On Semifields of order q^4, q an odd prime, $q > 3$, admitting a Klein 4-group of automorphisms

Mashhour Bani-Ata

Department of Mathematics

PAAET - Kuwait

The 4th Novi Sad Algebraic Conference

& Semigroups and Applications 2013

Novi Sad, Serbia, June 5-9, 2013.

Hering's Question:

This talk was inspired by a question of Hering, that is:
Given a finite group G, is it possible to find a vector space V and a spread $\mathcal{K}$ on V [$\mathcal{K}$ is a set of subspaces U of V with $\dim(U) = \frac{1}{2}\dim(V)$ and any non-zero element of V is contained in exactly one member of $\mathcal{K}$] such that $G \leq GL(V)$ and preserves $\mathcal{K}$ (i.e. $G \leq$ translation complement of $\mathcal{K}$)?

So our concern is about finding triples $(V, G, \mathcal{K})_{\mathbb{F}_q}$, where V is an even dimensional vector space over $\mathbb{F}_q$, $\mathcal{K}$ is a spread of V, $G \leq GL(V)$, G preserves $\mathcal{K}$ and acts freely on V.

Hering's Question:

The most elementary example is:
The triple $(V, \Gamma, \mathcal{K}_d)$, where V is a 2-dimensional subspace over $\mathbb{F}_q$, $\Gamma = Aut(\mathbb{F}_q)$, $\mathcal{K}_d$ is the spread corresponding to the desarguesian plane.

One might ask whether it is possible to construct a less trivial example. The answer is yes. Hence, it is worthwhile to study as a first step cases where G is an elementary abelian 2-group and a semifield A over $\mathbb{F}_q$ (non-associative division algebra) with $G \leq Aut(A) \leq$ translation complement).

Background

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. It is not a good choice to start with a finite field $GF(q^4)$ as $Aut(GF(q^4))$ is cyclic by G is not.

We will show now that there is a semifield of order q^4, $q > 3$, q an odd prime, admitting $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ as an automorphism subgroup.

In [Bani-Ata: Semifields as free modules, Quartely Journal of Maths **62** (2011), 1 - 6], it has been proved that: If S is a finite semifield over a finite field admitting an elementary abelian 2-group of automorphisms, then E acts freely on S. If E acts freely of rank 1 on S, and S is even, then $|E| \leq 4$.

In [Bani-Ata and Al-Shemas, Forum Mathematicum, to appear], it is proved that there is no semifield of order q^8, q is odd prime, $q > 3$, admitting an elementary abelian group of automorphisms of order 8.

The Semifield and The 9-structure constants

Lemma 1. *Let A be a semifield with unit e of order q^4, $q > 3$ (q an odd prime) admitting an automorphism group $E \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, then there are 9-constants $t_i, \lambda_i, \mu_i \in \mathbb{F}_q^*$, $i = 1, 2, 3$ which determine A completely.*

Sketch of the proof:
As E acts freely of rank 1, $A \cong \mathbb{F}_q[E] \leftrightarrow \exists b \in A$ such that $\{b^g \mid g \in E\}$ is a base of A. So, let $E = \{1, \sigma_1, \sigma_2, \sigma 3\}$, $A = \{e = e_0, e_1, e_2, e_3\}$. Thus,

$$e_i^{\sigma_j} = \begin{cases} e_i & \text{if } i = j, \\ -e_i & \text{if } i \neq j. \end{cases} \qquad \rightarrow \qquad e_i^2 = t_i e, \qquad i = 1, 2, 3.$$

Thus

$$\begin{aligned} \lambda_3 e_3 &= e_1 e_2 & \qquad e_1 e_3 &= \mu_2 e_2 \\ \lambda_1 e_1 &= e_2 e_3 & \qquad e_3 e_2 &= \mu_1 e_1 \\ \lambda_2 e_2 &= e_3 e_1 & \qquad e_2 e_1 &= \mu_3 e_3. \end{aligned}$$

A matrix form of the semifield

Remark 1. $\forall a \in A$, $\alpha_a : A \to A$

$\alpha_a x = ax \Rightarrow$ *if* $x = x_0 e + x_1 e_1 + x_2 e_2 + x_3 e_3$ *for* $x \in A$, *then*

$$\overline{R}_x = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ t_1 x_1 & x_0 & \mu_2 x_3 & \lambda_3 x_2 \\ t_2 x_2 & \lambda_1 x_3 & x_0 & \mu_3 x_1 \\ t_3 x_3 & \mu_1 x_2 & \lambda_2 x_1 & x_0 \end{bmatrix}.$$

$\overline{R}_x$ *is non-singular if* $(x_0, x_1, x_2, x_3) \neq (0, 0, 0, 0)$.

Remark 2. *This process is reversible in the sense that if the constants* t_i, λ_i, μ_i *are given such that the matrices* R_x *as constructed above are non-singular for all* $x = (x_1, x_2, x_3, x_4) \neq (0, 0, 0, 0)$, *then we can construct a semifield of order* q^4 *admitting a free automorphism group* $E \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ *as follows:*

The 9-constants afford the semifield

Take $A = \mathbb{F}_q^4 = \{(x_0, x_1, x_2, x_3) \mid x_i \in \mathbb{F}_q\}$ define multiplication $x \cdot y = xR_y$ for $x, y \in \mathbb{F}_q^4$ and

$$\sigma_1 = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix}, \sigma_2 = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}, \sigma_3 = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}$$

are automorphisms of A.

Lemma 2. *For any non-square $t \in \mathbb{F}_q^*$ one can choose a basis for A such that $t_1 = t_2 = t_3 = t$ so that all λ_i's are squares and μ_i's are non-squares or the other way around.*

The main result

Theorem 1. *Let q be an odd prime power, $q > 3$, then there exist non-squares $\lambda, t \in \mathbb{F}_q^*$ such that $\lambda^2 + t \neq 0$. Then, the constants $t_1 = t_2 = t_3 = t$, $\lambda_1 = \lambda_2 = \lambda_3 = \lambda$, $\mu_1 = \mu_2 = t/\lambda, \mu_3 = \lambda^3/t$ define A with the above properties.*

Proof.

$$\overline{R}_x = \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ tx_1 & x_0 & \frac{t}{\lambda}x_3 & \lambda x_2 \\ tx_2 & \lambda x_3 & x_0 & \frac{\lambda^3}{t}x_1 \\ tx_3 & \frac{t}{\lambda}x_2 & \lambda x_1 & x_0 \end{bmatrix}.$$

To show that $\overline{R}_x$ is non-singular if $(x_0, x_1, x_2, x_3) \neq (0,0,0,0)$, we conjugate $\overline{R}_x$ with

$g = \begin{bmatrix} 1 & & \\ & 1 & \\ & & \lambda \end{bmatrix}$ and obtain $\square$

The main result

$$R_x^g = \left[\begin{array}{cc|cc} x_0 & x_1 & \lambda x_2 & x_3 \\ t x_1 & x_0 & t x_3 & \lambda x_2 \\ \hline \frac{t}{\lambda} x_2 & x_3 & x_0 & \frac{\lambda^2}{t} x_1 \\ t x_3 & \frac{t}{\lambda} x_2 & \lambda^2 x_1 & x_0 \end{array}\right] = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right].$$

Hence, $\det(R_x) = \det(R_x^g) = \det(A_{11}A_{22} - A_{12}A_{21}) =$

$$\det \begin{bmatrix} x_0^2 + \lambda^2 x_1^2 - t(x_2^2 + x_3^2) & (\lambda^2 + t)\left[\frac{x_0 x_1}{t} - \frac{x_2 x_3}{\lambda}\right] \\ t(\lambda^2 + t)\left[\frac{x_0 x_1}{t} - \frac{x_2 x_3}{\lambda}\right] & x_0^2 + \lambda^2 x_1^2 - t(x_2^2 + x_3^2) \end{bmatrix} = \begin{vmatrix} Y & Z \\ tZ & Y \end{vmatrix} = 0$$

if and only if $Y = Z = 0$ as t is non-square and $\lambda^2 + t \neq 0$, then $(x_0, x_1, x_2, x_3) = (0, 0, 0, 0)$. Hence, the claim.

Thank You

The End