ELSEVIER

Journal of Pure and Applied Algebra 178 (2003) 297–306

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

On the product of two primitive elements of maximal subfields of a finite field

B.V. Petrenko

Department of Mathematics, University of Illinois, 1409 West Green Street, Urbana, IL 61801, USA

Received 14 March 2002; accepted 19 June 2002

Communicated by J. Walker

Abstract

Let $\mathbb{F}_r$ denote a finite field with r elements. Let q be a power of a prime, and p_1, p_2, p_3 be distinct primes. Put

$$y_1 = p_1 p_2, \quad y_2 = p_1 p_3, \quad y_3 = p_2 p_3, \quad z = p_1 p_2 p_3,$$

$$A = \{(t_1, t_2) \in \mathbb{F}_{q^{y_1}} \times \mathbb{F}_{q^{y_2}} \mid \mathbb{F}_q(t_1) = \mathbb{F}_{q^{y_1}}, \mathbb{F}_q(t_2) = \mathbb{F}_{q^{y_2}}, \mathbb{F}_q(t_1 t_2) \neq \mathbb{F}_{q^z}\}.$$

We express the number of elements in A in terms of q, p_1, p_2, p_3.

MSC: 11T30; 11A99; 12E20

1. Introduction

The following question has been studied by Browkin et al. [3], Isaacs [4], Kaplansky [5], and Petrenko [8]:

Let K be a field and $L_1 = K(a_1)$, $L_2 = K(a_2)$ be field extensions of finite degrees d_1, d_2, respectively. What conditions should one place on K, a_1, a_2, d_1, d_2 to ensure that $K(a_1, a_2) = K(a_1 + a_2)$?

In this paper we investigate when for a finite field K we have $K(a_1, a_2) = K(a_1 a_2)$. We look for criteria in terms of d_1, d_2, char(K). Firstly, we observe that $\gcd(d_1, d_2) = 1$ implies $K(a_1, a_2) = K(a_1 a_2)$ (Remark 3). Hence, it is natural to investigate the case $\gcd(d_1, d_2) > 1$. This leads to the following question.[1]

E-mail address: petrenko@uiuc.edu (B.V. Petrenko).

[1] $\mathbb{F}_r$ denotes a field of r elements and $|W|$ denotes the number of elements in a finite set W.

0022-4049/03/$ - see front matter

PII: S0022-4049(02)00196-2

Let q be a power of a prime, and p_1, p_2, p_3 be distinct primes. Put

$$y_1 = p_1 p_2, \quad y_2 = p_1 p_3, \quad y_3 = p_2 p_3, \quad z = p_1 p_2 p_3,$$

$$A = \{(t_1, t_2) \in \mathbb{F}_{q^{y_1}} \times \mathbb{F}_{q^{y_2}} \mid \mathbb{F}_q(t_1) = \mathbb{F}_{q^{y_1}},\ \mathbb{F}_q(t_2) = \mathbb{F}_{q^{y_2}},\ \mathbb{F}_q(t_1 t_2) \neq \mathbb{F}_{q^z}\}.$$

What is $|A|$ in terms of q, p_1, p_2, p_3?

We answer this question in Theorem 10. This allows us to show that if primitive elements $t_1 \in \mathbb{F}_{q^{y_1}}$, $t_2 \in \mathbb{F}_{q^{y_2}}$ are randomly chosen under a uniform distribution, then the probability P of $\mathbb{F}_q(t_1 t_2) = \mathbb{F}_{q^z}$ tends to 1 as $(q, p_1, p_2, p_3) \to +\infty$ under some norm (Proposition 14). It turns out that the smallest value of $P(q, p_1, p_2, p_3)$ is $P(2, 2, 3, 5) = \frac{295}{297} > 0.993$ (Proposition 14).

If we replace p_1, p_2, p_3 with arbitrary pairwise relatively prime positive integers, then the formula for $|A|$ in Theorem 10 no longer holds (Example 13). However, if we consider W, the subgroup of $\mathbb{F}^*_{q^{y_1}} \times \mathbb{F}^*_{q^{y_2}}$ generated by A, then we obtain the formula for $|W|$ that is valid when p_1, p_2, p_3 are replaced with m_1, m_2, m_3, distinct pairwise relatively prime positive integers (Remark 15 and Theorem 16).

