Advances in Group Theory and Applications
© 2020 AGTA - www.advgrouptheory.com/journal
10 (2020), pp. 67–81 ISSN: 2499-1287
DOI: 10.32037/agta-2020-010

Conjugacy Class Sizes in Affine Semi-linear Groups

Hossein Shahrtash

(*Received Jan. 20, 2020; Accepted Mar. 16, 2020 — Communicated by L.S. Kazarin*)

Abstract

The aim of this work is to study the structure and sizes of conjugacy classes in certain affine semi-linear groups. This provides a wealth of finite groups of small conjugate rank that are solvable and non-nilpotent.

Mathematics Subject Classification (2020): 20E45

Keywords: affine semi-linear group; conjugacy class

1 Introduction

In this work we study the conjugacy classes of affine semi-linear groups. These groups play an important role in the study of solvable linear groups and solvable permutation groups and have been studied, for example, in [2]. Given a prime power q^n, where q is a prime and $n > 1$, F_{q^n} will denote the finite field of size q^n. We note that $F^*_{q^n}$ is a cyclic group of order $q^n - 1$. Another component of the structure of an affine semi-linear group is $\mathrm{Gal}(F_{q^n}/F_q)$, which is a cyclic group of order n, generated by the automorphism f of F_{q^n} defined by $f(x) = x^q$. To construct an affine semi-linear group, we begin with the action of $F^*_{q^n}$ on $F^+_{q^n}$ via multiplication, giving rise to the semidirect product $F^+_{q^n} \rtimes F^*_{q^n}$, which is a semi-linear group. Next, we will consider the natural action of $\mathrm{Gal}(F_{q^n}/F_q)$ on $F^+_{q^n} \rtimes F^*_{q^n}$, which gives rise to the affine semi-linear group

$$G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$$

with the following group multiplication:

$$(x,t,\tau)(y,s,\sigma) = \left(x + t^{-1}y^{\tau^{-1}}, ts^{\tau^{-1}}, \tau\sigma\right)$$

In this paper we fully calculate the conjugacy classes of an affine semi-linear group

$$G = (F^+_{q^p} \rtimes F^*_{q^p}) \rtimes \mathrm{Gal}(F_{q^p}/F_q),$$

where p and q are primes, and our main results are Theorems 3.2 and 3.3.

Throughout this paper all groups are finite. If x is an element of a group G, we denote by x^G the conjugacy class of x in G. We use $\mathrm{cs}(G)$ to denote the set of all conjugacy class sizes of G, and the conjugate rank of G, $\mathrm{crk}(G)$, is given by $\mathrm{crk}(G) = |\mathrm{cs}(G)| - 1$. We also use N and Tr to denote the norm and trace functions respectively.

2 Calculating the conjugacy classes in affine semi-linear groups

We start off with the following lemma which facilitates the calculation of the conjugacy classes of $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$.

Lemma 2.1 *$F^+_{q^n}$ is a normal subgroup of $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$.*

Proof — Let

$$(x,t,\tau) \in G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q) \quad \text{and} \quad (y,1,1) \in F^+_{q^n}$$

be arbitrary elements. Then we have

$$\begin{aligned}&(x,t,\tau)^{-1}(y,1,1)(x,t,\tau)\\ &= (t^\tau(-x)^\tau, (t^{-1})^\tau, \tau^{-1})(y,1,1)(x,t,\tau)\end{aligned}$$

$$= (t^\tau(-x)^\tau + t^\tau y^\tau, (t^{-1})^\tau, \tau^{-1})(x, t, \tau)$$
$$= (t^\tau(-x)^\tau + t^\tau y^\tau + t^\tau x^\tau, 1, 1) = (t^\tau y^\tau, 1, 1)$$

which lies in $F^+_{q^n}$. □

Corollary 2.2 *The finite group* $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *has a conjugacy class of size* $q^n - 1$.

