УДК 514.161

Антропова Г.Р., кандидат педагогических наук, Набережночелнинский институт ФГАОУ ВО «Казанский (Приволжский) федеральный университет», e-mail: antropovagr@mail.ru
Матвеев С.Н., кандидат физико-математических наук, доцент, Набережночелнинский институт ФГАОУ ВО «Казанский (Приволжский) федеральный университет», e-mail: semen967@rambler.ru

О МОДЕЛЯХ ПРОЕКТИВНОЙ ПЛОСКОСТИ ПОЛЯ ГАЛУА

Аннотация. Исследуются модели конечной проективной плоскости, индуцируемой полем Галуа. Рассмотрены возможные способы построения трехмерного векторного пространства с использованием линейного оператора и системы компьютерной алгебры Maxima, проективная эквивалентность полученных моделей малых порядков.

Ключевые слова: поле, примитивный элемент, конечная проективная плоскость, сложное отношение, проективное преобразование.

Приведём первоначально некоторые сведения, необходимые для определения задачи. Поле Галуа $GF(p^n)$ – это конечное множество с числом элементов p^n с двумя бинарными операциями (сложение и умножение), что образует коммутативное ассоциативное кольцо с единицей, где p – простое число, называемое характеристикой поля, n- натуральное число, причем ненулевые элементы образуют мультипликативную группу. Эта группа циклическая, то есть в ней есть порождающий (примитивный) элемент A, все остальные получаются возведением в степень примитивного элемента, причем $A^{p^n-1}=1$. Число примитивных элементов определяется функцией Эйлера. Поле $GF(p^n)$ естественным образом определяет структуру векторного пространства с базисом $\{1, A, \dots A^{n-1}\}$ [1]. Мы приводим решение задачи для случая $n=3$ и некоторых p.

Под конечным проективным пространством, порожденным векторным пространством $V_{\mathrm{m+1}}$ (без нуль вектора), понимаем непустое множество P_{m}, удовлетворяющее аксиомам проективного пространства, если задано сюрьективное отображение $\varphi: V_{\mathrm{m+1}} \to P_{\mathrm{m}}$, при котором коллинеарным векторам соответствует единственный элемент (проективная точка). Конечная проективная плоскость порядка k (k> 2, k – некоторое натуральное число) это множество точек и множество прямых, некоторые элементы которых связаны отношением инцидентности: каждой прямой проективной плоскости инцидентны точно k + 1 точек.

Здесь приводим построение проективного пространства размерности m= 2, то есть проективной плоскости, порожденной векторным пространством, индуцированным $GF(p^3)$. В качестве модели проективной плоскости принимаем конечное множество, в котором проективный репер определяется четырьмя упорядоченными точками $R = (A_1, A_2, A_3, E)$, где E – единичная точка, и всякая точка относительного репера задается однородными координатами (x_1, x_2, x_3) или неоднородными координатами $x = \frac{x_2}{x_1}, y = \frac{x_3}{x_1}$ которые принимают значения остатков от деления на простое число p. Действия над ними производим согласно определенным операциям алгебры системы вычетов по модулю p. Считаем, что две модели проективно эквивалентны, если существует проективное отображение одной модели на другую, то есть эквивалентные модели определяют одну и ту же проективную структуру.

Наиболее вероятным является предположение о том, что каждая конечная проективная плоскость имеет порядок, равный степени простого числа [2]. Вопрос о единственности проективной плоскости данного порядка изучен также не полностью. Так, конечные проективные плоскости порядка меньше 9 единственны как алгебраические структуры, однако вопрос единственности проективной структуры плоскостей над соответствующими полями Галуа мало изучен. С другой стороны известно, что проективные плоскости порядка выше 8 не единственны как алгебраические структуры, например, существуют (по крайней мере) четыре неизоморфные плоскости девятого порядка [2]. Следует заметить, что с увеличением порядка возрастает порядок вычислений, поэтому применение математических пакетов становиться необходимостью. Здесь проявляется одно из главных достоинств математических пакетов – возможность исследования более сложных математических моделей, благодаря сокращению громоздких вычислений и рутинных операций.

1. Рассмотрим $GF(p^3), p = 2$. Для построения трехмерного векторного пространства введем линейный оператор с матрицей $\mathcal{A} = \begin{pmatrix} 0 & 0 & \gamma \\ 1 & 0 & \beta \\ 0 & 1 & \alpha \end{pmatrix}$, где $A^3 = \alpha A^2 + \beta A + \gamma 1$, и решим уравнение $\mathrm{A}^7 = 1$ равносильное системе

$$\begin{cases} \alpha^5 + 4\alpha^3\beta + 3\alpha^2\gamma + 3\alpha\beta^2 + 2\beta\gamma = 0, \\ \alpha^4\beta + \alpha^3\gamma + 3\alpha^2\beta^2 + \beta^3 + 4\alpha\beta\gamma + \gamma^2 = 0, \\ \alpha^4\gamma + 3\alpha^2\beta\gamma + \beta^2\gamma + 2\alpha\gamma^2 = 1. \end{cases} (1)$$

Реализация некоторых вычислений с помощью системы компьютерной алгебры Maxima имеет вид:

B: matrix([0,0,gamma], [1,0,beta], [0,1,alpha]);

$$\begin{bmatrix} 0 & 0 & \Gamma \\ 1 & 0 & \beta \\ 0 & 1 & \alpha \end{bmatrix}$$

B5:ratsimp(B.B.B.B.B);

$$\begin{bmatrix} (\beta+\alpha^2)\Gamma & \Gamma^2 + (2\alpha\beta+\alpha^3)\Gamma & 2\alpha\Gamma^2 + (\beta^2 + 3\alpha^2\beta + \alpha^4)\Gamma \\ \alpha\Gamma + \beta^2 + \alpha^2\beta & (2\beta+\alpha^2)\Gamma + 2\alpha\beta^2 + \alpha^3\beta & \Gamma^2 + (4\alpha\beta+\alpha^3)\Gamma + \beta^3 + 3\alpha^2\beta^2 + \alpha^4\beta \\ \Gamma + 2\alpha\beta + \alpha^3 & 2\alpha\Gamma + \beta^2 + 3\alpha^2\beta + \alpha^4 & (2\beta + 3\alpha^2)\Gamma + 3\alpha\beta^2 + 4\alpha^3\beta + \alpha^5 \end{bmatrix}$$

M:{}$ for alpha: 0 thru 1 do for beta: 0 thru 1 do for gamma: 0 thru 1 do if integer (alpha) and integer (beta) and integer (gamma) and mod ((2*beta+3*alpha^2)*gamma+3*alpha*beta^2+4*alpha^3*beta+alpha^5,2)=0 and mod (gamma^2+(4*alpha*beta+alpha^3)*gamma+beta^3+3*alpha^2*beta^2+ +alpha^4*beta, 2)=0 and mod(2*alpha*gamma^2+(beta^2+3*alpha^2*beta+alpha^4)*gamma,2)=1 then M:{M,[alpha, beta, gamma]}$ flatten(M); cardinality(%);

{[0,1,1],[1,0,1]}.

A^1=[0,1,0]; A^2=[1,0,0]; A^3=[alpha:1,beta:0,gamma:1];

```
for i: 3 thru 6 do if i=3 then print(A^(i+1)=[u[i+1]: mod(alpha*alpha+beta,2),
v[i+1]:mod(beta*alpha+gamma,2), w[i+1]:mod(gamma*alpha,2)]) else if i>3 then
print(A^(i+1)=[u[i+1]:mod(alpha*u[i]+v[i],2),
[i+1]:mod(beta*u[i]+w[i],2),w[i+1]:mod(gamma*u[i],2)]);
```

A=[0,1,0], A^2=[1,0,0], A^3=[1,0,1], A^4=[1,1,1], A^5=[0,1,1], A^6=[1,1,0], A^7=[0,0,1].

Таким образом, решение системы (1) приводит к двум линейным операторам с соответствующими матрицами $\mathcal{A}_{\mathrm{I}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, $\mathcal{A}_{\mathrm{II}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Построенное с использованием оператора $\mathcal{A}_{\mathrm{I}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ двумерное векторное пространство порождает конечную проективную плоскость второго порядка из семи точек, которые определяются следующими однородными проективными координатами: A=[0,1,0], A^2=[1,0,0],A^3=[1,0,1], A^4=[1,1,1], A^5=[0,1,1], A^6=[1,1,0], A^7=[0,0,1].

Отличные от A мультипликативные образующие могут быть выбраны шестью ($\varphi(7) = 6$) способами, где $\varphi(p^2 - 1)$ определяется значением функции Эйлера. Значит, возможны следующие мультипликативные образующие: $\{A, A^2, A^3, A^4, A^5, A^6\}$, их показатели взаимно просты с числом 7. Следовательно, замена мультипликативной образующей приводит к соответствующим преобразованиям $\{f_2, f_3, f_4, f_5, f_6\}$ построенной модели. Получено, что $\{f_2, f_4\}$ - проективные преобразования (с одной инвариантной точкой), в отличие от преобразований $\{f_3, f_5, f_6\}$, причем образы изоморфизмов $\{f_3, f_5, f_6\}$ также проективно эквивалентны.

Таким образом, выбор оператора $\mathcal{A}_{\mathrm{I}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ приводит двум алгебраически изоморфным, но проективно не эквивалентным структурам.

Аналогичные вычисления с использованием следующего возможного оператора $\mathcal{A}_{\mathrm{II}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ также приводят к двум алгебраически изоморфным, но проективно не эквивалентным структурам.

2. Рассмотрим $GF(p^3), p = 3$. Находим возможные операторы, решив систему $\mathcal{A}^{26} = 1$, первое уравнение которой после упрощения имеет вид:

$$2\beta\Gamma^8 + 2\alpha^9\beta\Gamma^5 + (2\alpha^{12}\beta + 2\alpha^{14})\Gamma^4 + (2\beta^{10} + \alpha^{12}\beta^4 - \alpha^{18}\beta)\Gamma^2 +$$
$$+(\alpha^3\beta^{10} + \alpha^5\beta^9 + \alpha^9\beta^7 + \alpha^{11}\beta^6 + \alpha^{21}\beta + \alpha^{24})\Gamma = 1.$$

Всего возможных операторов восемь, из которых четыре приводят к структуре конечной проективной плоскости третьего порядка:

$$\mathcal{A}_{\mathrm{I}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}, \mathcal{A}_{\mathrm{II}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$
$$\mathcal{A}_{\mathrm{III}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \mathcal{A}_{\mathrm{IV}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}.$$

Построенное с использованием оператора $\mathcal{A}_{\mathrm{I}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ двумерное векторное пространство порождает конечную проективную плоскость третьего порядка из тринадцати точек, которые определяются следующими однородными проективными координатами: A=[0,1,0], A^2=[1,0,0], A^3=[2,0,1], A^4=[1,1,2], A^5=[0,2,1], A^6=[2,1,0], A^7=[2,0,2], A^8=[1,2,2], A^9=[1,2,1], A^{10}=[1,1,1], A^{11}=[0,1,1], A^{12}=[1,1,0], A^3=[0,0,1].

Отличные от A мультипликативные образующие могут быть выбраны шестью ($\varphi(26) = 12$) способами. Значит, возможны следующие мультипликативные образующие: $\{A, A^3, A^5, A^7, A^9, A^{11}, A^{15}, A^{17}, A^{19}, A^{21}, A^{23}, A^{25}\}$, их показатели взаимно просты с числом 26. Следовательно, замена мультипликативной образующей приводит к соответствующим преобразованиям $\{f_i\}$ построенной модели. Получено, что $\{f_3, f_9\}$ - проективные преобразования (с одной инвариантной точкой), в отличие от преобразований $\{f_5, f_7, f_{11}, f_{15}, f_{17}, f_{19}, f_{21}, f_{23}, f_{25}\}$, причем образы последних изоморфизмов также разбиваются на подгруппы трех проективно эквивалентны структур.

Таким образом, выбор оператора $\mathcal{A}_{\mathrm{I}} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}$ приводит четырем алгебраически изоморфным, но проективно не эквивалентным структурам.

Литература

1. Арнольд В.И. Динамика, статистика и проективная геометрия полей Галуа.–М.: МЦНМО, 2005.– 72с.

2. Афанасьев В.В. Конечные геометрии // Современная математика. Фундоментальные направления. – 2007. - Т22. - С.127-138.

3. Матвеев С.Н., Сиразов Ф.С. Использование системы компьютерной алгебры Maxima в изучении конечных проективных прямых // Высшее образование сегодня. - 2015. - №2. - С. 72-75.

4. Матвеев С.Н., Сиразов Ф.С. Модели конечной проективной прямой, индуцируемые полем Галуа // Актуальные проблемы математического образования. Сб. статей международной научно-практической конференции. - Набережные Челны: ФГБОУ ВПО «НИСПТР», 2015. - С.37-40.

Antropova Gyuzel Raviljevna, associate professor, candidate of pedagogical science, Naberezhnye Chelny Institute of Kazan (Volga region) Federal University
Matveev Semen Nikolaevish, associate professor, candidate of physical and mathematical sciences, Naberezhnye Chelny Institute of Kazan (Volga region) Federal University

ABOUT THE MODELS OF PROJECT PLANE OF THE FIELD OF GALOIS

Abstract. We study the model of a finite projective line induced Galois field. The possible ways to construct a two-dimensional vector space and projective equivalence of the obtained models of the finite projective plane of order.

Key words: field, a primitive element, projective line, a complex relationship, involution.