Complex Representations of $\mathrm{GL}(2, K)$ for Finite Fields K

Ilya Piatetski-Shapiro

1983

Contents

Forward

These are lectures notes of a course that I gave in Tel Aviv University. The aim of these notes is to present the theory of the representations of $\mathrm{GL}(2, K)$ where K is a finite field. However, the presentation of the material has in mind the theory of infinite-dimensional representations of $\mathrm{GL}(2, K)$ for local fields K.

I am very grateful to Moshe Jarden who took these notes and worked them out. Without him, it would have been completely impossible to prepare them.

This course and its notes are the first outcome of the Cissie & Aaron Beare Chair in Algebra and Number Theory.

Ilya Piatetski-Shapiro
Tel Aviv
November, 1982

Introduction

The aim of these notes is to give a description of the complex irreducible representations of the group $G = \mathrm{GL}(2, K)$, where K is a finite field with $q > 2$ elements. In addition, these notes should also serve as a motive for the study of the representation of $\mathrm{GL}(2, K)$, where K is a local field. Therefore, an attempt has been made to reprove theorems by not explicitly using the finiteness of K.

A central role in the description of the representations of G is played by the Borel subgroup consisting of all matrices

$$b = \begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix} \qquad \alpha, \delta \in K^\times, \qquad \beta \in K.$$

If μ_1, μ_2 are characters of $K^\times$, then a character μ of B can be defined by $\mu(b) = \mu_1(\alpha)\mu_2(\delta)$. Let $\hat{\mu} = \mathrm{Ind}_B^G$ be the induced representation. If $\mu_1 = \mu_2$, then $\hat{\mu}$ splits as the direct sum of a one-dimensional representation ρ'_{μ_1,μ_1} which is given by formula $\rho'_{\mu_1,\mu_1}(g) = \mu_1(\deg g)$, and a q-dimensional irreducible representation ρ_{μ_1,μ_1}. There are $q - 1$ representations of each kind. If $\mu_1 \neq \mu_2$, then $\hat{\mu} = \rho_{\mu_1,\mu_2}$ is an irreducible representation of dimension $q + 1$. There are $\frac{1}{2}(q - 1)(q - 2)$ representations of this kind. Irreducible representations that are not of the above types are of dimension $q - 1$ and are called cuspidal representations. They are however also connected with linear characters in the following way. Let L be the unique quadratic extension of K and let ν be a character of $L^\times$ for which there does not exist a character χ of $K^\times$ such that $\chi(\mathrm{N}_{L/K}\, z) = \nu(z)$ for every $z \in L^\times$. Such a ν is said to be non-decomposable. For each non-decomposable character ν of $L^\times$, we explicitly construct an irreducible representation ρ_ν of G and prove that it is cuspidal. Conversely, w prove that every cuspidal representation of G is of the form ρ_ν for some non-decomposable character ν of $L^\times$. Thus, there are $\frac{1}{2}\left(q^2 - q\right)$ cuspidal representations.

The connection between the irreducible representations of G and the characters of $K^\times$ and $L^\times$ gives rise to a reciprocity law. Let $W(L/K) = L^\times \rtimes \mathrm{Gal}(L/K)$ be the semi-direct product of $L^\times$ by $\mathrm{Gal}(L/K)$. The irreducible representations of $W(L/K)$ (which is called the small Weil group) of dimension ≤ 2. The announced reciprocity law is a natural bijection between the two-dimensional representations of $W(L/K)$ (including the reducible ones) and the irreducible representations of G of dimension > 1.

Next, we attempt to give explicit models for the irreducible representations of G. Let ψ be a non-unit character of K^+. The additive group K^+ can be canonically identified with the subgroup U of G consisting of all the matrices of the form

$$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}, \qquad \beta \in K.$$

Therefore, ψ can also be constructed as a character of U. We prove that $\mathrm{Ind}_U^G\, \psi$ splits into the direct sum of all irreducible representations ρ of G of dimension > 1.; each ρ appears with multiplicity 1. The space V_ρ on which ρ acts can therefore be embedded into $\mathrm{Ind}_U^G\, V_\psi$. Thus, to each $v \in V_\rho$, there corresponds a function $W_v\colon G \to \mathbb{C}$ such that $W_v(ug) = \psi(u)W'_v(g)$ for every $u \in U$ and $g \in G$. The action of ρ on these functions is given by $W_{\rho(s)v}(g) = W_v(gs)$. The collection of all the W_v is called a Whittaker model for ρ. It has the following property: for all characters ω of $K^\times$, except possible two, there exists complex numbers $\Gamma_\rho(\omega)$

such that

$$\Omega_\rho(\omega) \sum_{x \in K^\times} W_v \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \omega(x) = \sum_{x \in K^\times} W_v \begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix} \omega(x) \tag{0.1}$$

for every $v \in V_\rho$. If ρ is a cuspidal representation, then $\Gamma_\rho(\omega)$ is defined for every ω.

Among the Whittaker functions for ρ, there is a special one, J_ρ, called the Bessel function of ρ, that satisfies

$$J_\rho(gu) = J_\rho(ug) = \psi(u) J_\rho(g) \qquad \text{for} \qquad u \in U, g \in G.$$

Further, $J_\rho(1) = 1$ and $J_\rho(u) = 0$ for $u \in U$ and $u \neq 1$. Substituting this function for W_v in (0.1),

$$\Gamma_\rho(w) = \sum_{x \in K^\times} J_\rho \begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix} \omega(x).$$

This formula is then used to express $\Gamma_\rho(\omega)$ in terms of Gauss sums.