Proof — It follows by the proof of Lemma 2.1 that we have

$$(y, 1, 1)^G = \{((t^\tau y^\tau, 1, 1) | t \in F^*_{q^n}, \tau \in \mathrm{Gal}(F_{q^n}/F_q)\}.$$

Therefore if $(0, 1, 1) \neq (y, 1, 1) \in G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$, then we have

$$(y, 1, 1)^G = \{(x, 1, 1) | x \in F^*_{q^n}\}.$$

The statement is proved. □

Corollary 2.3 *Let* (x, t, τ) *and* (y, r, σ) *be elements of*

$$G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$$

that lie in the same conjugacy classes. Then (t, τ) *and* (r, σ) *must be conjugate in* $F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)$. *Also we must have* $\tau = \sigma$.

Proof — These follow from $F^+_{q^n} \trianglelefteq (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ and $F^+_{q^n} \rtimes F^*_{q^n} \trianglelefteq (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$. □

Remark 2.4 Let $\sigma \in \mathrm{Gal}(F_{q^n}/F_q)$. Then $|C_{\mathrm{Gal}(F_{q^n}/F_q)}(\sigma)| = n$. This follows from the fact that $\mathrm{Gal}(F_{q^n}/F_q)$ is a cyclic group of order n.

Lemma 2.5 *Let* $(\lambda, \sigma) \in F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)$, *where* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$. *Then we have* $|C_{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda, \sigma)| = n(q - 1)$.

Proof — Suppose

$$(\lambda_1, \sigma_1) \in C_{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}((\lambda, \sigma)).$$

Therefore we must have

$$(\lambda_1, \sigma_1)(\lambda, \sigma) = (\lambda, \sigma)(\lambda_1, \sigma_1),$$

which implies $\lambda_1\lambda^{\sigma_1^{-1}} = \lambda\lambda_1^{\sigma^{-1}}$, or equivalently, $\lambda^{-1}\lambda^{\sigma_1^{-1}} = \lambda_1^{-1}\lambda_1^{\sigma^{-1}}$. To count the number of elements (λ_1, σ_1) satisfying this equation, we choose an element $\sigma_1 \in \mathrm{Gal}(F_{q^n}/F_q)$. Now if we consider the element on the left hand side of the previous equation, namely $\lambda^{-1}\lambda^{\sigma_1^{-1}}$, it is clear that this is an element of norm 1. Now we note that σ is a generator of $\mathrm{Gal}(F_{q^n}/F_q)$ and therefore by Hilbert's theorem 90 (see Theorem 7.6. in [1]), there exists $\lambda_1 \in F_{q^n}^*$ satisfying the aformentioned equation. Furthermore, in the case of $\sigma_1 = 1$ the previous equation simplifies to $1 = \lambda_1^{-1}\lambda_1^{\sigma^{-1}}$. In order for λ_1 to satisfy this equation it has to be in the kernel of the $F_{q^n}^*$ homomorphism $t \mapsto t^{-1}t^{\sigma^{-1}}$, and we know there are exactly $q-1$ elements in the kernel of this homomorphism, which is the same as the fixed field of σ. Considering there are exactly n choices for σ_1, we get

$$|C_{F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda, \sigma)| = n(q-1).$$

The statement is proved. □

Lemma 2.6 *Let* $(\lambda, 1) \in F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$. *Then we have:*

$$|C_{F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda, 1)| = (q^n - 1)m$$

where m *is the size of the set* $\{\tau \in \mathrm{Gal}(F_{q^n}/F_q) | \lambda^\tau = \lambda\}$.

Proof — Suppose an element $(t, \tau) \in C_{F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda, 1)$. Therefore we must have

$$(\lambda, 1)(t, \tau) = (t, \tau)(\lambda, 1),$$

and hence we get $\lambda t = t\lambda^{\tau^{-1}}$, which implies $\lambda^\tau = \lambda$. Therefore we have

$$C_{F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda, 1) = \{(t, \tau) | t \in F_{q^n}^*, \lambda^\tau = \lambda\}$$

and the result follows. □

Lemma 2.7 *Let* $(a, \sigma), (b, \sigma) \in F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$, *where* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$. *Then* (a, σ) *is conjugate to* (b, σ) *if and only if* $N(a) = N(b)$.

Proof — The elements (a, σ) and (b, σ) are conjugate if and only if there exists $(t, \tau) \in F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ such that

$$(t, \tau)^{-1}(a, \sigma)(t, \tau) = (b, \sigma).$$

Equivalently, we can say the elements (a, σ) and (b, σ) are conjugate if and only if there exist

$$(t, \tau) \in F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$$

satisfying the equation $(t^{-1})^\tau (t^\tau)^{\sigma^{-1}} = b(a^{-1})^\tau$. Suppose there exists $(t, \tau) \in F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ satisfying the equation

$$(t^{-1})^\tau (t^\tau)^{\sigma^{-1}} = b(a^{-1})^\tau.$$

Then we note the the element on the left side of the equation, namely $(t^{-1})^\tau (t^\tau)^{\sigma^{-1}}$, has norm 1, and therefore we must have

$$N(b(a^{-1})^\tau) = 1,$$

which implies

$$N(a) = N(b).$$

Conversely, suppose we have $N(a) = N(b)$. Let $\tau = 1 \in \mathrm{Gal}(F_{q^n}/F_q)$. Therefore the equation

$$(t^{-1})^\tau (t^\tau)^{\sigma^{-1}} = b(a^{-1})^\tau$$

simplifies to

$$(t^{-1})(t)^{\sigma^{-1}} = b(a^{-1}).$$

Since by assumption $N(a) = N(b)$, it follows that $N(b(a^{-1}) = 1$, and hence by Hilbert's theorem 90, there exist $t \in F_{q^n}^*$ satisfying

$$(t^{-1})(t)^{\sigma^{-1}} = b(a^{-1}),$$

which implies (a, σ) and (b, σ) are conjugate. □

Corollary 2.8 *Suppose* $(a, \sigma) \in F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$, *where* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$. *Then* (a, σ) *is conjugate to* $(1, \sigma)$ *if and only if* $N(a) = 1$.

Proof — This follows immediately from Lemma 2.7 together with the fact that $N(1) = 1$. □

Corollary 2.9 *Let* p *and* q *be primes. The semi-linear subgroup*

$$H = F_{q^p}^* \rtimes \mathrm{Gal}(F_{q^p}/F_q)$$

has conjugate rank 2 *and, furthermore,* $\mathrm{cs}(H) = \{1, p, \frac{q^p-1}{q-1}\}$*. The conjugacy class size of an element* (λ, σ) *lying in this subgroup of the affine semi-linear group is summarized as follows:*

λ	σ	$\lvert(\lambda,\sigma)^H\rvert$
$F^*_{q^p}$	$\neq 1$	$\frac{q^p-1}{q-1}$
F^*_q	1	1
$F^*_{q^p} - F_q$	1	p

Proof — If
$$(\lambda, \sigma) \in F^*_{q^p} \rtimes \mathrm{Gal}(F_{q^p}/F_q)$$
where σ is a generator of $\mathrm{Gal}(F_{q^p}/F_q)$, then it follows by Lemma 2.5 that the conjugacy class of (λ, σ) has $\frac{q^p-1}{q-1}$ elements. Next, we consider an element of the form $(\lambda, 1)$. It follows by Lemma 2.6 that if λ is an element of the base field, then the element $(\lambda, 1)$ would be a central element; otherwise the centralizer of $(\lambda, 1)$ has $q^p - 1$ elements and hence the conjugacy class of this element has p elements. Therefore the set of the conjugacy classes of $(\lambda, \sigma) \in F^*_{q^p} \rtimes \mathrm{Gal}(F_{q^p}/F_q)$ is $\{1, p, \frac{q^p-1}{q-1}\}$. □

Lemma 2.10 *Let* $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *and let* $(0, \lambda, \sigma) \in G$*. Suppose* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$*. If* λ *is an element of norm* 1*, we have*
$$|C_G((0, \lambda, \sigma))| = n(q-1)q,$$
otherwise we have
$$|C_G((0, \lambda, \sigma))| = n(q-1).$$

Proof — Suppose $(a, \lambda_1, \sigma_1) \in C_G(0, \lambda, \sigma)$. Therefore we have
$$(a, \lambda_1, \sigma_1)(0, \lambda, \sigma) = (0, \lambda, \sigma)(a, \lambda_1, \sigma_1)$$
which results in the following equations:
$$a = \lambda^{-1} a^{\sigma^{-1}}, \quad \lambda_1 \lambda^{\sigma_1^{-1}} = \lambda \lambda_1^{\sigma^{-1}} \quad \text{and} \quad \sigma_1 \sigma = \sigma \sigma_1.$$

This can be put as follows:

$$C_G((0,\lambda,\sigma)) = \{(a,\lambda_1,\sigma_1) : a = \lambda^{-1}a^{\sigma^{-1}},$$
$$(\lambda_1,\sigma_1) \in C_{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda,\sigma)\}$$

and we note that the size of $C_{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda,\sigma)$ is calculated in Lemma 2.5. It remains to calculate the number of elements a that satisfy the equation $a = \lambda^{-1}a^{\sigma^{-1}}$. We note that $a = 0$ always satisfies the equation. Now if $a \neq 0$ then this equation could be rewritten as $\lambda = a^{-1}a^{\sigma^{-1}}$. Using Hilbert's Theorem 90, if λ is an element of norm 1, then there exists an element a satisfying this equation, and in fact, using the same argument as in the proof of Lemma 2.5, it follows that there are exactly q elements (the number of elements in the fixed field of σ) satisfying this equestion. On the other hand if the norm of λ is not equal to 1, then we must have $a = 0$ and this completes the proof. □

Corollary 2.11 *Let* $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *and let* $(0,\lambda,\sigma) \in G$. *Suppose* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$. *If* λ *is an element of norm 1, we have*

$$|(0,\lambda,\sigma)^G| = \frac{q^{n-1}(q^n-1)}{q-1},$$

otherwise we have

$$|(0,\lambda,\sigma)^G| = \frac{q^n(q^n-1)}{q-1}.$$

Proof — This is an immediate consequence of Lemma 2.10, considering the fact that $|G| = nq^n(q^n-1)$ □

Lemma 2.12 *Let* $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *and let* $(0,\lambda,1) \in G$, *where* $\lambda \neq 1$. *Then we have*

$$|C_G(0,\lambda,1)| = |C_{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda,1)|.$$

Proof — If an element (a,b,τ) lies in the centralizer of $(0,\lambda,1)$, we must have $a = 0$ and $(b,\tau) \in C_{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}(\lambda,1)$, and the result follows. □

Corollary 2.13 *Let* $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *and let* $(0,\lambda,1) \in G$, *where* $\lambda \neq 1$. *Then we have:*

$$|(0,\lambda,1)^G| = q^n \cdot \left|(\lambda,1)^{F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)}\right|.$$

Proof — This is just a rephrasing of the previous lemma. □

As we observed earlier, it is possible for a conjugacy class of

$$F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$$

to give rise to a single conjugacy class of G, or to split and give rise to more than one classes of G. The following results are aimed at determining whether a conjugacy class of $F_{q^n}^* \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ splits.

Lemma 2.14 *Let* $G = (F_{q^n}^+ \rtimes F_{q^n}^*) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *and let* $(a, 1, \sigma)$ *and* $(0, 1, \sigma)$ *be elements of* G *where* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$*. Then* $(a, 1, \sigma)$ *and* $(0, 1, \sigma)$ *are conjugate if and only if* $\mathrm{Tr}(a) = 0$*.*

Proof — The elements $(a, 1, \sigma)$ and $(0, 1, \sigma)$ are conjugate if and only if there exists $(x, t, \tau) \in G$ such that

$$(x, t, \tau)^{-1}(0, 1, \sigma)(x, t, \tau) = (a, 1, \sigma).$$

This equation further simplifies to

$$(t^\tau(-x)^\tau + t^\tau x^{\tau\sigma^{-1}}, (t^{-1})^\tau t^{\tau\sigma^{-1}}, \sigma) = (a, 1, \sigma).$$

Therefore $(a, 1, \sigma)$ and $(0, 1, \sigma)$ are conjugate if and only if there exist $(x, t, \tau) \in G$ such that

$$(t^{-1})^\tau t^{\tau\sigma^{-1}} = 1 \quad \text{and} \quad t^\tau(-x)^\tau + t^\tau x^{\tau\sigma^{-1}} = a.$$

Suppose there exist $(x, t, \tau) \in G$ such that

$$(t^{-1})^\tau t^{\tau\sigma^{-1}} = 1 \quad \text{and} \quad t^\tau(-x)^\tau + t^\tau x^{\tau\sigma^{-1}} = a.$$

We note that it follows from $(t^{-1})^\tau t^{\tau\sigma^{-1}} = 1$ that $t^\tau = t^{\tau\sigma^{-1}}$, and hence the equation

$$t^\tau(-x)^\tau + t^\tau x^{\tau\sigma^{-1}} = a$$

is equivalent to $-(tx)^\tau + ((tx)^\tau)^{\sigma^{-1}} = a$. The element on the left side of this equation, namely $-(tx)^\tau + ((tx)^\tau)^{\sigma^{-1}}$, has trace zero and therefore we must have $\mathrm{Tr}(a) = 0$. Conversely suppose we have $\mathrm{Tr}(a) = 0$. Let $t = 1$ and $\tau = 1$. Then the equation $(t^{-1})^\tau t^{\tau\sigma^{-1}} = 1$ holds true trivially and the equation

$$t^{\tau}(-x)^{\tau} + t^{\tau}x^{\tau\sigma^{-1}} = a$$

simplifies to $-x + x^{\sigma^{-1}} = a$. Using the fact that $\mathrm{Tr}(a) = 0$, Hilbert's theorem 90 guarantees that there exists $x \in \mathbb{F}_{q^n}$ that satisfies the equation $-x + x^{\sigma^{-1}} = a$, and consequently, $(a, 1, \sigma)$ and $(0, 1, \sigma)$ are conjugate as desired. □

Lemma 2.15 *Let* $G = (\mathbb{F}^+_{q^n} \rtimes \mathbb{F}^*_{q^n}) \rtimes \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *and let* $(a, 1, \sigma)$ *and* $(b, 1, \sigma)$ *be elements of* G *where* σ *is a generator of* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ *and* $\mathrm{Tr}(a) \neq 0$. *Then* $(a, 1, \sigma)$ *and* $(b, 1, \sigma)$ *are conjugate if and only if* $\mathrm{Tr}(b) \neq 0$.

Proof — The elements $(a, 1, \sigma)$ and $(b, 1, \sigma)$ are conjugate if and only if there exists $(x, t, \tau) \in G$ such that

$$(x, t, \tau)^{-1}(a, 1, \sigma)(x, t, \tau) = (b, 1, \sigma).$$

This equation is equivalent to

$$(t^{\tau}(-x)^{\tau} + t^{\tau}a^{\tau} + t^{\tau}x^{\tau\sigma^{-1}}, (t^{-1})^{\tau}t^{\tau\sigma^{-1}}, \sigma) = (b, 1, \sigma).$$

Therefore $(a, 1, \sigma)$ and $(b, 1, \sigma)$ are conjugate if and only if there exists $(x, t, \tau) \in G$ such that

$$(t^{-1})^{\tau}t^{\tau\sigma^{-1}} = 1 \quad \text{and} \quad t^{\tau}(-x)^{\tau} + t^{\tau}a^{\tau} + t^{\tau}x^{\tau\sigma^{-1}} = b.$$

Suppose there exists $(x, t, \tau) \in G$ such that

$$(t^{-1})^{\tau}t^{\tau\sigma^{-1}} = 1 \quad \text{and} \quad t^{\tau}(-x)^{\tau} + t^{\tau}a^{\tau} + t^{\tau}x^{\tau\sigma^{-1}} = b.$$

Then it follows from $(t^{-1})^{\tau}t^{\tau\sigma^{-1}} = 1$ that $t^{\tau} = t^{\tau\sigma^{-1}}$, and hence the equation $t^{\tau}(-x)^{\tau} + t^{\tau}a^{\tau} + t^{\tau}x^{\tau\sigma^{-1}} = b$ would be equivalent to

$$-(tx)^{\tau} + ((tx)^{\tau})^{\sigma^{-1}} = b - t^{\tau}a^{\tau}.$$

The element on the left side of this equation has trace zero and therefore we must have $\mathrm{Tr}(b - t^{\tau}a^{\tau}) = 0$. Using the linearity property of trace, and the fact that t^{τ} is an element of the base field, it follows that $\mathrm{Tr}(b) = t^{\tau}\,\mathrm{Tr}(a)$. Since by assumption $\mathrm{Tr}(a) \neq 0$, we have $\mathrm{Tr}(b) \neq 0$ as desired. Conversely, suppose we have $\mathrm{Tr}(b) \neq 0$. Let $t = \mathrm{Tr}(b)/\mathrm{Tr}(a)$ and $\tau = 1$. We note that not only is t an element that lies in $F^*_{q^n}$, but also it lies in the base field. Hence the equation $(t^{-1})^\tau t^{\tau\sigma^{-1}} = 1$ holds true trivially and the equation

$$t^\tau(-x)^\tau + t^\tau a^\tau + t^\tau x^{\tau\sigma^{-1}} = b$$

simplifies to

$$-x + x^{\sigma^{-1}} = b\frac{\mathrm{Tr}(a)}{\mathrm{Tr}(b)} - a.$$

We observe that the element on the right side of this equation has trace zero and Hilbert's theorem 90 guarantees that there exists $x \in F_{q^n}$ that satisfies the equation , and consequently, $(a, 1, \sigma)$ and $(b, 1, \sigma)$ are conjugate as desired. □

Corollary 2.16 *Let* $G = (F^+_{q^n} \rtimes F^*_{q^n}) \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *and let*

$$(\lambda, \sigma) \in F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q).$$

Then we have:

(1) *If* $\sigma = 1$ *and* $\lambda \neq 1$, *then the conjugacy class of* $(\lambda, 1)$ *would not split.*

(2) *If* σ *is a generator of* $\mathrm{Gal}(F_{q^n}/F_q)$, *then the conjugacy of* (λ, σ) *in* $F^*_{q^n} \rtimes \mathrm{Gal}(F_{q^n}/F_q)$ *would split precisely when* $\mathrm{N}(\lambda) = 1$.

Proof — (1) follows from Corollary 2.13. (2) follows from Corollary 2.11. □

Remark 2.17 In the previous corollary, the case where σ is not a generator remains to be further investigated.

3 Main Results

Lemma 3.1 *Let* $G = (F^+_{q^p} \rtimes F^*_{q^p}) \rtimes \mathrm{Gal}(F_{q^p}/F_q)$, *where* p *and* q *are primes. The size of the conjugacy class of an element* $(a, \lambda, \sigma) \in G$ *would be as follows.*

a	λ	σ	$\lvert(a,\lambda,\sigma)^G\rvert$
0	1	1	1
$F^*_{q^p}$	1	1	q^p-1
F_{q^p}	$F_q-\{1\}$	1	q^p
F_{q^p}	$F_{q^p}-F_q$	1	pq^p
$\mathrm{Tr}(a)=0$	$N(\lambda)=1$	$\neq 1$	$\frac{q^{p-1}(q^p-1)}{q-1}$
$\mathrm{Tr}(a)\neq 0$	$N(\lambda)=1$	$\neq 1$	$\frac{(q^p-q^{p-1})(q^p-1)}{q-1}$
F_{q^p}	$N(\lambda)\neq 1$	$\neq 1$	$\frac{q^p(q^p-1)}{q-1}$

Proof — Let $(a,\lambda,\sigma)\in G$. We shall consider all possible scenarios for this element and in each case will calculate the class size.

Case 1: $\sigma=1$. If $\lambda=1$, then the conjugacy class of

$$(1,1)\in F^*_{q^p}\rtimes \mathrm{Gal}(F_{q^p}/F_q)$$

would split as follows:

1.1 The conjugacy class of $(0,1,1)$, namely the identity element of G, which has size 1.

1.2 The conjugacy class of $(1,1,1)$, which as we've seen in Corollary 2.2 has size q^p-1.

Next, suppose $1\neq\lambda\in F^*_{q^p}$. Then by Corollary 2.16 the conjugacy class of $(\lambda,1)\in F^*_{q^p}\rtimes\mathrm{Gal}(F_{q^p}/F_q)$ would not split and therefore by Corollary 2.9 we have the following two possibilities.

1.3 If λ is an element of the base field (and $\lambda\neq 1$), then the conjugacy class of $(0,\lambda,1)$ has size q^p.

1.4 If λ is not an element of the base field, then the conjugacy class of $(0,\lambda,1)$ has size pq^p.

Case2: $\sigma\neq 1$. We note that σ will be a generator for $\mathrm{Gal}(F_{q^p}/F_q)$. In this situation the conjugacy class of $(\lambda,\sigma)\in F^*_{q^p}\rtimes\mathrm{Gal}(F_{q^p}/F_q)$ would split depending on whether or not λ is an element of norm 1. More precisely, as we've seen in Corollary 2.11, if $N(\lambda)\neq 1$ then the conjugacy class of (λ,σ) would not split and if $N(\lambda)=1$ then the conjugacy class of (λ, σ) would split. We also take into account the fact that by Corollary 2.9 in this situation the class of

$$(\lambda, \sigma) \in F^*_{q^p} \rtimes \mathrm{Gal}(F_{q^p}/F_q)$$

has size $\frac{q^p-1}{q-1}$. This could be summarized as follows:

2.1 If $N(\lambda) \neq 1$ then the conjugacy class of (λ, σ) would not split, and therefore using the conjugacy class of $(0, \lambda, \sigma)$ has size

$$\frac{q^p(q^p-1)}{q-1}.$$

2.2 If $N(\lambda) = 1$ then the conjugacy class of (λ, σ) would split as in Lemma 2.14 and Lemma 2.15 and we get two conjugacy classes of sizes $\frac{(q^p-q^{p-1})(q^p-1)}{q-1}$ and $\frac{q^{p-1}(q^p-1)}{q-1}$.

The statement is proved. □

Theorem 3.2 *Let* $G = (F^+_{2^p} \rtimes F^*_{2^p}) \rtimes \mathrm{Gal}(F_{2^p}/F_2)$, *where* p *is a prime. The set of conjugacy class sizes of* G, *namely* $\mathrm{cs}(G)$, *is as follows.*

$$\mathrm{cs}(G) = \{1, 2^p - 1, p2^p, 2^{p-1}(2^p - 1)\}$$

Proof — This follows from Lemma 3.1 where $q = 2$. We note that since $q = 2$, the cases 1.3. and 2.1., as in the proof of Lemma 3.1, would not occur and we have to eliminate the corresponding class sizes. □

Theorem 3.3 *Let* $G = (F^+_{q^p} \rtimes F^*_{q^p}) \rtimes \mathrm{Gal}(F_{q^p}/F_q)$, *where* p *and* q *are primes and* $q \neq 2$. *The set of conjugacy class sizes of* G, *namely* $\mathrm{cs}(G)$, *is as follows:*

$$\left\{1, q^p - 1, q^p, pq^p, \frac{q^{p-1}(q^p-1)}{q-1}, \frac{q^p(q^p-1)}{q-1}, \frac{(q^p-q^{p-1})(q^p-1)}{q-1}\right\}$$

Proof — The class sizes have all been calculated in the proof of Lemma 3.1. □

Corollary 3.4 *Let* $G = (F^+_{q^p} \rtimes F^*_{q^p}) \rtimes \mathrm{Gal}(F_{q^p}/F_q)$, *where* p *and* q *are primes. Then we have* $\mathrm{crk}(G) \leqslant 6$.

Proof — As we observed in the previous corollary, the set of conjugacy class sizes of G is contained in the set:

$$\left\{1, q^p - 1, q^p, pq^p, \frac{q^{p-1}(q^p-1)}{q-1}, \frac{q^p(q^p-1)}{q-1}, \frac{(q^p - q^{p-1})(q^p-1)}{q-1}\right\}$$

and therefore the are at most 6 nontrivial class sizes. □

Corollary 3.5 *Let* $G = (F^+_{2^p} \rtimes F^*_{2^p}) \rtimes \mathrm{Gal}(F_{2^p}/F_2)$, *where* p *is a prime. Then* G *has conjugate rank 3.*

Proof — As we observed in Theorem 3.2 the set of conjugacy class sizes of G is $cs(G) = \{1, 2^p - 1, p2^p, 2^{p-1}(2^p-1)\}$, and it's fairly easy to observe that the elements of this set are always distinct. Hence we have $crk(G) = 3$. □

Remark 3.6 Let $G = (F^+_{q^p} \rtimes F^*_{q^p}) \rtimes \mathrm{Gal}(F_{q^p}/F_q)$, where p and q are primes. Then as we've seen in Lemma 3.1 the identity element is the only element of index 1, and hence $Z(G) = 1$. This implies G cannot be nilpotent.

Example 3.7 Let $n = q = 2$. We note that $|F^+_4| = 4$, $|F^*_4| = 3$ and

$$|\mathrm{Gal}(F_4/F_2)| = 2.$$

Therefore

$$G = (F^+_4 \rtimes F^*_4) \rtimes \mathrm{Gal}(F_4/F_2)$$

is a group of size 24. To be able to carry out the multiplication in G, we need to have a clear understanding of multiplication and addition within F_4. First off we notice that two elements have to be 0 and 1, and we call the other elements a and b. We know that the multiplicative group F^*_4 is cyclic of order 3; hence we must have $a^2 = b$, $b^2 = a$, and $ab = 1$. Using the properties of a field we can also check $a + 1 = b$, $b + 1 = a$, and $a + b = 1$. Suppose σ is the generator of $\mathrm{Gal}(F_4/F_2)$; and we know the way σ acts on any element is by squaring that element. By Corollary 2.3 calculating the conjugacy classes of $(F^*_4) \rtimes \mathrm{Gal}(F_4/F_2)$ would facilitate the process of finding the conjugacy classes of G. As it turns out, $(F^*_4) \rtimes \mathrm{Gal}(F_4/F_2)$ is a non-abelian group of order 6 and has three conjugacy classes as follows:

- $C_1 = \{(1, 1)\}$;
- $C_2 = \{(a, 1), (b, 1)\}$;

- $C_3 = \{(1,\sigma),(a,\sigma),(b,\sigma)\}$.

Next, using the above classes together with Corollary 2.3 and finding the centralizer of elements deemed necessary, we can calculate the conjugacy classes of G as follows.

C_1 gives rise to D_1 and D_2:

- $D_1 = \{(0,1,1)\}$;
- $D_2 = \{(1,1,1),(a,1,1),(b,1,1)\}$.

C_2 gives us the following conjugacy class:

- $D_3 = \{(0,a,1),(1,a,1),(a,a,1),(b,a,1),(0,b,1),(1,b,1),(a,b,1),(b,b,1)\}$.

C_3 generates the following two conjugacy classes:

- $D_4 = \{(0,1,\sigma),(1,1,\sigma),(0,a,\sigma),(b,a,\sigma),(0,b,\sigma),(a,b,\sigma)\}$;
- $D_5 = \{(a,1,\sigma),(b,1,\sigma),(1,a,\sigma),(a,a,\sigma),(1,b,\sigma),(b,b,\sigma)\}$.

Remark 3.8 According to GAP, the symmetric group S_4 is the only group of order 24 with the conjugacy class sizes $\{1,3,6,8\}$ and hence we must have

$$(F_4^+ \rtimes F_4^*) \rtimes \mathrm{Gal}(F_4/F_2) \simeq S_4.$$

Acknowledgment

I'd like to extend my thanks to Professor Alexandre Turull for his invaluable advice and suggestions.

REFERENCES

[1] T.W. Hungerford: "Algebra", *Springer*, Berlin (1974).

[2] O. Manz – T.R. Wolf: "Representations of Solvable Groups", *Cambridge University Press*, Cambridge (1993).

Hossein Shahrtash
Department of Mathematics
Cabrini University
610 King of Prussia Road
19087 Radnor, PA (USA)
e-mail: hs10274@cabrini.edu