Chapter 2

Inductive algebras for the affine group of a finite field

In this chapter we show that *each irreducible representation of the affine group of a finite field has a unique maximal inductive algebra, and it is self-adjoint.*

In Section 2.1, we recall the structure of the affine group of a finite field, and set up the notation. In Section 2.2, we recall its representation theory, and formulate our main result. The main result is proved in Section 2.3.

2.1 The affine group of a finite field

Let k be a finite field of order $q = p^n$, where p is prime. Let $k^\times$ denote the multiplicative group of non-zero elements of k. Recall that the affine group of k is the group G of affine automorphisms of k. Thus an element g of G is a map $g : k \to k$ of the form $g(x) = ax + b$ where $a \in k^\times$ and $b \in k$, and the group law is composition.

The group G may be identified with the group of matrices

$$\left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \;\middle|\; a \in k^\times,\, b \in k \right\}.$$

Let $\iota : k \to G$, $p : G \to k^\times$ and $s : k^\times \to G$ be defined by

$$\iota(b) = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}, \quad p\left(\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}\right) = a, \text{ and } \quad s(a) = \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}.$$

Then ι, p and s are homomorphisms, $\iota(k) \lhd G$ and

$$\begin{tikzcd} 0 \arrow[r] & k \arrow[r, "\iota"] & G \arrow[r, "p"] & k^\times \arrow[l, dashed, bend left, "s"] \arrow[r] & 1 \end{tikzcd}$$

is an exact sequence with splitting s. Thus G is a semidirect product $k^\times \ltimes k$. We note for future reference that $s(a')\iota(b)s(a')^{-1} = \iota(a'b)$.

2.2 Formulation

The irreducible unitary representations of G may be constructed using the *Mackey machine* (see [5, §3.9]). There are $q-1$ characters (one-dimensional representations), and one $(q-1)$-dimensional representation (up to unitary equivalence).

Obviously, the characters have only the trivial inductive algebra $\mathbb{C}$, which is self-adjoint.

The $(q-1)$-dimensional representation is

$$\pi = \mathrm{Ind}_{\iota(k)}^{G} \chi,$$

where $\chi : k \to \mathbb{C}^\times$ is a non-trivial homomorphism (i.e. $\chi \not\equiv 1$). The representation π acts on the space

$$V = \{f : G \to \mathbb{C} \mid f(\iota(b')g') = \chi(b')f(g') \qquad \forall b' \in k, g' \in G\}$$

by

$$\left[\pi(g)f\right](g') = f(g'g).$$

Let $\mathcal{H}$ denote the Hilbert space of all complex-valued functions on $k^\times$ equipped with the inner product

$$\langle F_1, F_2\rangle = \sum_{a' \in k^\times} F_1(a')\overline{F_2(a')}.$$

Let $F \in \mathcal{H}$. Since every $g' \in G$ may be expressed uniquely as $\iota(b')s(a')$ with $b' \in k$ and $a' \in k^\times$, we may define a function $f : G \to \mathbb{C}$ by

$$f(g') = \chi(b')F(a').$$

Then for all $b \in k$, we have

$$\begin{aligned} f\left(\iota(b)g'\right) &= f(\iota(b+b')s(a')) \\ &= \chi(b+b')F(a') \\ &= \chi(b)\chi(b')F(a') \\ &= \chi(b)f(g'). \end{aligned}$$

Therefore $f \in V$. On the other hand, an element $f \in V$ is determined by $f \circ s$. Indeed, if $f \in V$ and $g' = \iota(b')s(a')$ then $f(g) = \chi(b')f(s(a'))$. Thus $f \mapsto f \circ s$ is an isomorphism from $V \to \mathcal{H}$. Conjugation by this isomorphism gives an action of G

on $\mathcal{H}$. Indeed, if $g = \iota(b)s(a)$ then

$$\begin{aligned}(\pi(g)f)\,(s(a')) &= f\,(s(a')\iota(b)s(a)) \\ &= f\left(s(a')\iota(b)s(a')^{-1}s(a'a)\right) \\ &= f\,(\iota(a'b)s(a'a)) \\ &= \chi(a'b)f(s(a'a)).\end{aligned}$$

Therefore the representation π may be realized on $\mathcal{H}$ by

$$(\pi(g)F)(a') = \chi(a'b)F(a'a), \qquad g = \iota(b)s(a).$$

For each $\varphi \in \mathcal{H}$, let $m_\varphi : \mathcal{H} \to \mathcal{H}$ be defined by $m_\varphi(F) = \varphi F$. Let

$$\mathcal{B} = \{m_\varphi \mid \varphi \in \mathcal{H}\}.$$

Then $\mathcal{B}$ is a maximal-abelian subalgebra of $\mathcal{B}(\mathcal{H})$ (see [21, Prop 4.7.6]), and $\mathcal{B}$ is π-inductive. Therefore $\mathcal{B}$ is a maximal π-inductive algebra. Moreover, it is self-adjoint. Our main result is the following theorem.

Theorem 2.2.1. *$\mathcal{B}$ is the only maximal π-inductive algebra.*

2.3 The proof

If χ is a character of the additive group k, and $b \in k$, let χ_b be defined by $\chi_b(b') = \chi(bb')$ for $b' \in k$. Observe that χ_b is also a character of the additive group k. We need the following lemma in the course of the proof.