- If $\rho = \rho_{\mu_1, \mu_2}$ is a non-cuspidal representation of G, then

$$\Gamma_\rho(\omega) = \frac{\omega(-1)}{q} G_K\left(\mu_1^{-1}\omega^{-1}, \psi\right) G_K\left(\mu_2^1 \omega^{-1}, \psi\right).$$

- If $\rho = \rho_\nu$ is a cuspidal representation, then

$$\Gamma_\rho(\omega) = \frac{\nu(-1)}{q} G_L\left(\nu \circ (\omega \circ \mathrm{N}_{L/K})^{-1}, \psi \circ \mathrm{Tr}_{L/K}\right).$$

The Gauss sum $G_K(\chi, \psi)$ is defined for a character ψ of $K^\times$ by

$$G_K(\chi, \psi) = \sum_{x \in K^\times} \chi(x) \psi(x).$$

In particular, it follows that in every case $|\Gamma_\rho(\omega)| = 1$.

All of these results are finally applied in order to compute the character table for G.

THEME 1

PRELIMINARIES: REPRESETATION THEORY; THE GENERAL LINEAR GROUP

In the first three sections of this chapter, we bring all the definitions and theorems about linear representations of finite groups that we need in these notes. We refer to the appendix for proofs. The remaining two sections are devoted to a description of the group-theoretic properties of $\mathrm{GL}(2, K)$, where K is a finite field.

1.1 Linear representations of finite groups

Let V be a finite-dimensional vector space over the field $\mathbb{C}$ of the complex numbers. Denote by $\mathrm{Aut}(V)$ the group of all automorphisms of V. Let G be a finite group. A *linear representation* of G in V is a homomorphism ρ of G into $\mathrm{Aut}(V)$. Then V is said to be the *representation space* of ρ and is also denoted by V_ρ. We shall also say that G *acts on* V_ρ *through* ρ. The *dimension* of ρ is defined to be the dimension of V_ρ and is denoted by $\dim \rho$. Two representations ρ and ρ' of G are said to be *isomorphic* if there exists an isomorphism $\theta\colon V_\rho \to V_{\rho'}$ such that $\theta \circ \rho(g) = \rho'(g) \circ \theta$ for every $g \in G$. We shall usually identify isomorphic representations.

A representation of G of dimension 1 is a homomorphism μ of G into the multiplicative group $\mathbb{C}^\times$ of $\mathbb{C}$. Such a representation is called in these notes a *character* of G. In particular, the unit character is the homomorphism of G into $\mathbb{C}^\times$ obtaining the value 1 for every $g \in G$.

Let ρ be a representation of G and let H be a subgroup of G. Suppose that μ is a character of H for which there exists a nonzero $v \in V_\rho$ such that $\rho(h)v = \mu(h)v$ for every $h \in H$. Then μ is said to be an *eigenvalue* of H (with respect to ρ), and v is said to be an *eigenvector* of H that belongs to μ.

Again, consider a representation ρ of G and let V' be a subspace of $V = V_\rho$ which is left invariant by $\rho(g)$ for every $g \in G$. In this case, we say that V' is *left-invariant* by G or that V' is a G-subspcae of V. Then the restriction map of $\rho(g)$ to V' gives rise to a representation ρ' of G with V' as its representation space. This representation is said to be a *subrepresentation* of ρ, and we write $\rho' \leq \rho$.

By a theorem of Maschke V' has a complement in V, i.e., there exists another G-subspace v'' of V such that $V = V' \oplus V''$. Let ρ'' be the corresponding subrepresentation of ρ. Then ρ is said to be a *direct sum* of ρ' and ρ'', and we write $\rho = \rho' \oplus \rho''$. Clearly $\dim \rho = \dim \rho' + \dim \rho''$. The direct sum of n representations of G, all isomorphic to ρ, is denoted by $n\rho$. A representation ρ of V is said to be *irreducible* if its does not have a subrepresentation ρ' of a lower dimension. By the theorem of Maschke, this is equivalent to saying that ρ cannot be decomposed as a direct sum $\rho = \rho' \oplus \rho''$ with $\dim \rho', \dim \rho'' < \dim \rho$. It follows that every representation ρ of G can be represented as a direct sum

$$\rho = \bigoplus_{i=1}^{k} n_i \rho_i,$$

where the ρ_i are distinct (i.e., not-isomorphic) irreducible representations of G. This decomposition of ρ is unique, up to the order of the summands.

There are only finitely many irreducible representations $\rho_1, \ldots, \rho_n$ of G. Their number h is called to the number of the conjugacy classes of G. Their dimensions satisfy the formula

$$\sum_{i=1}^{n} (\dim \rho_i)^2 = |G|. \tag{1.1}$$

If G is abelian, then (1.1) implies that the irreducible representations of G are of dimension 1 (i.e., they are characters) and that their number is equal to $|G|$, which in this case is the number of the conjugacy classes of G. Further, the set of characters of G forms a multiplicative group $\widehat{G}$ which is isomorphic to G. If $1 \neq \chi \in \widehat{G}$, then we have the following orthogonality relation:

$$\sum_{g \in G} \chi(g) = 0.$$

A lemma of Artin says that the characters of G are linearly independent; i.e., if a_χ are complex numbers such that $\sum_{\chi \in \widehat{G}} a_\chi \chi(g) = 0$ for every $g \in G$, then $a_\chi = 0$ for all $\chi \in G$. Now, G is canonically isomorphic to the dual $\widehat{\widehat{G}}$ of $\widehat{G}$. Hence, the dual to this lemma is also true: if b_g are complex numbers such that $\sum_{g \in G} b_g \chi(g) = 0$ for every $\chi \in G$, then $b_g = 0$ for all $g \in G$.

If G is again an arbitrary group, then we deduce it has $[G : G^c]$ characters, where G^c is the commutator subgroup of G. Another consequence of (1.1) is that if distinct irreducible representations $\rho_1, \ldots, \rho_n$ of G satisfy $\sum_{i=1}^{n} (\dim \rho_i)^2 = |G|$, then they are all the irreducible representations of G.

Let ρ be a representation of a finite group G. Then V_ρ can also be considered as a module over the group ring $\mathbb{C}[G]$. If ρ' is an additional representation, then we write $(\rho, \rho') = (\rho, \rho')_G := \dim \mathrm{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'})$. The form (ρ, ρ') is clearly symmetric and bilinear with respect to direct sums. If ρ and ρ' are irreducible, then, by a lemma of Schur, $(\rho, \rho') = 1$ if $\rho = \rho'$ and $(\rho, \rho') = 0$ if $\rho \neq \rho'$. It follows that two arbitrary representations ρ and ρ' are *disjoint*, i.e., have no common irreducible subrepresentations, if and only if $(\rho, \rho') = 0$. In particular, an irreducible representation ρ *appears* in a representation ρ', i.e., $\rho \leq \rho'$, if and only if $(\rho, \rho') \neq 0$; indeed, (ρ, ρ') is equal to the multiplicity in which ρ appears in ρ'.

Let $\mathrm{End}_{\mathbb{C}[G]} V_\rho := \mathrm{Hom}_{\mathbb{C}[G]}(V_\rho, V_\rho)$. It is an algebra over $\mathbb{C}$ called the *Schur algebra*. If ρ is irreducible, then $\mathrm{End}_{\mathbb{C}[G]} V)_{n\rho}$ is isomorphic to $M_n(\mathbb{C})$, the algebra of all $n \times n$ matrices over $\mathbb{C}$. If $\rho = \bigoplus_{i=1}^{k} n_i \rho_i$ is the canonical decomposition of a representation ρ, then, by Schur's lemma,

$$\mathrm{End}_{\mathbb{C}[G]} V_\rho = \bigoplus_{i=1}^{k} M_{n_i}(\mathbb{C}).$$

Hence, $(\rho, \rho) = \dim \mathrm{End}_{\mathbb{C}[G]} V_\rho = \sum_{i=1}^{k} n_i^2$. It follows that ρ has no multiple components, i.e., that $n_i = 1$ for all i, if and only if $\mathrm{End}_{\mathbb{C}[G]} V_\rho$ is commutative. In this case, $\dim \mathrm{End}_{\mathbb{C}[G]} V_\rho$ is the number of components of ρ.

Finally, consider a vector space V of dimension n over $\mathbb{C}$. Every base $v_1, \ldots, v_n$ of V canonically defines an isomorphism $\mathrm{Aut}\, V \cong \mathrm{GL}(n, \mathbb{C})$ (which is the group of all $n \times n$ invertible matrices over $\mathbb{C}$). If $\rho\colon G \to \mathrm{Aut}\, V$ is a representation of G, then we define $\chi_\rho(g)$ to be the trace of $\rho(g)$, where $\rho(g)$ is now considered as an element of $\mathrm{GL}(n, \mathbb{C})$ via the above isomorphism. Clearly, $\mathrm{tr}\, \rho(g)$ does not depend on the choice of the basis $v_1, \ldots, v_n$ of V. Hence, $\chi_\rho\colon G \to \mathbb{C}$ is a well-defined function, called the *character of* ρ. It is constant on conjugacy classes. Also, $\chi_{\rho_1 \oplus \rho_2} = \chi_{\rho_1} + \chi_{\rho_2}$. Therefore, χ_ρ is said to be *irreducible* if ρ is irreducible. If $\dim \rho = 1$, then $\chi_\rho = \chi$. In general, one defines $\dim \chi_\rho = \dim \rho$ and refers to χ_ρ as a *higher-dimensional character*.

1.2 Induced representations

Let G be a finite group and let H be a subgroup operating on a finite-dimensional $\mathbb{C}$-vector space W through a representation $\tau\colon H \to \mathrm{Aut}\, W$. Define a vector space V to be the set of all functions $f\colon G \to W$ that satisfy

$$f(hg) = \tau(h) f(g) \qquad \text{for all } h \in H \text{ and } g \in G.$$

Thus, in order to define an element $f \in V$, it suffices to give its values on a system of representatives G/H of the left classes of G modulo H. Define an operation of G on V by

$$(sf)(g) \coloneqq f(gs) \qquad \text{for } s, g \in G \text{ and } f \in V.$$

The $\mathbb{C}[G]$-module V thus obtained is called the *induced module of W from H to G* and is denoted by $\operatorname{Ind}_H^G \tau$.

We embed W in V by mapping each $w \in W$ to the function $f_w \colon W \to \mathbb{C}$ defined by $f_w(g) \coloneqq \tau(g)w$ if $g \in H$ and $f_w(g) = 0$ if $g \in G \setminus H$. Clearly, this is a $\mathbb{C}[H]$-module embedding. The image of W in V consists of all the functions $f \in V$ that vanish on $G \setminus H$.

Let now $G = \bigsqcup_{r \in R} rH$ be a decomposition of G into left classes modulo H. For every $f \in V$ and for every $r \in R$, we define a function $f_r \in V$ by $f_r(g) \coloneqq f(g)$ if $g \in Hr^{-1}$ and $f_r(g) = 0$ otherwise. Then $r^{-1} f_r$ belongs go W (after identifying W with its image in V), and

$$f = \sum_{r \in R} r \left(r^{-1} f_r \right).$$

Thus, V is isomorphic to $\bigoplus_{r \in R} rW$. In particular, we have that $\dim V = [G : H] \dim W$.

Using this isomorphism, one obtains also a canonical isomorphism $V \cong \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$, where G operates on the right-hand side by multiplication on the left of the first factor. This form of the induced representation is convenient to prove the following fundamental properties.

(a) Transitivity: If J is a subgroup of H and $\tau \colon J \to \operatorname{Aut} U$ is a representation of J, then

$$\operatorname{Ind}_J^G U = \operatorname{Ind}_H^G \left(\operatorname{Ind}_J^H U \right).$$

(b) Frobenius reciprocity theorem: With the above notation, let E be a $\mathbb{C}[G]$-module, and denote by $\operatorname{Res}_H^G E$ the $\mathbb{C}[H]$-module obtained from E by considering only the action of H. Then we have the following canonical isomorphism:

$$\operatorname{Hom}_{\mathbb{C}[G]} \left(\operatorname{Ind}_H^G W, E \right) \cong \operatorname{Hom}_{\mathbb{C}[H]} \left(W, \operatorname{Res}_H^G E \right).$$

In particular,

$$\dim \operatorname{Hom}_{\mathbb{C}[G]} \left(\operatorname{Ind}_H^G W, E \right) = \dim \operatorname{Hom}_{\mathbb{C}[H]} \left(W, \operatorname{Res}_H^G E \right).$$

If τ and σ are representations of H and G that correspond to W and E, respectively, then the last equality can be rewritten, in the notation of Section 1.1, as

$$\left(\operatorname{Ind}_H^G \tau, \sigma \right)_G = \left(\tau, \operatorname{Res}_H^G \sigma \right)_H.$$

In particular, if both τ and σ are irreducible, then the multiplicity of σ in $\operatorname{Ind}_H^G \tau$ is equal to the multiplicity of τ in $\operatorname{Res}_H^G \sigma$.

Finally, if τ is a representation of a subgroup H of a group G, and $\sigma = \operatorname{Ind}_H^G \tau$, then χ_ρ can be calculated from χ_τ by the following formula

$$\chi_\rho(g) = \frac{1}{|H|} \sum_{r \in G} \widetilde{\chi}_\tau \left(sgs^{-1} \right) = \sum) r \in R \widetilde{\chi}_\tau \left(rgr^{-1} \right),$$

where $\widetilde{\chi}_\tau$ is the function on G that vanishes outside H and coincides with χ_τ on H; R is a system of representatives of right classes of G modulo H.

1.3 The Schur algebra

Proposition 1.1. Let H and J be subgroups of a finite group G. Let ρ and σ be representations of H and J, respectively. Then $\mathrm{Hom}_{\mathbb{C}[G]}\left(\mathrm{Ind}_H^G V_\rho, \mathrm{Ind}_J^G V_\sigma\right)$ is isomorphic to the vector space of all functions $F\colon G \to \mathrm{Hom}_{\mathbb{C}}(V_\rho, V_\sigma)$ satisfying

$$F(jgh) = \sigma(j) \circ F(g) \circ \rho(h) \tag{1.2}$$

for all $j \in J$, $g \in G$, and $h \in H$.

Proof. Let $\widehat{\rho} \coloneqq \mathrm{Ind}_H^G \rho$, $\widehat{\sigma} \coloneqq \mathrm{Ind}_J^G \sigma$, and $n \coloneqq [G : H]$. Denote by F' the vector space of all functions

$$\varphi\colon G \times G \to \mathrm{Hom}_{\mathbb{C}}(V_\rho, V_\sigma)$$

that satisfy

$$\varphi(jg_q, hg_2) = \sigma(j) \circ \varphi(g_1, g_2) \circ \rho(h)^{-1} \tag{1.3}$$

for all $j \in J$, $h \in H$, and $g_1, g_2 \in G$. For every $\varphi \in F'$, we define an element $T_\varphi \in \mathrm{Hom}_{\mathbb{C}}(V_{\widehat{\rho}}, V_{\widehat{\sigma}})$ as follows: If $f \in V_{\widehat{\rho}}$, then $T_\varphi f\colon G \to V_\sigma$ is the map defined

$$(T_\varphi f)(g) \coloneqq \frac{1}{n} \sum_{r \in G} \varphi(g, r)(f(r)); \tag{1.4}$$

clearly, the map $\varphi \mapsto T_\varphi$ is a homomorphism $F' \to \mathrm{Hom}_{\mathbb{C}}(V_{\widehat{\rho}}, V_{\widehat{\sigma}})$. It is injective. Indeed, suppose that $T_\varphi = 0$. Let $s \in G$, let $v \in V_\rho$, and define a function $f_{sb} \in V_{\widehat{\rho}}$ by

$$f_{sv}(g) \coloneqq \begin{cases} \rho(h)v & \text{if } g = hs, \\ 0 & \text{if } g \notin Hs. \end{cases}$$

Then substituting $f = f_{sv}$ in (1.4) we have by (1.3) that $\varphi(g, s)v = 0$. Hence, $\varphi(g, s) = 0$; i.e., $\varphi = 0$.

The dimension of F' is equal to $[G : H][G : J](\dim \rho)(\dim \sigma)$ by (1.3). This is also the dimension of $\mathrm{Hom}_{\mathbb{C}}(V_{\widehat{\rho}}, V_{\widehat{\sigma}})$. Hence, T is an isomorphism.

Denote now by F'_G the subspace of all $\varphi \in F'$ such that $T_\varphi \in \mathrm{Hom}_{\mathbb{C}[G]}(V_{\widehat{\rho}}, V_{\widehat{\sigma}})$. Clearly $\varphi \in F'_G$ if and only if

$$\sum_{r \in G} \varphi\left(g, rx^{-1}\right)(f(r)) = \sum_{r \in G} \varphi(gx, r)(f(r)) \tag{1.5}$$

for all $f \in V_{\widehat{\rho}}$ and $x \in G$. Substituting $f = f_{sv}$ in (1.5), we have that (1.5) is equivalent to the condition

$$\varphi\left(g, rx^{-1}\right) = \varphi(gx, r) \qquad \text{for all } g, r, x \in G. \tag{1.6}$$

For every function $F\colon\ \mathrm{Hom}_{\mathbb{C}}(V_\rho, V_\sigma)$ that satisfies (1.2), we define a function $\varphi\colon G \times G \to \mathrm{Hom}_{\mathbb{C}}(V_\rho, V_\sigma)$ by

$$\varphi(g_1, g_2) \coloneqq F\left(g_1 g_2^{-1}\right). \tag{1.7}$$

Then φ satisfies (1.6), and thus it belongs to F'_G. Conversely, starting from φ in F'_G, we define an $F\colon G \to \mathrm{Hom}_{\mathbb{C}}(V_\rho, V_\sigma)$ by

$$F(g) \coloneqq \varphi(g, 1).$$

Then F satisfies (1.2), and the φ defined by (1.7) coincides with the one we started with. Thus, F is isomorphic to F'_G.

For every $F \in F$, denote by T_F the element of $\mathrm{Hom}_{\mathbb{C}[G]}(V_{\widehat{\rho}}, V_{\widehat{\sigma}})$ defined by

$$(T_F f)(g) \coloneqq \frac{1}{n} \sum_{r \in G} F\left(gr^{-1}\right)(f(r)). \tag{1.8}$$

Then the map $F \mapsto T_F$ is the desired isomorphism. ∎

Corollary 1.2. In the notation of Proposition 1.1, we have

$$\left(\mathrm{Ind}_H^G, \mathrm{Ind}_J^G \sigma\right) \leq |J\backslash G/H|(\dim \rho)(\dim \sigma)$$

where $J\backslash G/H$ denotes the set of double classes of G modulo J and H.

The most interesting conclusion of Proposition 1.1 arises in the special case where $H = J$ and $\rho = \sigma$. In this case $\mathrm{Hom}_{\mathbb{C}[G]}\left(\mathrm{Ind}_H^G V_\rho, \mathrm{Ind}_J^G V_\sigma\right) = \mathrm{End}_{\mathbb{C}[G]}(V_{\widehat{\rho}})$, the Schur algebra of $\widehat{\rho}$. The bijection between F and this algebra established in Proposition 1.1 turns F into an algebra and the product between two elements F_1 and F_2 of F is given by

$$(F_1 * F_2)(g) \coloneqq \frac{1}{[G:H]} \sum_{s \in G} F_1\left(gs^{-1}\right) F_2(s). \tag{1.9}$$

This can be easily verified from the basic relation $T_{F_1} T_{F_2} = T_{F_1 * F_2}$ and the definition (1.8).

1.4 The group $\mathrm{GL}(2, K)$

In this section, we fix our notation for the rest of these notes.

Let K be a finite field with q elements and suppose $q > 2$. We denote by G the group $\mathrm{GL}(2, K)$ of all 2×2 invertible matrices with entries in K. We further reserve some letters for distinguished subgroups of G that will concern us in the sequel. The letter B stands for the *Borel* subgroup of G consisting of all upper triangular matrices

$$B \coloneqq \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix} : \alpha, \delta \in K^\times, \beta \in K \right\}.$$

Clearly $|B| = (q-1)^2 q$. Straightforward calculations show that the matrix $w \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, together with the matrices $\begin{bmatrix} 1 & 0 \\ \gamma & 1 \end{bmatrix}$, $\gamma \in K$, form a system of representatives for the left (and also for the right) classes of G modulo B. Hence, $[G : B] = q + 1$ and thus $|G| = (q-1)^2 q(q+1)$. The idempotent matrix w will play an important role in the sequel.

Note B is a solvable group. Indeed, B contains the normal abelian subgroup

$$U \coloneqq \left\{ \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} : \beta \in K \right\}$$

of all unipotent upper-triangular matrices. This group is isomorphic to the additive group K^+ of the field K. Indeed,

$$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \beta' \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \beta + \beta' \\ 0 & 1 \end{bmatrix}.$$

We shall therefore sometimes identify an element β of K with the corresponding matrix of U. The quotient group B/U is isomorphic to the *Cartan* group

$$D \coloneqq \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix} : \alpha, \delta \in K^\times \right\}$$

of all diagonal matrices. It is isomorphic to $K^\times \times K^\times$ and hence is abelian. Clearly, $U \cap D = 1$ and $UD = B$. Hence, B is the semi-direct product of U by D. Simple calculation shows that U is the commutator subgroup of B. (Here we are using the assumption $q > 2$. In the case $q = 2$, we have $B = U$ and $B^c = 1$.) In particular, it follows that B has exactly $(q-1)^2$ characters.

Another important normal subgroup of B is

$$P \coloneqq \left\{ \begin{bmatrix} \alpha & \beta \\ 0 & 1 \end{bmatrix} : \alpha \in K^\times, \beta \in K \right\}$$

of order $(q-1)q$ and of index $q-1$ in B. The center

$$Z := \left\{ \begin{bmatrix} \delta & 0 \\ 0 & \delta \end{bmatrix} : \delta \in K^{\times} \right\}$$

of G is also contained in B. Clearly $Z \cap P = 1$ and $ZP = B$; i.e., B is the semi-direct product of Z and P.

Note that U is contained in P. In fact, U is also the commutator subgroup of P. A complement of U in P is the group

$$A := \left\{ \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} : \alpha \in K^{\times} \right\},$$

which is canonically isomorphic to $K^{\times}$. Thus, P is the semi-direct product of U by A. The action of A on U by conjugation corresponds to the action of $K^{\times}$ on K^{+} by multiplication

$$\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha\beta \\ 0 & 1 \end{bmatrix}.$$

Our method of constructing the representations of G consists of three stages: First of all we use general principles and easily determine the representations of P. Then we make a jump to B and induce characters from B to G. The last and most difficult stage is to explore those representations of G that do not appear in the former stage. In doing this we shall use the *Bruhat decomposition* of G, namely $G = B \sqcup BwU$. Indeed, if $\gamma \neq 0$, then

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \beta - \alpha\gamma^{-1}\delta & \alpha \\ 0 & \gamma \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & \gamma^{-1}\delta \\ 0 & 1 \end{bmatrix}.$$

1.5 The conjugacy classes of $\mathrm{GL}(2,K)$

Before we start to investigate the irreducible representations of G, we would like to compute their number. It is equal to the number of the conjugacy classes of G. The computation of this number will be done by explicitly giving a representative for each of the conjugacy classes. This will also help us later to give the *character table* of G, i.e., the values of the irreducible higher-dimensional characters at the conjugacy classes.

An element g of G has two eigenvalues. If one of them belongs to K, then so does the other, since they both the same quadratic equation, $\deg(g - XI) = 0$ over K. All the elements in the conjugacy class of G have the same eigenvalues. There are therefore two possibilities.

(a) The eigenvalues of g belong to K.

In this case, g is conjugate over K to a unique matrix in a canonical Jordan form. If both eigenvalues are equal to the same element α of K, then the Jordan form is

$$c_1(\alpha) := \begin{bmatrix} \alpha & 0 \\ 0 & \alpha \end{bmatrix} \qquad \text{or} \qquad c_2(\alpha) := \begin{cases} \alpha & 1 \\ 0 & \alpha \end{cases},$$

depending on whether the minimal polynomial of g is different from the characteristic polynomial or equal to it. If the eigenvalues are α, β and $\alpha \neq \beta$, then the Jordan form is

$$c_3(\alpha, \beta) := \begin{cases} \alpha & 0 \\ 0 & \beta \end{cases}.$$

There are $q-1$ matrices of the form $c_1(\alpha)$, $q-1$ of the form $c_2(\alpha)$, and $\frac{1}{2}(q-1)(q-2)$ of the form $c_3(\alpha, \beta)$.

(b) The eigenvalues of g do not belong to K.

In this case, they belong the unique quadratic extension L of K. Denote by $p(X)$ the characteristic polynomial of g. Then $p(X)$ is irreducible over K, and its roots $\alpha, \overline{\alpha}$, which are the eigenvalues of g, are conjugate over K. They are distinct, since K as a finite field is perfect. If we denote $\mathrm{Tr}(\alpha) := \alpha + \overline{\alpha}$ and $\mathrm{N}(\alpha) := \alpha\overline{\alpha}$, then $p(X) = X^2 - \mathrm{Tr}(\alpha)X + \mathrm{N}(\alpha)$.

Let v be a nonzero vector in K^2. Then v, gv form a basis for K^2 over K, since otherwise there would exist a $\lambda \in K$ such that $gv = \lambda v$. This λ would then be an eigenvalue, contrary to our hypothesis. Recalling that $p(g) = 0$ (by the Cayley–Hamilton theorem), we have that the matrix of g, when considered as a linear operator on K^2 with respect to the basis v, gv is

$$c_4(\alpha) := \begin{bmatrix} 0 & -\mathrm{N}(\alpha) \\ 1 & \mathrm{Tr}(\alpha) \end{bmatrix}.$$

Thus, g is conjugate in G to $c_4(\alpha)$.

Conversely, given an $\alpha \in L \setminus K$, then $c_4(\alpha)$ is a matrix in G with the eigenvalues $\alpha, \overline{\alpha}$. If β is an additional element of $L \setminus K$, then $c_4(\alpha)$ is conjugate to $c_4(\beta)$ if and only if $\beta = \alpha$ or $\beta = \overline{\alpha}$, since then $p(\beta) = 0$.

There are $q^2 - q$ elements in $L \setminus K$. Hence, there are $\frac{1}{2}\left(q^2 - q\right)$ matrices of the form $c_4(\alpha)$.

We sum up our results in the following.

Proposition 1.3. The conjugacy classes of G are classified in four families.

(a) $q - 1$ classes, represented by $c_1(\alpha)$, with equal eigenvalues in K such that the characteristic polynomial is different from the minimal polynomial;

(b) $q - 1$ classes, represented by $c_2(\alpha)$, with equal eigenvalues in K such that the characteristic polynomial is equal to the minimal polynomial;

(c) $\frac{1}{2}(q-1)(q-2)$ classes, represented by $c_3(\alpha, \beta)$, with distinct eigenvalues in K;

(d) $\frac{1}{2}\left(q^2 - q\right)$ classes, represented by $c_4(\alpha)$, with eigenvalues in $L \setminus K$.

Theme 2
The Representations of $\mathrm{GL}(2, K)$

This chapter starts with the representations of P, then investigates the behavior of representations of G that are induced from characters of B, and finally describes the cuspidal representations of G, i.e., those representations that do not appear as components of the induced ones. The chapter ends with Weil's reciprocity law.

2.1 The representations of P

We use the method of "small groups" of Wigner in order to determine the representations of P.

First, we fix for the rest of these notes a non-unit character ψ of K^+. We consider it also as a character of U. For every $a \in A$, we define a character ψ_a of U by

$$\psi_a(u) := \psi\left(aua^{-1}\right), \qquad \text{for } u \in U. \tag{2.1}$$

If $a \neq a'$, then $\psi_a \neq \psi_{a'}$. Indeed, if

$$a := \begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix}, \qquad a' := \begin{bmatrix} \alpha' & 0 \\ 0 & 1 \end{bmatrix}, \qquad \text{and} \qquad u := \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix},$$

then $\psi_a(u) = \psi(\alpha\beta)$, and $\psi_a = \psi_{a'}$ implies that $\psi((\alpha - \alpha')\beta) = 0$ for all $\beta \in K$; hence $\alpha = \alpha'$; hence $a = a'$. We thus get $q - 1$ distinct representatives of U. These, together with the unit representation of U, are all the characters of U since $|U| = q$.

Every character χ of A can be lifted to a character $\widetilde{\chi}$ of P defined by $\widetilde{\chi}(ua) := \chi(a)$. The $q - 1$ distinct characters $\widetilde{\chi}$ of P obtained in this way are all the characters of P since $[P : P^c] = [P : U] = q - 1$.

In order to find the higher-dimensional representations of P, we induce ψ from U to P and claim

$$\mathrm{Res}_U^P \mathrm{Ind}_U^P \psi \stackrel{?}{=} \bigoplus_{a \in A} \psi_a. \tag{2.2}$$

Indeed, for every $a \in A$, we define a function $f_a \in \mathrm{Ind}_U^P V_\psi$ by

$$f_a(a') := \begin{cases} 1 & \text{if } a = a', \\ 0 & \text{if } a \neq a', \end{cases} \qquad \text{where } a' \in A.$$

Then f_a is an eigenvector of U that belongs to the eigenvalue ψ_a. In order to prove this claim, we have to show that $f_a(pu) = \psi_a(u) f_a(p)$ for every $p \in P$ and every $u \in U$. Writing $p = u'a'$ with $u' \in U$ and $a' \in A$ and using the identity $f_a(u'p') = \psi(u')f_a(p')$ for $p' \in P$, we see that it suffices to show that

$$f_a(a'u) \stackrel{?}{=} \psi_a(u) f_a(a'). \tag{2.3}$$

Indeed,

$$f_a(a'u) = f_a\left(a'u(a')^{-1}a'\right) = \psi\left(a'u(a')^{-1}\right) f_a(a') = \psi_{a'}(u) f_a(a').$$

The right-hand side is equal to zero if $a \neq a'$ and equal to $\psi_a(u)f_a(a')$ if $a = a'$; hence, (2.3) is true in both cases. Thus, the vector f_a generates the one-dimensional space V_{ψ_a}.

If we let a vary, we get $q-1$ linearly independent vectors f_a of the $(q-1)$-dimensional vector space $\operatorname{Ind}_U^P V_\psi$. Hence, $\operatorname{Res}_U^P \operatorname{Ind}_U^P V_\psi = \bigoplus_{a\in A} V_{\psi_a}$ as U-modules. This proves (2.2).

As a consequence of (2.2), we prove the following fundamental theorem.

Theorem 2.1. The group P has q irreducible representations.

(a) $(q-1)$ of them are one-dimensional; they are the lifting of the characters of A;

(b) one $(q-1)$-dimensional representation which is $\pi := \operatorname{Ind}_U^P \psi$.

Proof. We only have to prove (b). First, note that $\dim \operatorname{Ind}_U^P \psi = [P : U] = q-1$. Second, by the Frobenius reciprocity theorem and by (2.2),

$$\left(\operatorname{Ind}_U^P \psi, \operatorname{Ind}_U^P \psi\right)_P = \left(\psi, \bigoplus_{a\in A} \psi_a\right) = 1;$$

hence $\operatorname{Ind}_U^P \psi$ is an irreducible character of P.

In order to prove that there is no additional representation of P, one can observe that

$$\sum_{a\in A} (\dim \psi_a)^2 + \left(\dim \operatorname{Ind}_U^P \psi\right)^2 = (q-1) + (q-1)^2 = |P|.$$

We would however also like to prove the last assertion without using the finiteness of G. In order to do this, note first that one can in fact replace ψ in (2.2) by $\psi_{a'}$ and have

$$\operatorname{Res}_U^P \operatorname{Ind}_U^P \psi_{a'} = \bigoplus_{a\in A} \psi_a. \tag{2.4}$$

Hence, we can prove, as before, that $\operatorname{Ind}_U^P \psi_{a'}$ is an irreducible representation of P. Further, by (2.4),

$$\left(\operatorname{Ind}_U^P \psi, \operatorname{Ind}_U^P \psi_{a'}\right) = \left(\psi, \bigoplus_{a\in A} \psi_a\right) = 1.$$

Hence,

$$\operatorname{Ind}_U^P \psi = \operatorname{Ind}_U^P \psi_{a'}. \tag{2.5}$$

Now, let σ be an arbitrary irreducible representation of P and consider $\operatorname{Res}_U^P \sigma$. If there exists an $a' \in A$ such that $\psi_{a'}$ appears in $\operatorname{Res}_U^P \sigma$, then by (2.5),

$$\left(\sigma, \operatorname{Ind}_U^P\right) = \left(\operatorname{Res}_U^P \sigma, \psi_{a'}\right) > 0.$$

Hence, $\sigma = \operatorname{Ind}_U^P \psi$ because both representations are irreducible. Otherwise, $\operatorname{Res}_U^P \sigma$ is a multiple of the unit character of U; i.e., $\sigma(u)v = v$ for every $v \in V_\sigma$. Consider therefore $\operatorname{Res}_A^P V_\sigma$. It decomposes into linear A-subspaces because A is abelian. In particular, there exists a nonzero vector $v \in V_\sigma$ and a character of A, say χ, such that $\sigma(a)v = \chi(a)v$ for every $a \in A$. Hence, if $u \in U$, then $\sigma(au)v = \chi(a)v$. It follows that $\sigma = \widetilde{\chi}$. ∎

Remark 2.2. Note that we have also proved that our description of the representations of P is independent of the choice of ψ.

Remark 2.3. The distinguished representation $\pi = \operatorname{Ind}_U^P \psi$ will play an important rule in the sequel. This is the reason for reserving the letter π for it.

2.2 The representations of B

We have already that the commutator of B is U (see section 1.4). Moreover, B is the semi-direct product of D and U. The group D is canonically isomorphic to $K^\times \times K^\times$. Hence, every pair (μ_1, μ_2) of characters of $K^\times$ defines a unique character μ of B which is given by the formula

$$\mu\left(\begin{bmatrix}\alpha & \beta \\ 0 & \delta\end{bmatrix}\right) := \mu_1(\alpha)\mu_2(\beta), \qquad \alpha, \delta \in K^\times. \tag{2.6}$$

Conversely, to every character μ of B, there corresponds a pair of characters (μ_1, μ_2) of $K^\times$ such that (2.6) holds. Thus, the $(q-1)^2$ characters of B given by (2.6) are all the characters of B.

An easy computation shows that the normalizer of D in G is generated by D and w.[1] Indeed, we have

$$w\begin{bmatrix}\alpha & 0 \\ 0 & \delta\end{bmatrix}w^{-1} = \begin{bmatrix}\delta & 0 \\ 0 & \alpha\end{bmatrix}.$$

For every character μ of B given by (2.6), we define a character μ_w of B by

$$\mu_w\left(\begin{bmatrix}\alpha & \beta \\ 0 & \delta\end{bmatrix}\right) := \mu_2(\delta)\mu_2(\alpha).$$

Then $\mu_w(d) = \mu\left(wdw^{-1}\right)$ for every $d \in D$, and

$$\mu_w = \mu \iff \mu_1 = \mu_2.$$

In order to find the higher-dimensional representations of B, recall that B is also the semi-direct product of Z by P. The abelian group Z has $q-1$ characters χ. Each of them can be extended to a character $\widetilde{\chi}$ of B by

$$\widetilde{\chi}(zp) := \chi(z) \qquad \text{for } z \in Z, p \in P.$$

Also, composing the canonical map $B \to P$ with kernel Z, with the representation π of B (see Theorem 2.1), we get an irreducible representation $\widetilde{\pi}$ of B of dimension $q-1$:

$$\widetilde{\pi}(zp) := \pi(p) \qquad \text{for } z \in Z, p \in P.$$

The tensor product

$$(\widetilde{\chi} \otimes \widetilde{\pi})(zp) := \chi(z)\pi(p), \qquad \text{for } z \in Z, p \in P \tag{2.7}$$

is an irreducible $(q-1)$-dimensional representation of B whose restriction to Z is χ. Varying χ on all characters of Z, we get $q-1$ different $(q-1)$-dimensional representations of B. These, together with the $(q-1)^2$ characters of B, are all the irreducible representations of B because

$$(q-1)^2 + (q-1)(q-1)^2 = q(q-1)^2 = |B|.$$

We have therefore proved the following theorem.

Theorem 2.4. The group B has the following irreducible representations.

(a) $(q-1)^2$ characters by (2.6).

(b) $(q-1)$ different $(q-1)$-dimensional representations given by (2.7).

[1] This needs $q > 2$.

2.3 Inducing characters from B to G

2.4 The Schur algebra of $\mathrm{Ind}_B^G \mu$

2.5 The dimension of cuspidal representations

2.6 The description of $\mathrm{GL}(2, K)$ by generators and relations

2.7 Non-decomposable characters of $L^\times$

2.8 Assigning cuspidal representations to non-decomposable characters

2.9 The correspondence between ν and P_ν

2.10 The small Weil group and the small reciprocity law

THEME 3

Γ-FUNCTIONS AND BESSEL FUNCTIONS

Appendix A
Review of Representation Theory

In this appendix, we review the representation theory of finite groups used throughout this book. As such, throughout this section, G is a finite group, and we will only consider finite-dimensional representations in $\mathbb{C}$.

A.1 Basic Constructions

Let's start at the beginning.

Definition A.1 (representation)**.** Fix a group G. Then a (finite-dimensional) G-*representation* (over $\mathbb{C}$) is a finite-dimensional $\mathbb{C}$-vector space V equipped with a homomorphism $\rho\colon G \to \operatorname{Aut}(V)$. We occasionally call ρ itself the representation and write V_ρ to denote the "underlying" vector space.

Remark A.2. Fix a group G. Then a G-representation (over $\mathbb{C}$) has equivalent data to a $\mathbb{C}[G]$-module. On one hand, a $\mathbb{C}[G]$-module V is a $\mathbb{C}$-module (i.e., a $\mathbb{C}$-vector space), and it comes with a G-action from the module structure. On the other hand, a G-representation $\rho\colon G \to \operatorname{Aut}(V)$ extends the $\mathbb{C}$-action $\mathbb{C} \to \operatorname{End}(V)$ to a ring morphism $\mathbb{C}[G] \to \operatorname{End}(V)$.

Example A.3. The above remark has also told that any group G has the "regular representation" given by $\mathbb{C}[G]$.

This module-theoretic perspective tells us that we should define morphisms of representations (called "G-invariant") to be morphisms of $\mathbb{C}[G]$-modules so that the category of G-representations (over $\mathbb{C}$) is simply $\operatorname{Mod}_{\mathbb{C}[G]}$. This tells us that our category is abelian, so we may define subobjects (called "suprepresentations" or "invariant subspaces"), quotients (called "quotient representations"), direct sums, and tensor products in $\operatorname{Mod}_{\mathbb{C}[G]}$.

Example A.4. For any G-representation ρ, the G-invariants

$$V_\rho^G \coloneqq \{v \in V_\rho : \rho(g)v = v \text{ for all } g \in G\}$$

is a G-invariant subspace. Indeed, we can see directly that it is G-invariant, and it is the intersection of the kernels $\ker(\mathrm{id}_V - \rho(g))$ over all $g \in G$, so it is a subspace.

Definition A.5 (regular representation)**.** Fix a group G. Because $\mathbb{C}[G]$ is itself a $\mathbb{C}[G]$-module, we see that $\mathbb{C}[G]$ is a G-representation. It is called the *regular representation*.

Another perspective is that representation theory is linear algebra with some extra bells and whistles, so we attach many definitions from linear algebra to our representations. For example, the dimension of a G-representation ρ is

$$\dim \rho := \dim V_\rho.$$

Remark A.6. A quick benefit of a linear algebra perspective is that, for any G-representation ρ, the operator $\rho(g)$ is diagonalizable for any $g \in G$. Indeed, G is finite, so g and hence $\rho(g)$ has finite order. It thus follows that $\rho(g)$ is diagonalizable. To see this, it is enough to show that any vector in $V := V_\rho$ is a sum of eigenvectors of the operator $\varphi := \rho(g)$. Let n be the operator of φ. Then the minimal polynomial of φ is $x^n - 1$, which has no repeated roots when factored over $\mathbb{C}$, so φ is diagonalizable.

However, in contrast to both linear algebra and modules, we use the special structure to give Hom and $\otimes$ a special structure.

Definition A.7. Fix G-representations ρ and ρ'. Then $\operatorname{Hom}_{\mathbb{C}}(V_\rho, V_{\rho'})$ has the structure of G-representation by defining

$$g\varphi := \rho'(g) \circ \varphi \circ \rho(g)^{-1}.$$

One can check directly that this provides $\mathbb{C}[G]$-module structure. As a special case, we define the dual as $\rho^\vee := \operatorname{Hom}_{\mathbb{C}}(V_\rho, \mathbb{C})$.

Remark A.8. Let's explain the above definition. In the context of the previous definition, we claim that $\operatorname{Hom}_{\mathbb{C}}(V_\rho, V_{\rho'})^G = \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'})$. