ *разбивается отношением* ρ *на* $2^m - 1$ *классов эквивалентных элементов.* □

Утверждение 28 позволяет эффективно занумеровать классы ρ-эквивалентных векторов элементами множества

$$\left\{(i_1, i_2, \ldots, i_m) \mid i_1, i_2, \ldots, i_m \in \overline{0,1}\right\} \setminus \{(0, 0, \ldots, 0)\}$$

и считать, что вектор $\bar{a} = (a_1, a_2)$ лежит в классе с номером $(i_1, i_2, \ldots, i_m)$ тогда и только тогда, когда для любого $j \in \overline{1,m}$ в случае $i_j = 0$ имеет место равенство $a_1^{(j)} = a_2^{(j)}$ и в случае $i_j = 1$ неравенство $a_1^{(j)} \neq a_2^{(j)}$.

Полученные результаты можно применять не только для внешних прямых произведений групп подстановок, но и для групп, им подстановочно изоморфным.

Напомним, что группы подстановок G и G' на множествах Ω и Ω' соответственно называются подстановочно изоморфными (см., например, [6]), если существуют биективные отображения $\chi\colon G \to G'$ и $\psi\colon \Omega \to \Omega'$, такие что χ — изоморфизм групп и $\psi(g(a)) = \chi(g)(\psi(a))$ для всех $a \in \Omega$, $g \in G$. При этом пара отображений (χ, ψ) называется изоморфизмом групп подстановок.

Утверждение 29. *Пусть (χ, ψ) — изоморфизм групп подстановок G и G' на множествах Ω и Ω' соответственно, $\rho = \rho(l, G)$ и $\rho' = \rho(l, G')$. Тогда*

1) *векторы $\bar{a}, \bar{b} \in \Omega^{[l]}$ ρ-эквивалентны тогда и только тогда, когда ρ'-эквивалентны векторы $\psi(\bar{a})$ и $\psi(\bar{b})$;*
2) *группы $S(\Omega, \rho)$ и $S(\Omega', \rho')$ подстановочно изоморфны.*

Доказательство. 1. Достаточно заметить, что для подстановки $g \in G$ равенство $g(\bar{a}) = \bar{b}$ имеет место тогда и только тогда, когда $\chi(g)(\psi(\bar{a})) = \psi(\bar{b})$.

2. Определим отображение $\tilde{\chi}\colon S(\Omega) \to S(\Omega')$, положив $\tilde{\chi}(h)(c) = \psi(h(\psi^{-1}(c)))$ для всех $c \in \Omega'$, $h \in S(\Omega)$. Тогда $(\tilde{\chi}, \psi)$ — изоморфизм групп подстановок и $\chi(g) = \tilde{\chi}(g)$ для любой подстановки $g \in G$.

По определению группы $S(\Omega, \rho)$ принадлежность $h \in S(\Omega, \rho)$ равносильна тому, что любой вектор $\bar{a} \in \Omega^{[l]}$ ρ-эквивалентен $h(\bar{a})$. По определению отношений ρ и ρ' имеем, что $\bar{a}\ \rho\ h(\bar{a})$ тогда и только тогда, когда ρ'-эквивалентны векторы $\psi(\bar{a})$ и $\psi(h(\bar{a})) = \tilde{\chi}(h)(\psi(\bar{a}))$. В силу биективности отображения ψ это означает, что $h \in S(\Omega, \rho)$ тогда и только тогда, когда $\tilde{\chi}(h) \in S(\Omega', \rho')$. Теперь можно корректно определить отображение $\chi'\colon S(\Omega, \rho) \to S(\Omega', \rho')$ равенством $\chi'(h) = \tilde{\chi}(h)$, $h \in S(\Omega, \rho)$. В этом случае, как нетрудно видеть, (χ', ψ) — изоморфизм групп подстановок $S(\Omega, \rho)$ и $S(\Omega', \rho')$, что и завершает доказательство. □

Следствие 30.

