MACKEY-WIGNER'S LITTLE GROUP METHOD WITH AN APPLICATION TO $\mathrm{Aff}(q)$

RUPERT LI

Abstract. We define the affine group $\mathrm{Aff}(q)$ over a finite field $\mathbb{F}_q$ and provide some preliminary background on representation theory. We then introduce Mackey-Wigner's little group method, a powerful method that can completely construct all irreducible representations of a semidirect product. Decomposing the affine group as a semidirect product of translations and dilations, we apply the little group method to determine the irreducible representations of $\mathrm{Aff}(q)$.

1. Introduction to the affine group $\mathrm{Aff}(q)$

We closely follow Terras [T, p. 281–283].

In $\mathbb{R}^2$, dilation, translation, rotation, and their compositions preserve lines and parallelism, which makes them so-called affine transformations. More generally, an *affine transformation* of an affine space (which Euclidean space is a special case) is an automorphism that preserves the dimension of any affine subspaces (e.g., sends lines to lines) and the ratios of parallel line segments. This last condition implies that the affine transformations of $\mathbb{R}$ are the transformations of the form $x \mapsto ax + b$ with $a \neq 0$. We can view this map as the matrix multiplication

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} ax + b \\ 1 \end{pmatrix}.$$

These matrices $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ form a group, and so the affine transformations of $\mathbb{R}$ can be seen as a group action. We can generalize this idea of groups of affine transformations to other affine spaces. In particular, instead of working over $\mathbb{R}$, we will work over a finite field $\mathbb{F}_q$, yielding the analogous definition of the affine group.

Definition 1.1. For finite field $\mathbb{F}_q$, the *affine group* $\mathrm{Aff}(q)$ is the group of matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ for $a, b \in \mathbb{F}_q$ with $a \neq 0$.

Because of its group action interpretation, the affine group is sometimes called the finite $ax + b$ group.

The affine group has a particularly elegant structure as a semidirect product, which we now define.

Definition 1.2. For subgroups A and H of G, we say G is the *semidirect product* of A and H, denoted $G = A \ltimes H$, if A is a normal subgroup, $G = A \cdot H$ is the product of the two subgroups, and $A \cap H = \{e\}$, where e is the identity of G.

Lemma 1.3. *The affine group* $\mathrm{Aff}(q) = A \ltimes H$, *where*

$$A = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle| x \in \mathbb{F}_q \right\} \cong \mathbb{F}_q \quad \text{and} \quad H = \left\{ \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \middle| y \in \mathbb{F}_q^\times \right\} \cong \mathbb{F}_q^\times.$$

Proof. To show A is normal, note that

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y^{-1} & -xy^{-1} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & yz \\ 0 & 1 \end{pmatrix} \in A.$$

Any element $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) \in G$ can be written as

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \in A \cdot H.$$

Finally, we see $A \cap H = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ is the trivial group. □

Notice that A and H are both abelian. Viewing the affine group as the group of affine transformations $x \mapsto ax + b$, we see that A corresponds to translations $x \mapsto x + b$ and H corresponds to dilations $x \mapsto ax$, so Lemma 1.3 essentially shows that the group of affine transformations can be decomposed into translations and dilations.

2. A primer on representation theory

We first recall some preliminary definitions from representation theory.

Definition 2.1. A (finite-dimensional) *representation* of a finite group G is a pair (V, π) consisting of a finite-dimensional vector space V over $\mathbb{C}$ and a group homomorphism $\pi : G \to \mathrm{GL}(V)$. Frequently the representation will be identified solely by its homomorphism, i.e., π, instead of both V and π.

As V is a finite-dimensional vector space, $V \cong \mathbb{C}^n$ for some n, and thus π can be seen as a group homomorphism sending G to a group of complex matrices. From this perspective, we can easily concatenate two representations (V, π) and (U, ρ) to yield a representation $\pi \oplus \rho$ on $V \oplus U$; hence, the following definition of irreducibility allows us to restrict attention to the atomic representations.

Definition 2.2. A representation (V, π) of G is *irreducible* if it has no nontrivial subrepresentations, i.e., there does not exist a subspace $0 \subsetneq W \subsetneq V$ such that $\pi(g)W \subseteq W$ for all $g \in G$.

The classical result by Maschke in 1899 states that any representation π can be decomposed as the direct sum of irreducible representations (see [T, p. 247]). Irreducibility is equivalent to the non-existence of any basis such that $\pi(g)$ is always upper-triangular in block form. However, we generally wish for the behavior of a representation to not depend on a choice of basis, and so the following definition of equivalence views two representations as essentially identical if they only differ by a choice of basis.

Definition 2.3. Two representations (V, π) and (V, ρ) of G into V are *equivalent* if there exists $T \in \mathrm{GL}(V)$ such that $T\pi(g)T^{-1} = \rho(g)$ for all $g \in G$.

With an equivalence relation on representations, we wish for elegant representatives of each equivalence class; every representation of a finite group G is equivalent to a unitary representation (see [T, p. 244]), defined as follows.

Definition 2.4. A representation π of G into $V \cong \mathbb{C}^n$ is *unitary* if $\pi(g)$ is unitary for all $g \in G$, i.e.,

$$\pi(g) \in U(n) = \left\{ A \in \mathrm{GL}(n, \mathbb{C}) \middle| \overline{A}^T A = I \right\},$$

where $U(n)$ denotes the unitary group.

Unitary matrices A preserve the standard Hermitian inner product on $\mathbb{C}^n$, i.e., $\langle Au, Av \rangle = \langle u, v \rangle = \overline{u}^T v$ for all $u, v \in \mathbb{C}^n$. As any representation is equivalent to a unitary representation and irreducible representations are the atoms creating all representations, we define the dual of G to be the full set of irreducible unitary representations, our periodic table for representations.

Definition 2.5. The *dual* $\widehat{G}$ of a finite group G is any complete set of inequivalent irreducible unitary representations of G.

One way to combine two representations together that will be useful later is the tensor product of representations.

Definition 2.6. The *tensor product* $\sigma \otimes \phi$ of representations σ and ϕ of G, where σ is k-dimensional and ϕ is m-dimensional, is the km-dimensional representation of G where $(\sigma \otimes \phi)(g)$ is defined by forming a $k \times k$ array of $m \times m$ blocks such that the i, j block is $\sigma_{i,j}(g)\phi(g)$ for all $1 \leq i, j \leq k$.

Frequently, we will have representations of a group G while wanting representations of a related group G'. If we have a representation σ of G, we can always naturally restrict σ to a representation $\mathrm{Res}_H^G \sigma$ of a subgroup $H \subseteq G$. However, the reverse direction is nontrivial; the following definition of an induced representation allows one to obtain a representation of G using a representation of a subgroup $H \subseteq G$.

Definition 2.7. For a representation (W, σ) of a subgroup H of G, the *induced representation from H up to G* denoted $\phi = \mathrm{Ind}_H^G \sigma$ is the group homomorphism from G to $\mathrm{GL}(V)$, where

$$V = \{f : G \to W | f(hg) = \sigma(h)f(g), \text{ for all } h \in H, g \in G\},$$

given by

$$[\phi(g)f](x) = f(xg)$$

for all $x, g \in G$.

To check whether an induced representation is irreducible, we can use Mackey's criterion (see [S, p. 59]), which we now state without proof.

Theorem 2.8. *For a representation σ of $H \subseteq G$, the induced representation $\mathrm{Ind}_H^G \sigma$ is irreducible if and only if σ is irreducible and for each $s \in G \setminus H$, the two representations of $H_s = H \cap sHs^{-1}$ obtained by precomposing σ with the two injections $H_s \to H$ given by $x \mapsto x$ and $x \mapsto s^{-1}xs$ are disjoint.*

Here, *disjoint* means they share no irreducible component in common, i.e., the inner product of their characters is 0.

The character of an induced representation can be calculated using the Frobenius character formula for induced representations (see [T, p. 271]), which we state without proof.

Theorem 2.9. *The character of the induced representation* $\pi = \mathrm{Ind}_H^G \sigma$ *is given by*

$$\chi_\pi(g) = \sum_{\substack{a \in G/H \\ a^{-1}ga \in H}} \chi_\sigma(a^{-1}ga).$$

3. Mackey-Wigner's little group method

We refer readers to [S, p. 62] for additional discussion of Mackey-Wigner's little group method. The little group method constructs the irreducible representations of a semidirect product $G = A \ltimes H$. The crux of the method is that these irreducible representations can be built from the irreducible representations of A and those of their stabilizers in H.