We interpret Theorems 10 and 16 in terms of counting points of algebraic sets (Sections 5.1 and 5.2) and determining the kernel of a group homomorphism (Section 5.3).

2. Definitions and notation

We refer to [1,5–7,9,10] for standard definitions.

The cardinality of a finite set W is denoted by $|W|$.

If L is a field, we write L^* for the *multiplicative group* of L.

If L, M are fields, we denote their *compositum* by LM.

If a field L is an extension of a field K, then $(L:K)$ denotes the *degree* of L/K (it is equal to $\dim_K L$ by definition). If L/K is Galois, we write $Gal(L/K)$ for the *Galois group* of L/K. If $Gal(L/K)$ is finite cyclic, then L/K is called *cyclic*.

If L/K is a field extension, then $a \in L$ is called a *primitive element* (of this extension) if L is the smallest subfield of L containing $K \cup \{a\}$. In this case we write $L = K(a)$ and say that L/K is *simple*. The primitive element theorem states that L/K is simple if and only if it has finitely many intermediate subfields (see, for example, [6, Chapter V, Section 4, Theorem 4.6]). In particular, any Galois field extension is simple.

Define the set

$$Pr(L/K) = \{a \in L \mid K(a) = L\}.$$

We note that what we call a "primitive element" is called a "defining element" in [7], and a "primitive element" of a finite field, according to [7], is a generator of the multiplicative group.

$\mathbb{F}_r$, $\mathbb{F}_r^{\mathrm{alg}}$, $\mathbb{N}$, $\mathbb{P}$, $\mathbb{Z}$ denote a finite field of r elements, an algebraic closure of $\mathbb{F}_r$, the natural numbers, the positive primes, the integers, respectively.

Let $m, n \in \mathbb{N}$.

(1) If m divides n, we denote this by $m \mid n$.

(2) If $m \geqslant 2$, then define

$$\mathrm{ord}_m(n) = \max\{k \in \mathbb{N} \cup \{0\} \mid m^k \text{ divides } n\}.$$

To save repetition throughout the paper, we introduce the *subscripts* $i \in \{1, 2\}$ and $j \in \{1, 2, 3\}$.

Put

$$S_j = Pr(\mathbb{F}_{q^{y_j}}/\mathbb{F}_q).$$

Let q be a power of a prime p', and p_1, p_2, p_3 be distinct primes. Put

$$y_1 = p_1 p_2, \quad y_2 = p_1 p_3, \quad y_3 = p_2 p_3, \quad z = p_1 p_2 p_3,$$

$$A = \{(t_1, t_2) \in S_1 \times S_2 \mid \mathbb{F}_q(t_1 t_2) = \mathbb{F}_{q^{y_3}}\}.$$

It follows from Lemma 1 below that this definition of A is equivalent to the one given in Section 1.

Let $m_1, m_2, m_3 \in \mathbb{N}$ be pairwise relatively prime. Define the group

$$V = \{(t_1, t_2, t_3) \in \mathbb{F}^*_{q^{m_1 m_2}} \times \mathbb{F}^*_{q^{m_1 m_3}} \times \mathbb{F}^*_{q^{m_2 m_3}} \mid t_1 t_2 t_3 = 1\}.$$

3. Preliminary results

Let F_2/F_1 be a cyclic field extension and $a_1, a_2 \in F_2$. Lemmas 1 and 2 below relate $(F_1(a_1 a_2) : F_1)$ to $(F_1(a_1) : F_1)$ and $(F_1(a_2) : F_1)$.

