Representations over non-closed fields

Alexander Duncan

April 21, 2023

Throughout, k is a field of characteristic 0 and $\overline{k}$ is the algebraic closure of k. (For those uncomfortable with infinite Galois extensions, one can instead replace $\overline{k}$ with the Galois closure of the finitely many relevant finite field extensions showing up in any of the contexts we discuss below.)

Much of this is inspired from [Ser77, §12–13].

1 Representation Ring via Modules

Let G be a finite group.

Recall that kG is the group algebra of G over k. Since k has characterstic 0, we know kG is semisimple. We have a canonical decomposition

$$kG \cong \bigoplus_{i=1}^{r} A_i$$

where $A_1, \ldots, A_r$ are simple k-algebras.

Each A_i is a central simple F_i-algebra for a finite field extension F_i/k. Let $n_i = \deg(A_i)$ be the *degree* of A_i. Equivalently, we have $n_i^2 = \dim_{F_i}(A_i)$ or

$$A_i \otimes_{F_i} \overline{k} \cong \mathrm{M}_{n_i}(\overline{k})$$

as $\overline{k}$-algebras.

More precisely, there exists a central division F_i-algebra D_i and a positive integer m_i such that

$$A_i \cong \mathrm{M}_{m_i}(D_i)$$

as F_i-algebras. Both m_i and the isomorphism class of D_i are uniquely determined. Let $d_i := \mathrm{ind}(A_i)$ denote the Schur index of A_i. We have $d_i = \deg(D_i)$, which is equivalent to $d_i^2 = \dim_{F_i}(D_i)$. Also, we have $n_i = m_i d_i$.

Each A_i has a simple module V_i, which is unique up to isomorphism. Since $V_i \cong D_i^{\oplus n_i}$, we see that

$$\dim_k V_i = [F_i : k] m_i d_i^2 = [F_i : k] d_i n_i.$$

The vector spaces $V_1, \ldots, V_r$ are precisely the irreducible representations of G over k. The *Schur index* of V_i is defined to be the Schur index d_i of the associated algebra A_i.

Let Γ be the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$. Let $X_i := \mathrm{Hom}_{k-\mathrm{alg}}(F_i, \overline{k})$. Observe that X_i has a left action of Γ by post-composition. Informally, X_i can be thought of as the set of roots of the minimal polynomial of a primitive element of F_i/k. We have a $\overline{k}$-algebra isomorphism

$$\omega : F_i \otimes_k \overline{k} \cong \bigoplus_{\sigma \in X_i} \overline{k}$$

via $\omega(f \otimes \ell)_\sigma := \sigma(f)\ell$.

For each $\sigma \in X_i$, we may define a tensor product $A_i \otimes_\sigma \overline{k}$ of F_i-algebras where we use the structure map $F_i \to A_i$ on the left and the homomorphism $\sigma : F_i \to \overline{k}$ on the right. Via the sequence of isomorphisms of $\overline{k}$-algebras

$$A_i \otimes_k \overline{k} \cong A_i \otimes_{F_i} F_i \otimes_k \overline{k} \cong A_i \otimes_{F_i} \bigoplus_{\sigma \in X_i} \overline{k}$$

we obtain an isomorphism

$$\Omega : A_i \otimes_k \overline{k} \cong \bigoplus_{\sigma \in X_i} A_i \otimes_\sigma \overline{k}.$$

Let $W_{i,\sigma}$ be the irreducible representation of $\overline{k}G$ corresponding to $A_i \otimes_\sigma \overline{k}$. We conclude that we have the following decomposition

$$V_i \otimes_k \overline{k} \cong \bigoplus_{\sigma \in X_i} W_{i,\sigma}^{\oplus d_i}$$

for each irreducible representation V_i of kG.

If $\rho_{i,\sigma} : G \to \mathrm{GL}(W_{i,\sigma})$ are the corresponding maps, then notice that

$$\tau \circ \rho_{i,\sigma} = \rho_{i,\tau(\sigma)}$$

for every $\tau \in \Gamma$. Thus, there is a left action of Γ on the set of irreducible representations of G over $\overline{k}$ with orbits corresponding to the Γ-sets X_i.