To use the little group method, we must additionally stipulate that A is abelian, so that its irreducible representations $\chi \in \widehat{A}$ have degree 1. For any $\chi \in \widehat{A}$, we have $h \in H$ acts on χ via

$$(h\chi)(a) = \chi(h^{-1}ah)$$

for all $a \in A$, where $h^{-1}ah \in A$ since A is normal. The stabilizer of χ by this action is $H_\chi = \{h \in H | h\chi = \chi\}$, and to recover a group similar to $G = A \cdot H$, define $G_\chi = A \ltimes H_\chi \subseteq G$; these are our namesake "little groups." We now create representations of G_χ from representations of its two component parts. For the first part, we may extend χ to a representation of G_χ by defining $\chi(ah) = \chi(a)$ for all $a \in A$ and $h \in H_\chi$. Similarly, for any $\rho \in \widehat{H}_\chi$, we may lift to a representation of G_χ by defining $\rho(ah) = \rho(h)$ for all $a \in A$ and $h \in H_\chi$. These two types of representations essentially have all the information to create every irreducible representation of G, so we combine them using the tensor product to obtain $\chi \otimes \rho$. However, χ and ρ are both representations of G_χ and thus so is $\chi \otimes \rho$, so to obtain a representation on G, we use the induced representation $\mathrm{Ind}_{G_\chi}^G(\chi \otimes \rho)$ from G_χ up to G. This leads to our main result.

Theorem 3.1. *The irreducible representations of* G *are* $\theta_{\chi,\rho} = \mathrm{Ind}_{G_\chi}^G(\chi \otimes \rho)$ *as* χ *varies over orbit representatives of* $\widehat{A}$ *modulo the action of* H*.*

Proof. We prove the result in three steps: first, the $\theta_{\chi,\rho}$ are irreducible; second, the $\theta_{\chi,\rho}$ are inequivalent; third, every irreducible representation of G is equivalent to some $\theta_{\chi,\rho}$.

Step one. The first part uses Mackey's criterion, Theorem 2.8. It follows from the Schur orthogonality relations (see [T, p. 253]) that the tensor product of two irreducible representations is irreducible, and thus $\chi \otimes \rho$ is irreducible. Next, to check the two representations of $K_s = G_\chi \cap sG_\chi s^{-1}$ are disjoint, notice that if they were not disjoint in K_s, then they will not be disjoint when restricted to any subgroup of K_s. Note that A is a subgroup of K_s, so it suffices to show the restrictions to A are disjoint. As $\mathrm{Res}_A^{G_\chi} \rho$ is trivial, the first restricts to a multiple (namely the dimension of ρ) of χ, and similarly the second restricts to a multiple of $s\chi$ by definition of the action of H on $\widehat{A}$. However, $s \notin G_\chi \supseteq H_\chi$, so $s\chi \neq \chi$, but as both lie in $\widehat{A}$ and are thus irreducible, they are disjoint. This proves $\theta_{\chi,\rho}$ is irreducible.

Step two. To prove the $\theta_{\chi,\rho}$ are inequivalent, we will show that χ and ρ can be uniquely recovered from $\theta_{\chi,\rho}$. Using the Frobenius character formula, Theorem 2.9, we will show that the restriction of $\theta_{\chi,\rho}$ to A consists entirely of elements in the orbit $H\chi$ of χ. For $a \in A$, we have

$$\begin{aligned}\theta_{\chi,\rho}(a) &= \sum_{\substack{g\in G/G_\chi \\ g^{-1}ag\in G_\chi}} (\chi\otimes\rho)(g^{-1}ag) \\ &= \sum_{\substack{g\in G/G_\chi \\ g^{-1}ag\in G_\chi}} \chi(g^{-1}ag) \\ &= \sum_{h\in H/H_\chi} \chi(h^{-1}ah) \\ &= \sum_{h\in H/H_\chi} (h\chi)(a),\end{aligned}$$

so the restriction of $\theta_{\chi,\rho}$ to A indeed consists entirely of elements in $H\chi$. Here, the first equality follows from the Frobenius character formula. The second equality follows from the fact that $g^{-1}ag \in A$ by normality of A, so the ρ factor can be ignored in the character. The third equality follows from the fact that the quotient map $G \to H$ descends to a bijective projection map $G/G_\chi \to H/H_\chi$, and if $g \mapsto h$ under the quotient map, then $g^{-1}ag = h^{-1}ah$ as A is abelian. The fourth equality follows from the definition of the action of H on $\widehat{A}$.