Lemma 1. *Let F_2/F_1 be a cyclic field extension of degree d and $a_1, a_2 \in F_2$ such that $F_2 = F_1(a_1, a_2)$. Let $(F_1(a_i) : F_1) = d_i$ and $\pi = \{p \in \mathbb{P} \mid \mathrm{ord}_p(d_1) \neq \mathrm{ord}_p(d_2)\}$. Define $d_0 = (F_1(a_1 a_2) : F_1)$ and $d' = \prod_{p \in \pi} p^{\max_i\{\mathrm{ord}_p(d_i)\}}$. Then $\mathrm{lcm}(d_1, d_2) = d$ and $d' | d_0$.*

Proof. Put

$$I_i = Gal(F_2/F_1(a_i)), \quad J = Gal(F_2/F_1(a_1 a_2)).$$

Then from

$$F_2 = F_1(a_1)F_1(a_2) = F_1(a_i)F_1(a_1 a_2),$$

we deduce that

$$I_i \cap J = I_1 \cap I_2 = \{\mathrm{id}_{F_2}\}.$$

It follows that

$$\gcd(|I_i|, |J|) = \gcd(|I_1|, |I_2|) = 1.$$

Therefore, by Galois theory ([5, Part 1, Section 3]),

$$\mathrm{lcm}(d_i, d_0) = \mathrm{lcm}(d_1, d_2) = d.$$

We see that any $p \in \pi$ divides d_0 and $\mathrm{ord}_p(d_0) = \mathrm{ord}_p(d)$. Consequently, $\prod_{p \in \pi} p^{\max_i\{\mathrm{ord}_p(d_i)\}}$ divides d_0. $\square$

Lemma 2. *Let* $\pi' = \{p \text{ prime} \mid p \text{ divides } d\}$. *If* $\pi' = \pi$, *then* $F_1(a_1a_2) = F_2$.

Proof. By Lemma 1, $d' = \prod_{p\in\pi'} p^{\max_i\{\operatorname{ord}_p(d_i)\}} = \operatorname{lcm}(d_1, d_2) = d$.
Hence, $(F_2 : F_1) = (F_1(a_1a_2) : F_1)$ and $F_2 = F_1(a_1a_2)$. □

Remark 3. The conditions of Lemma 2 are satisfied when $\gcd(d_1, d_2) = 1$.

We would like to recall Lemma 3.5 of [8].

Lemma 4. *Let* G *be a group,* G_1, G_2, G_3 *subgroups of* G, *and* $G_0 = \bigcap_{j=1}^{3} G_j$. *Put* $G_j^{(0)} = G_j \setminus G_0$. *Define*

$$A_1 = \{(g_2g_1^{-1}, g_1g_3) \mid g_j \in G_j^{(0)}\} \quad \text{and} \quad B = \{(g_2g_1^{-1}, g_1g_3) \mid g_j \in G_j\}.$$

Then $|A_1||G_0| = \prod_j |G_j^{(0)}|$ *and* $|B||G_0| = \prod_j |G_j|$.

We sketch the idea of the proof for the convenience of the reader. Define the surjective map $\varphi : \prod_j G_j^{(0)} \to A_1$, $(g_1, g_2, g_3) \mapsto (g_2g_1^{-1}, g_1g_3)$. For any $t \in A_1$, one can show that $|\varphi^{-1}(t)| = |G_0|$. This establishes the formula for $|A_1|$. The formula for $|B|$ is obtained similarly.

Next, we prove two number-theoretic lemmas.

Lemma 5. *Let* $a, b, c \in \mathbb{N}$. *Then*

(1) $\operatorname{lcm}(\gcd(a, b), \gcd(a, c)) = \gcd(a, \operatorname{lcm}(b, c))$.
(2) *If* $a \geqslant 2$, *then* $\gcd(a^b - 1, a^c - 1) = a^{\gcd(b,c)} - 1$.

Proof.

(1) The result follows because $\mathbb{N}$ under division is a distributive lattice (see [1, Chapter XI, Section 3] for details).
(2) Put $\alpha = a^b - 1$, $\beta = a^c - 1$, $\gamma = a^{\gcd(b,c)} - 1$. We see that $\gamma \mid \alpha, \beta$; hence $\gamma \mid \gcd(\alpha, \beta)$.
Let $r \in \mathbb{N}$ be such that $r \mid \alpha, r \mid \beta$. Without loss of generality, $b > c$. Then $r \mid a^{b-c} - 1$. Therefore, $r \mid \gamma$ by Euclid's algorithm.
We have shown that $\gcd(\alpha, \beta) \mid \gamma$ and $\gamma \mid \gcd(\alpha, \beta)$. We conclude that the two numbers are equal. □

Before proving the following lemma, we recall that m_1, m_2, m_3 are assumed to be pairwise relatively prime.