1. *Пусть на множествах $\Omega, \Omega(1), \Omega(2), \ldots, \Omega(m)$ задана структура конечных коммутативных колец с единицей $R, R_1, R_2, \ldots, R_m$ соответственно, кольцо R изоморфно внешней прямой сумме $R_1 \oplus R_2 \oplus \ldots \oplus R_m$, $l \geqslant 2$, $\rho = \rho(l, \mathrm{AGL}(R))$, $\rho_j = \rho(l, \mathrm{AGL}(R_j))$, $j \in \overline{1, m}$. Тогда группы $S(\Omega, \rho)$ и $S(\Omega(1), \rho_1) \otimes S(\Omega(2), \rho_2) \otimes \ldots \otimes S(\Omega(m), \rho_m)$ подстановочно изоморфны.*
2. *Если $R = \mathbb{Z}/N$, $N = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_m^{n_m}$ — каноническое разложение натурального числа N, $l = 2$, то $|S(\Omega, \rho)| = (q!)^{\frac{q^n - 1}{q-1}}$.*

Доказательство. 1. Очевидно, что в условиях настоящего следствия аффинная группа кольца R будет подстановочно изоморфна группе

$$H = \mathrm{AGL}(R_1) \otimes \ldots \otimes \mathrm{AGL}(R_m).$$

Тогда группы $S(\Omega, \rho)$ и $S(\Omega', \rho(l, H))$, где $\Omega = \Omega(1) \times \Omega(2) \times \ldots \times \Omega(m)$, подстановочно изоморфны. Осталось заметить, что по следствию 25 справедливо равенство

$$S(\Omega', \rho(l, H)) = S(\Omega(1), \rho_1) \otimes S(\Omega(2), \rho_2) \otimes \ldots \otimes S(\Omega(m), \rho_m).$$

2. Хорошо известно, что $\mathbb{Z}/N \cong \mathbb{Z}/p_1^{n_1} \oplus \ldots \oplus \mathbb{Z}/p_m^{n_m}$. Тогда по доказанному

$$S(\Omega, \rho) = \prod_{j=1}^{m} S(\Omega(j), \rho_j),$$

где $\rho_j = \rho(2, \mathrm{AGL}(\mathbb{Z}/p_j^{n_j}))$, $j \in \overline{1,m}$. Так как $\mathbb{Z}/p_j^{n_j} = \mathrm{GR}(p_j^{n_j}, p_j^{n_j})$, то по утверждению 13

$$|S(\Omega(j), \rho_j)| = (p_j!)^{\frac{p_j^{n_j}-1}{p_j-1}},$$

и следовательно,

$$|S(\Omega, \rho)| = \prod_{j=1}^{m} (p_j!)^{\frac{p_j^{n_j}-1}{p_j-1}}. \qquad \square$$

Литература

[1] Алфёров А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — М.: Гелиос АРВ, 2001.

[2] Глухов М. М. О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // Труды по дискретной математике. Т. 1. — М.: ТВП, 1997. — С. 43—66.

[3] Глухов М. М., Погорелов Б. А. О некоторых применениях групп в криптографии // Математика и безопасность информационных технологий. Материалы конференции в МГУ 28—29 октября 2004 г. — М.: МЦНМО, 2005. — С. 19—31.

[4] Елизаров В. П. Конечные кольца. — М.: Гелиос АРВ, 2006.

[5] Нечаев А. А. Конечные кольца главных идеалов // Мат. сб. — 1973. — Т. 92, № 3. — С. 350—366.

[6] Погорелов Б. А. Основы теории групп подстановок. Часть 1. Общие вопросы. — М., 1986.

[7] Шнайер Б. Прикладная криптография. — М.: ТРИУМФ, 2002.

[8] McDonald B. R. Finite Rings with Identity. — New York: Marcel Dekker, 1974.

[9] Wielandt H. Finite Permutation Groups. — New York: Academic Press, 1964.