As χ various over orbit representatives, this uniquely determines χ. To recover ρ, suppose the representation space for $\theta_{\chi,\rho}$ is W; let W_χ be the subspace corresponding to χ, meaning the set of $x \in W$ such that $\theta_{\chi,\rho}(a)x = \chi(a)x$ for all $a \in A$. One can directly check that the representation of H_χ in W_i is isomorphic to ρ, uniquely recovering ρ from $\theta_{\chi,\rho}$.

Step three. Lastly, we prove every irreducible representation of G is equivalent to some $\theta_{\chi,\rho}$. Let (W,σ) be an arbitrary irreducible representation of G. Let $W = \bigoplus_{\chi\in\widehat{A}} W_\chi$ be the canonical decomposition of $\mathrm{Res}^G_A\,\sigma$, so that each W_χ corresponds to a multiple of χ. At least one of the W_χ is nonzero, so fix one such χ. For $s \in G$, we have $\sigma(s)$ transforms W_χ into another subspace of W, which we denote $W_{s(\chi)}$. Under this transformation, H_χ maps W_χ into itself. Let W' be an irreducible subrepresentation of W_χ, and let ρ be the corresponding representation of H_χ. Lifting ρ to G_χ, the restriction $\mathrm{Res}^G_{G_\chi}\,\sigma$ contains $\chi\otimes\rho$ at least once. Frobenius reciprocity then implies (see [S, p. 57]) that $\theta_{\chi,\rho} = \mathrm{Ind}^G_{G_\chi}(\chi\otimes\rho)$ contains σ at least once; as $\theta_{\chi,\rho}$ is irreducible, this implies σ and $\theta_{\chi,\rho}$ are equivalent. This completes the proof. □

4. Irreducible representations of $\mathrm{Aff}(q)$

We now apply the little group method to obtain all irreducible representations of $\mathrm{Aff}(q)$. For brevity of notation, let

$$(y,x) = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in G.$$

In this section, we will prove the following classification of irreducible representations of $\mathrm{Aff}(q)$.

Proposition 4.1. *The irreducible representations of* $\mathrm{Aff}(q)$ *consist of* $q-1$ *one-dimensional irreducible representations and one* $(q-1)$*-dimensional irreducible representation. In the first case, fixing a primitive root* b *of* $\mathbb{F}_q$*, we have a one-dimensional irreducible representation for all* $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ *given by*

$$\rho_m(b^j, x) = \exp\left(\frac{2\pi i m j}{q-1}\right),$$

for $(b^j, x) \in \mathrm{Aff}(q)$*. In the second case, our* $(q-1)$*-dimensional irreducible representation* $(L^2(H), \sigma)$ *is given by*

$$[\sigma(y,x)f](z,0) = \exp\left(\frac{2\pi i\, \mathrm{Tr}(zx)}{p}\right) f(zy,0),$$

for $(y,x) \in \mathrm{Aff}(q)$*,* $f \in L^2(H)$*, and* $(z,0) \in H$*.*

Recall the *trace* of $y \in \mathbb{F}_q$ is

$$\mathrm{Tr}(y) = y + y^p + y^{p^2} + \cdots + y^{p^{n-1}}$$

for $q = p^n$.

4.1. **Applying the little group method to** $\mathrm{Aff}(q)$**.** From Lemma 1.3, we know $\mathrm{Aff}(q) = A \ltimes H$ is a semidirect product with A abelian, so the assumptions of the little group method hold. Following the method, by identifying $(1,x) \in A$ with $x \in \mathbb{F}_q$, we first characterize the elements of $\widehat{A}$ as being the exponentials

$$\chi_a(1,x) = \exp\left(\frac{2\pi i\, \mathrm{Tr}(ax)}{p}\right) = \zeta_p^{\mathrm{Tr}(ax)}$$

for all $a \in \mathbb{F}_q$, where $\zeta_p = e^{2\pi i/p}$. An element $(y,0) \in H$ acts on this χ_a by

$$\begin{aligned}(y,0)\chi_a(1,x) &= \chi_a((y,0)^{-1}(1,x)(y,0)) \\ &= \zeta_p^{\mathrm{Tr}(axy^{-1})} \\ &= \chi_{y^{-1}a}(1,x),\end{aligned}$$

and so $(y,0)\chi_a = \chi_{y^{-1}a}$. If $a \neq 0$, then the orbit $\{y^{-1}a | y \in \mathbb{F}_q^\times\} = \mathbb{F}_q^\times$, so there are only two cosets of $\widehat{A}/H$, namely with representatives $\chi_0 \equiv 1$ and χ_1. These two representatives yield

$$\begin{aligned}H_{\chi_0} &= \{(y,0) \in H | y^{-1}0 = 0\} = H, \\ H_{\chi_1} &= \{(y,0) \in H | y^{-1}1 = 1\} = \{(1,0)\}.\end{aligned}$$

For simplicity of notation, we will let $H_0 = H_{\chi_0}$ and $H_1 = H_{\chi_1}$, and similarly use the simplified notation $G_i = A \ltimes H_i$. In particular, $G_0 = G$ and $G_1 = A$.

4.2. **The one-dimensional irreducible representations of** $\mathrm{Aff}(q)$**.** In the first case, as $H \cong \mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$, we have $\widehat{H} \cong \mathbb{Z}/(q-1)\mathbb{Z}$, consisting of $\rho_m : \mathbb{F}_q^\times \to \mathbb{C}$ given by

$$\rho_m(b^j) = \exp\left(\frac{2\pi i m j}{q-1}\right),$$

for b a fixed primitive root of $\mathbb{F}_q$, for all $m \in \{0, \ldots, q-2\}$. Lifting ρ_m to G, we express each element $(y, x) \in G$ as $(b^j, x) = (1, x)(b^j, 0)$ to yield

$$\rho_m(b^j, x) = \exp\left(\frac{2\pi i m j}{q-1}\right).$$

As

$$\theta_{\chi_0, \rho_m} = \mathrm{Ind}_G^G(\chi_0 \otimes \rho_m) = \rho_m,$$

this yields the 1-dimensional irreducible representations of $\mathrm{Aff}(q)$, of which there are $q-1$ in total.

4.3. **The $(q-1)$-dimensional irreducible representation of $\mathrm{Aff}(q)$.** The second case, where $\widehat{H}_1$ contains only the trivial representation, yields only one irreducible representation, $\sigma = \mathrm{Ind}_A^G(\chi_1)$; note that χ_1 need not be lifted as $G_1 = A$ already. This induced representation (V, σ) is on

$$\begin{aligned} V &= \{f : G \to \mathbb{C} | f(y, x+a) = \chi_1(1, a) f(y, x), \text{ for all } (1, a) \in A, (y, x) \in G\} \\ &= \{f \in L^2(G) | f(y, x+a) = \zeta_p^{\mathrm{Tr}(a)} f(y, x), \text{ for all } a, x \in \mathbb{F}_q, y \in \mathbb{F}_q^\times\}. \end{aligned}$$

This condition fixes all values of f given its values on H, as

$$f(y, x) = \zeta_p^{\mathrm{Tr}(x)} f(y, 0),$$

so $V \cong L^2(H) \cong \mathbb{C}^{q-1}$. Then

$$\begin{aligned} [\sigma(y, x) f](z, w) &= f((z, w)(y, x)) = f(zy, zx + w) \\ &= \zeta_p^{\mathrm{Tr}(w)} \zeta_p^{\mathrm{Tr}(zx)} f(zy, 0), \end{aligned}$$

where because $\sigma(y, x) f \in V$, we can reduce to only considering inputs in H, i.e.,

$$[\sigma(y, x) f](z, 0) = \zeta_p^{\mathrm{Tr}(zx)} f(zy, 0).$$

This defines a $(q-1)$-dimensional irreducible representation of $\mathrm{Aff}(q)$, which concludes the proof of Proposition 4.1.

With $q-1$ one-dimensional irreducible representations and one $(q-1)$-dimensional irreducible representation, we find

$$|\mathrm{Aff}(q)| = (q-1) \cdot 1 + (q-1)^2 = q(q-1) = |\mathbb{F}_q| \cdot |\mathbb{F}_q^\times|,$$

as expected. Hence, the little group method has found all irreducible representations of $\mathrm{Aff}(q)$.

References

[S] J.-P. Serre. *Linear Representations of Finite Groups.* Springer-Verlag (1977).

[T] A. Terras. *Fourier Analysis on Finite Groups and Applications.* Cambridge University Press (1999).

Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139