Lemma 6. *Let* $n \in \mathbb{N}$, $n \geqslant 2$, *then*

$$\frac{(n^{m_1} - 1)(n^{m_2} - 1)}{n - 1} = \gcd(n^{m_1m_2} - 1, \operatorname{lcm}(n^{m_1m_3} - 1, n^{m_2m_3} - 1)).$$

Proof. Put $a = n^{m_1m_2} - 1,\ b = n^{m_1m_3} - 1,\ c = n^{m_2m_3} - 1$. Then by Lemma 5,

$$\begin{aligned}\gcd(a, \operatorname{lcm}(b,c)) &= \operatorname{lcm}(\gcd(a,b), \gcd(a,c)) = \operatorname{lcm}(n^{m_1} - 1, n^{m_2} - 1)\\ &= \frac{(n^{m_1} - 1)(n^{m_2} - 1)}{n-1}. \qquad \square\end{aligned}$$

Next, we apply Lemma 6 to finite fields.

Lemma 7. $\mathbb{F}^*_{q^{m_1}}\mathbb{F}^*_{q^{m_2}} = \mathbb{F}^*_{q^{m_1m_2}} \cap (\mathbb{F}^*_{q^{m_1m_3}}\mathbb{F}^*_{q^{m_2m_3}})$.

Proof. We see that $|\mathbb{F}^*_{q^{m_1}}\mathbb{F}^*_{q^{m_2}}| = \frac{(q^{m_1}-1)(q^{m_2}-1)}{q-1}$ and

$$|\mathbb{F}^*_{q^{m_1m_2}} \cap (\mathbb{F}^*_{q^{m_1m_3}}\mathbb{F}^*_{q^{m_2m_3}})| = \gcd(q^{m_1m_2} - 1, \operatorname{lcm}(q^{m_1m_3} - 1, q^{m_2m_3} - 1)).$$

The group $\mathbb{F}^*_{q^{m_1m_2m_3}}$ is cyclic. Therefore, the result follows from Lemma 6. $\square$

We establish two calculus lemmas below. They will be used in the proof of Proposition 14.

Lemma 8. *The function* $f(t,x,y) = (t^x - t)(t^y - t)/(t^{xy} - t^x - t^y + t)$ *attains its maximum in the set* $\Omega_1 = \{(t,x,y) \in \mathbb{N}^3 \mid t \geqslant 2,\ x \geqslant 2,\ y \geqslant 3\}$ *only at the point* $(2,2,3)$.

Proof. We have

$$\frac{\partial f}{\partial x} = -\frac{(t^y - t)(t^{x+y} + t^{x(1+y)}(y-1) - yt^{1+xy})\ln t}{(t - t^x - t^y + t^{xy})^2} < 0,$$

$$\frac{\partial f}{\partial y} = -\frac{(t^x - t)(t^{x+y} + t^{y(1+x)}(x-1) - xt^{1+xy})\ln t}{(t - t^x - t^y + t^{xy})^2} < 0.$$

We conclude that $f(t,x,y)$ is a strictly decreasing function in x and y. It would be sufficient to show that $f(t,2,3)$ is a decreasing function.

Indeed, let $(t_0,x_0,y_0) \in \Omega_1$ be such that $(t_0,x_0,y_0) \neq (2,2,3)$ and $f(t_0,x_0,y_0) \geqslant f(2,2,3)$. Suppose that $x_0 > 2$, then

$$f(t_0,x_0,y_0) < f(t_0,2,y_0) \leqslant f(t_0,2,3) \leqslant f(2,2,3),$$

a contradiction. Similarly, $y_0 > 3$ cannot occur. Therefore, $x_0 = 2$ and $y_0 = 3$. If $t_0 > 2$, then

$$f(t_0,x_0,y_0) = f(t_0,2,3) < f(2,2,3),$$

a contradiction. It follows that (t_0,x_0,y_0) does not exist.

Put $h(t) = f(t,2,3)$. We have

$$h'(t) = \frac{1 - 2t + t^2 + 2t^3 - t^4}{(-1 + t + t^3)^2} = -\frac{(t^2 - t - 1 - \sqrt{2})(t^2 - t - 1 + \sqrt{2})}{(-1 + t + t^3)^2}.$$

The equation $1-2t+t^2+2t^3-t^4=0$ has exactly two real roots: $t_1=\frac{1}{2}(1-\sqrt{5+4\sqrt{2}})<0$ and $t_2=\frac{1}{2}(1+\sqrt{5+4\sqrt{2}})$. We have $2<t_2<3$ and $h'(t)<0$ for $t>t_2$. Since

$$h(2)=\tfrac{2}{9}>h(3)=\tfrac{6}{29},$$

it follows that $h(t)$ is a strictly decreasing function. □

Lemma 9. *The function* $g(t,x,y)=(t^y-t)/(t^{xy}-t^x-t^y+t)$ *attains its maximum in the set* $\Omega_2=\{(t,x,y)\mid t\geqslant 2,\ x\geqslant 2,\ y\geqslant 5\}$ *only at the point* $(2,2,5)$.

Proof. We have

$$\frac{\partial g}{\partial x}=-\frac{(t^y-t)(t^x-yt^{xy})\ln t}{(t-t^x-t^y+t^{xy})^2}<0,$$

$$\frac{\partial g}{\partial y}=-\frac{(t^{x+y}+(x-1)t^{y(1+x)}-xt^{1+xy})\ln t}{(t-t^x-t^y+t^{xy})^2}<0.$$

Define the function

$$s(t)=g(t,2,5)=\frac{1}{t^5+t-1}.$$

Then

$$s'(t)=-\frac{1+5t^4}{(t^5+t-1)^2}<0.$$

By an argument similar to the one used in the proof of Lemma 8, we see that $(2,2,5)$ is the only point of maximum for $g(t,x,y)$ in Ω_2. □

4. Properties of A and V

We now state and prove the main result of this paper.

Theorem 10. (1) *The following equalities hold*:

(a) $|A|=\frac{\prod_{j=1}^{3}(q^{p_j}-q)}{q-1}$,
(b) $A=\{(\beta_2\beta_1^{-1},\beta_1\beta_3)\mid\beta_j\in\mathbb{F}_{q^{p_j}}\setminus\mathbb{F}_q\}$,
(2) *For all* $t_1\in\mathbb{F}^*_{q^{y_1}}\setminus(\mathbb{F}^*_{q^{p_1}}\mathbb{F}^*_{q^{p_2}})$, $t_2\in\mathbb{F}^*_{q^{y_2}}\setminus\mathbb{F}^*_{q^{p_1}}$, *we have* $\mathbb{F}_q(t_1t_2)=\mathbb{F}_{q^z}$.
(3) *The image of the map* $\kappa:(t_1,t_2)\to(\mathbb{F}_q(t_1t_2):\mathbb{F}_q)$, $(t_1,t_2)\in S_1\times S_2$, *is* $\{y_3,z\}$.

Proof.

(1) Define the groups $G=\mathbb{F}^*_{q^z}$, $G_j=\mathbb{F}^*_{q^{p_j}}$ (see Lemma 4). Then $G_0=\mathbb{F}^*_q$. Put $A_1=\{(\beta_2\beta_1^{-1},\beta_1\beta_3)\mid\beta_j\in\mathbb{F}_{q^{p_j}}\setminus\mathbb{F}_q\}$.

We claim that $A_1=A$.

Let us prove that $A_1\subseteq A$. Let $(t_1,t_2)\in A_1$, then $t_1=\beta_1^{-1}\beta_2$ and $t_2=\beta_1\beta_3$ for some $\beta_j\in G_j^{(0)}$. Then $\mathbb{F}_q(t_i)=\mathbb{F}_{q^{y_i}}$, $\mathbb{F}_q(t_1t_2)=\mathbb{F}_q(\beta_2\beta_3)=\mathbb{F}_{q^{y_3}}$. We conclude that $(t_1,t_2)\in A$.

Let us prove that $A \subseteq A_1$. Suppose not. Let $(t_1,t_2) \in A \setminus A_1$. By Lemma 1, $\mathbb{F}_q(t_1t_2) = \mathbb{F}_{q^{y_3}}$. Next, by Lemma 7, $t_1 \in \mathbb{F}^*_{q^{p_1}}\mathbb{F}^*_{p^{p_2}}$ and $t_2 \in \mathbb{F}^*_{q^{p_1}}\mathbb{F}^*_{q^{p_3}}$. It follows that $t_1 = \beta_2\beta_1^{-1}$ and $t_2 = \beta_1\beta_3$ for some $\beta_j \in \mathbb{F}^*_{q^{p_i}}$.