2 Character Theory

We have only developed character theory over $\mathbb{C}$. However, since we are dealing with finite-dimensional representations of finite groups, by the Lefschetz principle all the results we discussed hold over an arbitary algebraically closed field of character 0. In particular, we may identify the representation rings $R(G) = R_{\mathbb{C}}(G) = R_{\overline{k}}(G)$ where $\overline{k}$ is the algebraic closure of k.

Recall that the representation ring $R_k(G)$ of G over k is the additive group of virtual representations over k with multiplication obtained extending the tensor product on the subrig $R_k^+(G)$. From above, we see that $R_k(G)$ is a free abelian group on the set $[V_1], \ldots, [V_r]$.

The map $[V] \mapsto [V \otimes_k \overline{k}]$ gives a canonical injective ring homomorphism

$$R_k(G) \hookrightarrow R_{\overline{k}} = R(G)$$

and therefore a canonical injective ring homomorphism

$$R_k(G) \hookrightarrow C(G)$$

where $C(G)$ is the set of complex class functions on G.

Just as in the complex case, given a representation (V, ρ) of G over k, we define the character $\chi_V : G \to k$ via the trace $\chi_V(g) := \mathrm{tr}(\rho(g))$. This agrees with the map $R_k(G) \hookrightarrow C(G)$ defined above. Thus, we identify $R_k(G)$ with a subring of $R(G)$ and $C(G)$ in what follows.

Let $\chi_1, \ldots, \chi_r$ be the irreducible representations of G over k corresponding to the algebras $A_1, \ldots, A_r$ above. Let $\psi_{i,\sigma} : G \to \overline{k}$ be the character corresponding to the irreducible representation $W_{i,\sigma}$ defined in the previous section.

Theorem 2.1. *For every $1 \leq i \leq r$, we have*

$$\chi_i = d_i \sum_{\sigma \in X_i} \psi_{i,\sigma}.$$

In particular, the characters $\chi_1, \ldots, \chi_r$ are an orthogonal basis for the subspace $R_k(G)$ of $C(G)$.

Proof. The description of χ_i follows from the results in the previous section. The orthogonality follows from the fact that the $\psi_{i,\sigma}$ are orthogonal. □

Note that we only have the $\{\chi_1, \ldots, \chi_r\}$ is an *orthogonal* basis; it is not necessarily orthonormal.

There are in fact *three* different traces that one may consider for each irreducible representation V_i. We have the ordinary trace $\chi_i(g) \in k$ as an element of $\mathrm{End}_k(V_i)$. We may also define $\phi_i(g) \in F_i$ as the trace of g in $\mathrm{End}_{F_i}(V_i)$. Finally, we have $\psi_i(g) \in F_i$ as the reduced trace $\mathrm{Trd}(g)$ viewing g as an element of the central simple F_i-algebra A_i. These traces are all related via

$$\chi_i = \mathrm{Tr}_{F_i/k} \circ \phi_i, \quad \phi_i = d_i \psi_i$$

where we recall that d_i is the Schur index of the central simple F_i-algebra A_i (equivalently, the representation V_i). Finally for each $\sigma \in X_i$, we see that $\psi_{i,\sigma} = \sigma \circ \psi_i$. This gives another way of obtaining the decomposition of $V_i \otimes_k \overline{k}$ above.

2.1 Definability of Representations

Recall, from the previous section, that the absolute Galois group permutes the irreducible representations of $\overline{k}G$. Indeed, if $\rho_{i,\sigma} : G \to \mathrm{GL}(W_{i,\sigma})$ is the map then we have

$$\tau \circ \rho_{i,\sigma} = \rho_{i,\tau(\sigma)}$$

for $\tau \in \Gamma$. This action is identical to the one obtained by acting on the characters

$$\tau \circ \phi_{i,\sigma} = \phi_{i,\tau(\sigma)}$$

where we recall $\phi_{i,\sigma} : G \to \overline{k}$ is just a particular class function.

