УДК 512.7

РЕГУЛЯРНЫЕ МНОЖЕСТВА И КВАЗИПОЛЯ КОНЕЧНЫХ ПРОЕКТИВНЫХ ПЛОСКОСТЕЙ ТРАНСЛЯЦИЙ

Яковлева Т.Н.,
научный руководитель д. ф.-м. н., профессор Левчук В.М.
Институт математики и фундаментальной информатики

1. Основные определения и регулярное множество

Работа посвящена построению и представлению регулярных множеств и квазиполей конечных проективных плоскостей трансляций.

Определение 1.1. *Проективная плоскость* – это множество точек, определенные подмножества которого называются прямыми и которое удовлетворяет следующим аксиомам:

A1. Две произвольные различные точки лежат на одной и только на одной прямой.

A2. Две произвольные различные прямые пересекаются в одной и только одной точке.

A3. Существуют четыре точки, никакие три из которых не лежат на одной прямой.

Определение 1.2. Множество Q = Q(+,○) с бинарными операциями сложения + и умножения ○ называют *квазиполем*, если выполняются следующие условия:

1) $Q(+)$ – абелева группа;
2) для любых $a, b \in Q, a \neq 0$, уравнения $a \circ x = b$ и $y \circ a = b$ однозначно разрешимы в Q;
3) существует единичный элемент $e \neq 0$, то есть такой, что $e \circ a = a \circ e = a$ для всех $a \in Q$;
4) выполняется левый дистрибутивный закон $(a + b) \circ c = a \circ c + b \circ c$ для любых $a, b, c \in Q$;
5) $a \circ 0 = 0$ для любого $a \in Q$;
6) если $a, b, c \in Q$ и $a \neq b$, то уравнение $x \circ a = x \circ b + c$ однозначно разрешимо в Q.

Известно, что проективную плоскость трансляций любого примарного порядка p^n с простым p удается построить, координатизируя ее n-мерным линейным пространством W над полем Z_p и снабжая W структурой квазиполя порядка p^n с помощью определенного регулярного множества.

Для построения плоскостей трансляций ранга n выбирают n-мерное линейное пространство W над полем F (*координатизирующее множество*), внешнюю прямую сумму $V = W \oplus W = \{(x, y) | x, y \in W\}$ двух копий W и расщепление μ аддитивной группы (V,+) такое, что $V = M \oplus N$ для любых M ≠ N из μ. Точки проективной плоскости трансляций π = π(V,μ) есть 1-мерные подпространства из V, а прямые – это подгруппы из μ и смежные классы по ним; по определению, смежные классы по одной и той же подгруппе пересекаются в одной и той же точке (∞), называемой особой, а особую прямую [∞] в π составляют все особые точки.

Далее мы введем определение регулярного множестваплоскости и установим соответствующее ему квазиполе на W.

Напомним, что расщеплением аддитивной группы называют набор ее подгрупп (компоненты расщепления), имеющих попарно нулевые пересечения и дающих в теоретико-множественном объединении всю группу. Компоненты выбранного расщепления μ группы (V,+) есть n-мерные подпространства в V. Более точно, верна следующая лемма, где полагаем

$$V(\sigma) = \{(v, v^{\sigma}) | v \in W\} \quad (\sigma \in GL(W)), V(0) = (W,0), \quad V(\infty) = (0,W).$$

Лемма 1.1 Допустим, что V(0), V(∞) ∈ μ. Тогда:

а) если M ∈ μ и M ≠ V(0), V(∞), то M = $V(\sigma)$ при единственном $\sigma \in GL(W)$ и, в частности, $\mu = \{V(\sigma) | \sigma \in R^* \cup \{0\}\} \cup \{V(\infty)\}$ при $R^* = \{\sigma \in GL(W) | V(\sigma) \in \mu\}$;

б) если $u, v \in W \setminus \{0\}$, то $u^{\sigma} = v$ при единственном $\sigma \in R^*$;

в) если $\tau, \rho \in R^*$ и $\tau \neq \rho$, то $\tau - \rho \in GL(W)$.

Верно и обратное: если подмножество R^* в GL(W) удовлетворяет условиям б) и в), то $\mu = \{V(0), V(\infty)\} \cup \{V(\sigma) | \sigma \in R^*\}$ есть расщепление группы (V,+) такое, что $V = M \oplus N$ для любых M ≠ N из μ.

Обозначения координат вектора (x, y) в V используют и для точек соответствующего аффинного пространства. С геометрической точки зрения компоненты $V(\sigma)$ и V(∞) есть прямые, проходящие через точку (0,0). Остальные прямые, исключая прямую на бесконечности, получаются из данных прямых трансляциями.

Определение 1.3. *Регулярным множеством* R плоскости π называют совокупность нулевого преобразования и произвольного подмножества R^* в GL(W) с единицей и условиями б), в).

Заметим, что свойство б) позволяет любому ненулевому элементу $u \in W$ сопоставить биективное отображение $\theta: W \to R^* \cup \{0\}$ по правилу:

$$\theta(v) = \sigma \quad (v \in W \setminus \{0\}, \; u^{\sigma} = v), \quad \theta(0) = 0.$$

Рассматривая W как пространство векторов-строк длины n, представляем R образом $\theta(W)$ в кольце всех $n \times n$ – матриц над F для биективного отображения $\theta: W \to R$ такого, что нулевая и единичная матрицы лежат в R, а любая ненулевая матрица и разность различных матриц из R являются невырожденными. Умножение ∘ на W вводим, записывая векторы из W координатными строками и полагая

$$x \circ y := x \cdot \theta(y) \quad (x, y \in W).$$

2. Представление регулярного множества

В этом параграфе мы рассмотрим представление Оямы[1] регулярного множества проективной плоскости.

Пусть $GF(q)$ есть конечное поле порядка q. Для элемента x из расширения $GF(q^n)$ степени n поля $GF(q)$ элемент $\overline{x} = x^q$ назовем сопряженным к x. Положим

$$x = x^{(0)}, \overline{x} = x^{(1)} = x^q \text{ и } x^{(i)} = x^{q^i}, i = 2, 3, \dots, n-1.$$

Тогда отображение $x \to x^{(i)}$ есть автоморфизм поля $GF(q^n)$, действующий тождественно на подполе $GF(q)$. Если $\alpha = (\alpha_{ij}) \in GL(n, q^n)$, то полагая

$\overline{\alpha}$ = $(\overline{\alpha_{ij}})$, $\qquad w = \begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \\ \vdots & \ddots & \ddots & \ddots & \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$,

гдеw - $n \times n$-матрица, введем множество$\mathcal{U} = \{\alpha \in GL(n, q^n) | \overline{\alpha} = \alpha w\}$.

Лемма 2.1. Для любого $\alpha_0 \in \mathcal{U}$ верно равенство $\mathcal{U} = GF(n, q)\alpha_0$. Кроме того, $n \times n$ – матрицаαнад$GF(q^n)$лежит в$\mathcal{U}$ тогда и только тогда, когда существуют линейно независимые над $GF(q)$ элементы $\alpha_0, \alpha_1, \dots, \alpha_{n-1}$ с условием

$$\alpha = \begin{pmatrix} \alpha_0 & \alpha_0^{(1)} & \dots & \alpha_0^{(n-1)} \\ \alpha_1 & \alpha_1^{(1)} & \cdots & \alpha_1^{(n-1)} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_{n-1} & \alpha_{n-1}^{(1)} & \cdots & \alpha_{n-1}^{(n-1)} \end{pmatrix}$$

Доказательство. Для любого элемента δ из $GL(n, q)$, $\overline{\delta\alpha_0} = \delta\overline{\alpha_0} = \delta\alpha_0 w$, следовательно$\delta\alpha_0 \in \mathcal{U}$. Иначе, для любого элемента α из $\mathcal{U}$, $\overline{\alpha\alpha_0^{-1}} = \alpha w w^{-1}\alpha_0^{-1}$ = $\alpha\alpha_0^{-1} \in GL(n, q)$ и поэтому $\alpha \in GL(n, q)\alpha_0$. Таким образом $\mathcal{U} \in GL(n, q)\alpha_0$.

Пусть $\alpha = (\alpha_{ij})$ это есть любой элемент из$\mathcal{U}$. Так как

$$\overline{\alpha} = \alpha w, \overline{\alpha_{ij}} = \alpha_{i2}, \overline{\alpha_{i1}} = \alpha_{i3}, \dots, \overline{\alpha_{in-1}} = \alpha_{in}, i = 1,2, \dots, \mathrm{n},$$

то$\alpha_{ij} = \alpha_{i1}^{(j-1)}$, i = 1,2, … , n; j = 2, 3, … ,n. В силуневырожденностиматрицыα, элементы $\alpha_{11}, \alpha_{21}, \dots, \alpha_{n1}$ линейно независимынад$GF(q)$.

Поскольку обратное утверждение очевидно, то доказательство завершено.

Сейчас несложно доказывается

Лемма 2.2. Если $\alpha \in \mathcal{U}$, то

$$\alpha^{-1} = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^{(1)} & \alpha_1^{(1)} & \cdots & \alpha_{n-1}^{(1)} \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_0^{(n-1)} & \alpha_1^{(n-1)} & \cdots & \alpha_{n-1}^{(n-1)} \end{pmatrix} \in GL(n, q^n).$$

Оказывается, в матричном представлении в регулярном множестве R все ненулевые матрицы имеют вид, описанный в леммы 2.1; кроме того, оно содержит нулевую и единичную матрицу, а разность любых различных матриц из R всегда есть невырожденная матрица.

Наряду с описанием регулярных множеств, исследуются некоторые их свойства.

.

[1] T. Oyama. *On quasifields*. – Osaka Journal of Mathematics. 22(1)P.35-P.54. 1985
[2] D.R. Hughes, F.C. Piper, *Projective planes* // Springer – Verlag: New-York Inc, 1973