Lemma 2.3.1. *Let χ be a non-trivial character of the additive group k. Every character ψ of the additive group k is of the form χ_b for some $b \in k$.*

Proof. Define $\Psi : k \to \widehat{k}$ by $\Psi(b) = \chi_b$. Since $\chi_{b_1+b_2} = \chi_{b_1}\chi_{b_2}$, Ψ is a group homomorphism. We have

$$\begin{aligned}
\ker(\Psi) &= \{b \in k \mid \chi_b \equiv 1\} \\
&= \{b \in k \mid \forall b' \in k, \chi(bb') \equiv 1\} \\
&= \{b \in k \mid \forall b' \in k,\, bb' \in \ker(\chi)\} \\
&= \{b \in k \mid bk \subset \ker(\chi)\} \\
&= \{0\},
\end{aligned}$$

because k is a field and χ is not the trivial character. Therefore Ψ is injective. Since $|\widehat{k}| = |k|$ (see [1, Proposition 4.6] and [1, Theorem 4.5(d)]), by the pigeonhole principle, Ψ is surjective, i.e., given $\psi \in \hat{k}$ there exists $b \in k$ such that $\psi = \chi_b$. $\square$

Let $\mathcal{A}$ be a maximal π-inductive algebra.

Lemma 2.3.2. *There are no non-zero nilpotent elements in* $\mathcal{A}$*.*

Proof. Let $\mathcal{N}$ denote the set of nilpotent elements in $\mathcal{A}$ (the nilradical of $\mathcal{A}$). Let

$$\mathcal{K} = \{F \in \mathcal{H} \mid T(F) = 0, \quad \forall T \in \mathcal{N}\}.$$

By Engel's theorem [2, A.16], $\mathcal{K} \neq 0$. Observe that $\mathcal{N}$ is normalized by $\pi(G)$, so $\mathcal{K}$ is $\pi(G)$-invariant. However, since π is irreducible, it follows that $\mathcal{K} = \mathcal{H}$, whence $\mathcal{N} = 0$. $\square$

Corollary 2.3.3. $\dim(\mathcal{A}) \leq q - 1$.

Proof. By Lemma 2.3.2, the Jordan-Chevalley decomposition [3, §4.2], and the fact that $\mathcal{A}$ is abelian, it follows that there is a (not necessarily orthonormal) basis for $\mathcal{H}$ in which each element of $\mathcal{A}$ is diagonal. Since $\dim(\mathcal{H}) = q - 1$, the result follows. $\square$

For $b' \in k$, define $\kappa(b') : \mathcal{A} \to \mathcal{A}$ by $\kappa(b')T = \pi(\iota(b'))T\pi(\iota(b'))^{-1}$. Then κ is a representation of the finite abelian group k on the vector space $\mathcal{A}$, which decomposes, by the Peter-Weyl theorem and Lemma 2.3.1, as

$$\mathcal{A} = \bigoplus_{b \in k} \mathcal{A}_b$$

where

$$\mathcal{A}_b = \{T \in \mathcal{A} \mid \kappa(b')T = \chi(bb')T, \quad \forall b' \in k\}.$$

Observe that

1. if $T \in \mathcal{A}_b$ and $T' \in \mathcal{A}_{b'}$, then $TT' \in \mathcal{A}_{b+b'}$, and
2. for each $a \in k^\times$, the map $T \mapsto \pi(s(a))^{-1}T\pi(s(a))$ is a linear isomorphism $\mathcal{A}_b \to \mathcal{A}_{ab}$.

Lemma 2.3.4. $\mathcal{A}_1 = 0$.

Proof. Suppose not. Then there exists a non-zero element $T \in \mathcal{A}_1$. By the first observation above, $T^p \in \mathcal{A}_0$. Since T is not nilpotent (see Lemma 2.3.2), it follows that $\dim(\mathcal{A}_0) \geq 1$. For $b \neq 0$, we have $\dim(\mathcal{A}_b) = \dim(\mathcal{A}_1) \geq 1$, by the second observation.

Therefore

$$\dim(\mathcal{A}) = \sum_{b \in k} \dim(\mathcal{A}_b) \geq |k| = q,$$

contradicting Corollary 2.3.3. □

Lemma 2.3.5. $\mathcal{A}_0 \subseteq \mathcal{B}$.

Proof. Observe that $\mathcal{H}$ is spanned by the set $\{\chi_{b'}|_{k^\times} \mid b' \in k\}$, hence $\mathcal{B}$ is spanned by the set $\{m_{(\chi_{b'}|_{k^\times})} \mid b' \in k\}$. If $T \in \mathcal{A}_0$, then T commutes with $m_{(\chi_{b'}|_{k^\times})}$ for each

$b' \in k$, whence T commutes with $\mathcal{B}$. Since $\mathcal{B}$ is maximal-abelian, it follows that $T \in \mathcal{B}$. □

By Lemma 2.3.4, and the second observation above, it follows that $\mathcal{A}_b = 0$ for all $b \in k^\times$, whence $\mathcal{A} = \mathcal{A}_0 \subseteq \mathcal{B}$. Since $\mathcal{A}$ is maximal, it follows that $\mathcal{A} = \mathcal{B}$.