Theorem 2.2. *Let $\overline{R}_k(G)$ be the subset of $R(G)$ consisting of characters whose class functions whose image is defined over k. Then $\overline{R}_k(G)$ has basis*

$$\frac{\chi_1}{d_1}, \frac{\chi_2}{d_2}, \cdots, \frac{\chi_r}{d_r}.$$

Thus $\overline{R}_k(G)$ can be completely recovered from the character table over $\mathbb{C}$. Namely, one can reconstruct the χ_i/d_i as the sums of Γ-orbits of the complex characters. To reconstruct $\overline{R}_k(G)$, one needs to know the Schur indices.

Proposition 2.3. *If G is an abelian group, then $R_k(G) = \overline{R}_k(G)$*

Proof. If G is abelian, then kG is commutative, so all constituent division algebras are fields. Thus all Schur indices are trivial. □

We are now in a position to prove an important theorem of Brauer, which essentially reduces the study of definability of representations of arbitrary fields of characteristic 0 to the case of cyclotomic fields.

Theorem 2.4. *If G is a finite group of exponent e, then every representation of G over an arbitrary field of characteristic 0 is conjugate to a representation defined over the cyclotomic field $\mathbb{Q}(\zeta_e)$.*

Proof. Let $K = \mathbb{Q}(\zeta_e)$. We want to show that $R_K(G) = R(G)$. By Brauer's theorem, we may write a general element χ of $R(G)$ in the form

$$\rho = \sum_{i=1}^{m} c_i \operatorname{Ind}_{H_i}^{G}(\tau_i)$$

where the c_i's are integers, the H_i are subgroups of G, and each τ_i is a one-dimensional representations of $R(H_i)$. A one-dimensional representation of H_i is defined over $\mathbb{Q}(\zeta_e)$ since H_i has exponent at most e. We conclude that χ is an integral linear combination of representations induced from $R_K(H_i)$, so is in $R_K(G)$ as desired. □

3 Column Orthogonality

We saw above that $\chi_1, \ldots, \chi_r$ are an orthogonal basis for $R_k(G)$. This amounts to showing that the *rows* of the character table of G (over k) are orthogonal. However, we now have "too many" columns if we expect a square character table. Here we investigate this issue.

For each positive integer n, define the *Adams operation* $\Psi^n : C(G) \to C(G)$ as the function that takes a class function χ to the class function $\Psi^n(\chi)$ defined by

$$\Psi^n(\chi)(g) := \chi(g^n)$$

for each $g \in G$.

Proposition 3.1. *Every Adams operation restricts to a ring homomorphism from $R_k(G)$ to itself.*

Proof. Let χ be the character of a representation (V, ρ). For a given g, consider the multiset of eigenvalues

$$a_1, \ldots, a_m$$

of $\rho(g)$. Thus $\chi(g) = p_1$ where p_1 is the first power sum polynomial in $a_1, \ldots, a_m$. We have $\chi(g^n) = p_n$ where p_n is the power sum polynomial

$$a_1^n + \cdots + a_m^n.$$

By the fundamental theorem of symmetric polynomials, there exists a polynomial f_n with integer coefficients such that

$$p_n = f_n(e_1, \ldots, e_m)$$

where $e_1, \ldots, e_m$ are the elementary symmetric polynomials in $a_1, \ldots, a_n$.

The function f_n does not depend on the eigenvalues, so we have an expression

$$\Psi^n(\chi) = f_n(\Lambda^1\chi, \ldots, \Lambda^n\chi)$$

in the ring $C(G)$. Since exterior powers of a representation are representations, we see that $\Psi^n(\chi)$ is in $R_k(G)$ as desired. □

Recall that the *exponent* e of a finite group is the least common multiple of the orders of all the elements $g \in G$. Equivalently, the exponent e is the least positive integer such that $g^e = 1$ for all $g \in G$.

Lemma 3.2. *If n is relatively prime to e, then the function $g \mapsto g^t$ is a bijection from G to itself, which takes conjugacy classes to conjugacy classes.*

Proof. Let s be the multiplicative inverse of n modulo e, which exists since t is relatively prime to e. The function $g \mapsto g^s$ is the inverse function to $g \mapsto g^t$ since $g^{ts} = g^1 = g$. □

From this we immediately conclude:

Corollary 3.3. *If t is relatively prime to e, then $\Psi^t : R(G) \to R(G)$ is an isomorphism.*

Thus, for appropriate t, the Adams operations Ψ^t permute the *columns* of the character table of $R(G)$.