From $A_1 = A$, Lemmas 4 and 7, we deduce 1(a) and 1(b).

(2) Suppose not. Then $\mathbb{F}_q(t_1t_2) = \mathbb{F}_{q^{y_3}}$ by Lemma 1. If $t_2 \in \mathbb{F}^*_{q^{y_2}} \setminus (\mathbb{F}^*_{q^{p_1}}\mathbb{F}^*_{q^{p_3}})$, then $(t_1,t_2) \in A$ contradicts $1(b)$. Therefore, $t_2 \in \mathbb{F}^*_{q^{p_1}}\mathbb{F}^*_{q^{p_3}}$. Put

$$D = \{t \in \mathbb{F}_{q^{y_1}} \mid tt_2 \in \mathbb{F}_{q^{y_3}}\}.$$

If $t', t'' \in D$, then

$$\frac{t'}{t''} = \frac{t't_2}{t''t_2} \in \mathbb{F}^*_{q^{y_1}} \cap \mathbb{F}^*_{q^{y_3}} = \mathbb{F}^*_{q^{p_2}}.$$

Hence $|D| \leqslant q^{p_2} - 1$. Write $t_2 = \beta_1^{-1}\beta_3$ for some $\beta_1 \in \mathbb{F}^*_{q^{p_1}}$, $\beta_3 \in \mathbb{F}^*_{q^{p_3}}$. Put

$$D_1 = \{\beta_1\beta_2 \mid \beta_2 \in \mathbb{F}^*_{q^{p_2}}\}.$$

Then $|D_1| = q^{p_2} - 1$ and $D_1 \subseteq D$. Hence, $D = D_1$. This shows that $t_1 \in \mathbb{F}^*_{q^{p_1}}\mathbb{F}^*_{q^{p_2}}$, a contradiction.

(3) Lemma 1 implies $\operatorname{Im}\kappa \subseteq \{y_3, z\}$. Since $\kappa^{-1}(y_3) = A$ and $0 < |A| < |S_1 \times S_2|$, we have $\operatorname{Im}\kappa = \{y_3, z\}$. □

Remark 11. The case $q = p_1 = 2,\ p_2 = 3,\ p_3 = 5$ was first handled by the author by the computer system MAGMA [2], inspiring the general method.

Remark 12. The statement of Theorem 10 is not true in general if we no longer require that p_1, p_2, p_3 be prime, as the following example shows.

Example 13. Observe that the group $Gal(\mathbb{F}_{q^z}/\mathbb{F}_q)$ acts on the set A by the rule $\sigma(t_1,t_2) := (\sigma(t_1), \sigma(t_2))$. We see that any element of A has trivial stabilizer. Hence, $|Gal(\mathbb{F}_{q^z}/\mathbb{F}_q)| = z$ divides $|A|$. In case $q = p_1 = 2,\ p_2 = 3,\ p_3 = 35$, for example, $z = 210$ does not divide $(1/(q-1))\prod_j (q^{p_j} - q) = 412316860392$. We conclude that $|A| \neq (1/(q-1))\prod_j (q^{p_j} - q)$ here.

Proposition 14. *Let $(s_1,s_2) \in S_1 \times S_2$ be randomly chosen under a uniform distribution. Then the probability of $\mathbb{F}_q(t_1t_2) = \mathbb{F}_{q^z}$ is*

$$P = P(q, p_1, p_2, p_3) = 1 - \frac{(q^{p_1} - q)(q^{p_2} - q)(q^{p_3} - q)}{(q-1)(q^{y_1} - q^{p_1} - q^{p_2} + q)(q^{y_2} - q^{p_1} - q^{p_3} + q)}.$$

$P(q, p_1, p_2, p_3)$ attains its minimum only at the point $(2,2,3,5)$, $P(2,2,3,5) = \frac{295}{297}$, and $\lim_{(q,p_1,p_2,p_3)\to+\infty} P = 1$.

Proof. By definition, $P = 1 - |A|/(|S_1||S_2|)$, where $|A| = (1/(q-1))\prod_j (q^{p_j} - q)$ by Theorem 10. This establishes the formula for P. Define $v(q, p_1, p_2, p_3) = 1 - P(q, p_1, p_2, p_3)$. We see that in terms of Lemmas 8 and 9, $v(q, p_1, p_2, p_3) = (1/(q-1)) f(q, p_1, p_2) g(q, p_1, p_3)$. Therefore, Lemmas 8 and 9 imply that $v(q, p_1, p_2, p_3)$ attains its maximum only at the point $(2,2,3,5)$.

We observe that

$$0 \leqslant v(q, p_1, p_2, p_3) \leqslant \frac{q^{p_1+p_2+p_3}}{\frac{1}{2}q^{p_1 p_2}\frac{1}{2}q^{p_1 p_3}} \to 0$$

as $(q, p_1, p_2, p_3) \to +\infty$, and so $\lim_{(q, p_1, p_2, p_3)\to+\infty} P = 1$. □

Remark 15. By Theorem 10, the subgroup W of $\mathbb{F}^*_{q^{y_1}}\mathbb{F}^*_{q^{y_2}}$ generated by A is $W = \{(\beta_2\beta_1^{-1}, \beta_1\beta_3) \mid \beta_j \in \mathbb{F}^*_{q^{p_j}}\}$. Then

$$|W| = \frac{1}{q-1}\prod_j (q^{p_j} - 1)$$

by Lemma 4. Example 13 above shows that the formula for $|A|$ in Theorem 10 does not hold in general if p_1, p_2, p_3 are composite. Nevertheless, Theorem 16 below implies that the formula for $|W|$ holds if we replace p_1, p_2, p_3 with pairwise relatively prime positive integers m_1, m_2, m_3.

Theorem 16. (1) $|V| = (1/(q-1))\prod_{j=1}^{3}(q^{m_j} - 1)$.

(2) $V = \{(\beta_2\beta_1^{-1}, \beta_1\beta_3^{-1}, \beta_3\beta_2^{-1}) \mid \beta_j \in \mathbb{F}^*_{q^{m_j}}\}$.

Proof. Consider the group epimorphism

$$\theta : V \to \mathbb{F}^*_{q^{m_1}}\mathbb{F}^*_{q^{m_2}}, (t_1, t_2, t_3) \mapsto t_2 t_3.$$

This map is well defined by Lemma 7. We see that

$$\mathrm{Ker}(\theta) = \{(1, t^{-1}, t) \mid t \in \mathbb{F}^*_{q^{m_3}}\}.$$

Therefore,

$$|V| = |\mathrm{Ker}(\theta)||\mathrm{Im}(\theta)| = \frac{1}{q-1}\prod_j (q^{m_j} - 1).$$

This proves Part 1.

To prove Part 2, we define the groups

$$V_1 = \{(\beta_2\beta_1^{-1}, \beta_1\beta_3^{-1}, \beta_3\beta_2^{-1}) \mid \beta_j \in \mathbb{F}^*_{q^{m_j}}\}, \quad W = \{(\beta_2\beta_1^{-1}, \beta_1\beta_3) \mid \beta_j \in \mathbb{F}^*_{q^{m_j}}\}.$$

They are isomorphic via the map $(v_1, v_2, v_3) \mapsto (v_1, v_2)$. Hence, $|V_1| = |W|$. We observe that $V_1 \subseteq V$. Define the groups $G_j = \mathbb{F}^*_{q^{m_j}}$, $G = \mathbb{F}^*_{q^{m_1 m_2 m_3}}$. Then by Lemma 4, $|W| = (1/(q-1))\prod_j (q^{m_j} - 1)$. Hence, by Part 1, $|V_1| = |W| = |V|$. □

5. Applications

We see that A and V are algebraic sets over $\mathbb{F}_q^{\mathrm{alg}}$. Therefore, by Theorems 10 and 16, we know the number of solutions of the systems of polynomial equations defining these sets. We make this observation precise in Sections 5.1 and 5.2 below.

Since the group $\mathbb{F}^*_{q^z}$ is cyclic, there is a bijection between the points of V and the kernel of a group homomorphism. We describe this homomorphism in Section 5.3 below.

5.1. V as an algebraic set

Note that V is defined over $\mathbb{F}_q^{\mathrm{alg}}$ by the following system of polynomial equations:

$$x_1^{q^{m_1 m_2}} = x_1,$$

$$x_2^{q^{m_1 m_3}} = x_2,$$

$$x_3^{q^{m_2 m_3}} = x_3,$$

$$x_1 x_2 x_3 = 1.$$

Hence, by Theorem 16, this system has $|V| = (q-1)^{-1}\prod_j (q^{m_j} - 1)$ solutions in $\mathbb{F}_q^{\mathrm{alg}}$.

5.2. A as an algebraic set

We observe that A is the set of ordered pairs (x_1, x_2) satisfying the following system of polynomial equations over $\mathbb{F}_q^{\mathrm{alg}}$:

$$\prod_{s_j \in S_j} (x_j - s_j) = 0,$$

$$x_1 x_2 x_3 = 1.$$

We observe that $\prod_{s_j \in S_j} (x_j - s_j) \in \mathbb{F}_{p'}[x_j] \subseteq \mathbb{F}_q[x_j]$, because they can be expressed as products of cyclotomic polynomials. By Theorem 10, this system has $(1/(q-1))\prod_j (q^{p_j} - q)$ solutions in $\mathbb{F}_q^{\mathrm{alg}}$.

5.3. $|V|$ as the size of the kernel of a group homomorphism

We shall give another interpretation of $|V|$. Let $\mu_j = q^{m_j} - 1$, $v_1 = q^{m_1 m_2} - 1$, $v_2 = q^{m_1 m_3} - 1$, $v_3 = q^{m_2 m_3} - 1$, and $v = q^{m_1 m_2 m_3} - 1$. Consider the group homomorphism

$$\eta : (\mathbb{Z}/v\mathbb{Z})^3 \to (\mathbb{Z}/v\mathbb{Z})^4$$

$$(m_1, m_2, m_3) \mapsto (v_1 m_1, v_2 m_2, v_3 m_3, m_1 + m_2 + m_3).$$

Then by Theorem 10, $|\mathrm{Ker}(\eta)| = |V| = (q-1)^{-1}\prod_{j=1}^{3} (q^{m_j} - 1)$. Moreover, we know that

$$\mathrm{Ker}(\eta) = \{(m_j) \in (\mathbb{Z}/v\mathbb{Z})^3 \mid m_1 = n_2 - n_1, m_2 = n_1 - n_3, m_3 = n_3 - n_2$$
$$\text{for some } n_j \in (\mathbb{Z}/v\mathbb{Z}), \text{ such that } n_j \mu_j = 0\}.$$

Acknowledgements

I thank Nigel Boston, Ilya Kapovich, Leon McCulloh, Everett C. Dade, Jimmy McLaughlin, Derek Robinson, Alexander Tumanov, Stephen Ullom, and Alexandru Zaharescu for helpful discussions.

References

[1] G. Birkhoff, S. MacLane, A Survey of Modern Algebra, Macmillan, New York, 1965.
[2] W. Bosma, J. Cannon, Handbook of MAGMA Functions, School of Mathematics and Statistics, University of Sydney, Sydney, 1993.
[3] J. Browkin, B. Diviš, A. Schinzel, Addition of sequences in general fields, Monatsh. Math. 82 (1976) 261–268.
[4] I.M. Isaacs, Degrees of sums in a separable field extension, Proc. Amer. Math. Soc. 25 (1970) 638–641.
[5] I. Kaplansky, Fields and Rings, The University of Chicago Press, Chicago, 1972.
[6] S. Lang, Algebra, Springer, Berlin, GTM 211, 2002.
[7] R. Lidl, H. Niederreiter, Finite Fields, in: Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press, Cambridge, 1997.
[8] B.V. Petrenko, On the sum of two primitive elements of maximal subfields of a finite field, 2001, to appear in Finite Fields and Their Applications.
[9] D.J.S. Robinson, A Course in the Theory of Groups, Springer, Berlin, GTM 80, 1996.
[10] J.J. Rotman, An Introduction to the Theory of Groups, Springer, Berlin, GTM 148, 1995.