In view of Theorem 2.4, we may assume that $k \subseteq K = \mathbb{Q}(\zeta_e)$ where e is the exponent of G. Let Γ be the Galois group of K/k. Observe that Γ is a subgroup of $(\mathbb{Z}/e\mathbb{Z})^\times$. Let Γ be generated by $\sigma_1, \ldots, \sigma_s$ where $\sigma(\zeta_e) = \zeta_e^t$ for some $t_1, \ldots, t_s$ in $(\mathbb{Z}/e\mathbb{Z})^\times$.

We now have two actions of Γ on $R(G)$. Given $\gamma \in \Gamma$ and $\chi \in R(G)$, we have

$$(\gamma * \chi)(g) := \gamma(\chi(g))$$

for all $g \in G$, where we view $\chi : G \to K$ as a function with codomain $K \subset \overline{k}$. We also have the action using the Adams operation which is generated by

$$\sigma_i *' \chi := \Psi^{t_i}(\chi)$$

for $1 \leq i \leq s$.

Proposition 3.4. *The two actions of* Γ *on* $R(G)$ *coincide.*

Proof. The eigenvalues of every matrix M in every representation of G is an eth root of unity. Thus, if χ is a character in $R(G)$, then

$$(\sigma_i \circ \chi)(g) = \Psi^{t_i}(\chi)(g)$$

for every $\sigma \in \Gamma$. □

Observe that we can define the Γ-action directly on the conjugacy classes of G using the above identification. In view of this, we define the Γ-*classes* (or K-*classes*) of G to be the unions of Γ-orbits of conjugacy classes. We therefore have:

Theorem 3.5. $\overline{R}_k(G)$ *is precisely the subset of* $R(G)$ *whose corresponding characters are fixed by the* Γ*-action.*

As an immediate corollary, we obtain:

Corollary 3.6. *The number of irreducible characters of* G *over* k *is equal to the number of* Γ*-classes of* G*.*

Note that the particular action of Γ on G is determined by a choice of isomorphism of Γ with its image in $(\mathbb{Z}/e\mathbb{Z})^\times$, but the Γ-classes do not depend on this choice. Thus the Γ-classes of G are totally group-theoretic. In particular, we don't actually need to compute the character table to determine the number of irreducible representations (just like over $\mathbb{C}$).

However, we only obtain $\overline{R}_k(G)$ from this analysis. More work needs to be done to identify the Schur indices.

3.1 Representations over the rationals

Here we consider the important special case where $k = \mathbb{Q}$. Let G be a finite group with exponent e. As above, $K = \mathbb{Q}(\zeta_e)$ where ζ_e is a primitive eth root of unity. The Galois group $\Gamma = \mathrm{Gal}(K/k)$ is isomorphic to the full group $(\mathbb{Z}/e\mathbb{Z})^\times$ by standard results on cyclotomic fields.

In this case, the Γ-classes from above have a simple description:

Lemma 3.7. *Two elements $g, h \in G$ belong to the same $\mathbb{Q}$-class if and only if they generate conjugate cyclic subgroups.*

Proof. Observe that $\langle g \rangle = \langle h \rangle$ if and only if $g^s = h$ and $h^t = g$ for some integers s and t. Observe that t, s are relatively prime to $n = \langle g \rangle$. Since n divides the exponent e of G, we have a surjective group homomorphism $(\mathbb{Z}/e\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. Thus, we may assume s and t are relatively prime to e. Since $\Gamma \cong (\mathbb{Z}/e\mathbb{Z})^\times$, we conclude $\langle g \rangle = \langle h \rangle$ if and only if g and h are in the same Γ-orbit. This respects conjugacy classes. □

We conclude the following:

Theorem 3.8. *The number of isomorphism classes of irreducible representations of a finite group G over $\mathbb{Q}$ is equal to the number of conjugacy classes of cyclic subgroups of G.*

We point out the following pleasant parallels with permutation representations and complex representations:

- The number of irreducible **permutation** representations are in bijection with the number of conjugacy classes of **subgroups**.
- The number of irreducible **rational** representations are in bijection with the number of conjugacy classes of **cyclic subgroups**.
- The number of irreducible **complex** representations are in bijection with the number of conjugacy classes of **elements**.

4 Representations over the reals

Let V be a finite-dimensional complex representation of a finite group G.

Proposition 4.1. *V has a G-invariant inner product.*

Proof. Let $b : V \times V \to \mathbb{C}$ be an inner product (not necessarily G-invariant). Define a function $B : V \times V \to \mathbb{C}$ by

$$B(v, w) = \sum_{g \in G} b(gv, gw)$$

for $v, w \in V$. Observe that B is also sesquilinear and that $B(v, v) > 0$ for all $v \neq 0$. Thus B is also an inner product. □

The previous proposition has the following interpretation:

Corollary 4.2. *Every finite subgroup of* $\mathrm{GL}_n(\mathbb{C})$ *is conjugate to a finite subgroup of the unitary group* $\mathrm{U}(n)$.

Crucially, we can only produce a *sesquilinear* form in general; there may not be a non-trivial *bilinear* form. For example, a non-trivial one-dimensional complex representation of $G = \mathbb{Z}/3\mathbb{Z}$ has no non-trivial G-invariant bilinear forms; otherwise, we have a contradiction

$$1 = (v, v) = (gv, gv) = (\zeta_3 v, \zeta_3, v) = \zeta_3^2 (v, v) = \zeta_3^2$$

for v a vector of norm one and g a generator of G.

However, we know that sesquilinear forms and bilinear forms are essentially the same over real closed fields. It turns out this leads to an interesting theory. We say that V is *realizable over* $\mathbb{R}$ if there exists a real representation W of G such that $W \otimes_{\mathbb{R}} \mathbb{C} \cong V$.

Theorem 4.3 (Frobenius-Schur)**.** *A complex representation V is realizable over $\mathbb{R}$ if and only if there exists a G-invariant non-degenerate symmetric bilinear form on V.*

Proof. Suppose first that V is realizable over $\mathbb{R}$. Let W be the real representation such that $V = W \otimes_{\mathbb{R}} \mathbb{C}$. Observe that W has a G-invariant non-degenerate symmetric bilinear form q by the same argument as Proposition 4.1 (inner products are the same as non-degenerate symmetric bilinear forms over $\mathbb{R}$). Now $q \otimes_{\mathbb{R}} \mathbb{C}$ is a G-invariant non-degenerate symmetric bilinear form on V.

For the converse, we have a non-degenerate symmetric bilinear form B on V. We also have a G-invariant inner product $(-, -)$. We define a function $\varphi : V \to V$ such that

$$B(x, y) = (\varphi(x), y)$$

for all $x, y \in V$ (this is unique and well-defined since both B and the inner product are non-degenerate). Observe that φ is conjugate-linear and bijective. Thus φ^2 is a linear automorphism of V.

We claim φ^2 is a positive-definite Hermitian operator. Indeed,

$$(\varphi^2(x), y) = B(\varphi(x), y) = B(y, \varphi(x)) = (\varphi(y), \varphi(x))$$

for all $x, y \in V$. Thus we have

$$\overline{(\varphi(x), \varphi(y))} = \overline{(\varphi^2(y), x)}.$$

Since inner products are conjugate-symmetric, we obtain

$$(\varphi^2(x), y) = (x, \varphi^2(y))$$

and conclude that φ^2 is Hermitian. Moreover, $(\varphi^2(x), x) = (\varphi(x), \varphi(x))$ implies that we have positive-definiteness.

Every positive-definite Hermitian operator φ^2 has a unique positive-definite Hermitian square root ω such that $\omega^2 = \varphi^2$. Moreover, ω commutes with φ. Let $\sigma = \varphi\omega^{-1}$. We see that $\sigma : V \to V$ is a conjugate-linear map with square equal to the identity. Moreover, σ is G-equivariant.

Since σ is conjugate-linear, it is in particular $\mathbb{R}$-linear. Let V_R be the (real) 1-eigenspace of σ and let V_I be the (real) -1-eigenspace of σ. Since σ is conjugate-linear, we see that $V_I = iV_R$. We therefore have $V = V_R \oplus iV_I$ as desired. □

Now assume V is irreducible and let χ be its character.

Definition 4.4. The *Frobenius-Schur indicator* of V is the number

$$\iota(V) := \frac{1}{|G|} \sum_{g \in G} \chi(g^2).$$

In order to understand representation theory over $\mathbb{R}$, it is worth pointing out that there are only three division $\mathbb{R}$-algebras: the real field $\mathbb{R}$, the complex field $\mathbb{C}$, and Hamilton's quaternions $\mathbb{H}$. The irreducible representation V is a simple module of $A \otimes_{\mathbb{R}} \mathbb{C}$ where A is a simple subalgebra of $\mathbb{R}G$ and $A \cong \mathrm{M}_n(D)$ where D is one of the three cases above.

Thus, we get a trichotomy of the real behavior of complex representations based on the division algebra to which they are associated.

Complex:

- The division algebra corresponding to V is $\mathbb{C}$,
- Frobenius-Schur indicator is $\iota(V) = 0$,
- V does not have a G-invariant non-degenerate bilinear form,
- χ is not real valued,
- V is not realizable over $\mathbb{R}$, and
- V is not isomorphic to its dual $V^\vee$.

Real:

- The division algebra corresponding to V is $\mathbb{R}$,
- Frobenius-Schur indicator is $\iota(V) = 1$,
- V has a G-invariant non-degenerate symmetric bilinear form,
- χ is real valued,
- V is realizable over $\mathbb{R}$, and
- $V \cong V^\vee$.

Quaternionic:

- The division algebra corresponding to V is $\mathbb{H}$,
- Frobenius-Schur indicator is $\iota(V) = -1$,
- V has a G-invariant non-degenerate skew-symmetric bilinear form,
- χ is real valued,
- V is not realizable over $\mathbb{R}$, but
- $V \oplus V$ is realizable over $\mathbb{R}$, and
- $V \cong V^\vee$.

We merely sketch why the above characterization holds, leaving details to the reader (or [Ser77, §13.2]). Most of the characterizations follow quickly from Wedderburn theory, so we focus on the bilinear forms.

Note that bilinear forms are equivalent to maps between V and $V^\vee$, where non-triviality is equivalent to non-degeneracy by Schur's Lemma since we want G-invariance. Schur's Lemma also tells us G-invariant bilinear forms are unique up to scaling. The decomposition of a bilinear form into a symmetric and skew-symmetric part is G-invariant, so uniqueness up to scaling implies that the form must be either symmetric or skew-symmetric. Having a *symmetric* bilinear form is equivalent to being realizable over the reals by Theorem 4.3 above.

Finally, we consider the Frobenius-Schur indicator. A G-invariant symmetric bilinear form on V is equivalent to having a trivial subrepresentation of $\mathrm{Sym}^2(V)$. Similarly, a G-invariant skew-symmetric bilinear form on V is equivalent to having a trivial subrepresentation of $\mathrm{Alt}^2(V)$. Recall the formulas for the characters of the symmetric and alternating squares:

$$\chi_{\mathrm{Sym}^2(V)} = \chi_V^2 + \Psi^2(\chi_V) \text{ and } \chi_{\mathrm{Alt}^2(V)} = \chi_V^2 - \Psi^2(\chi_V).$$

Thus, we have $(1, \chi_{\mathrm{Sym}^2(V)}) = 1$ iff V is real, $(1, \chi_{\mathrm{Alt}^2(V)}) = 1$ iff V is quaternionic, and they are 0 otherwise.

Now we simply observe that

$$\chi_V^2 = \chi_{\mathrm{Sym}^2(V)} + \chi_{\mathrm{Alt}^2(V)}$$

and

$$\iota(V) := \frac{1}{|G|} \sum_{g \in G} \chi(g^2) = (1, \Psi^2(\chi_V)).$$

References

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups.* Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott.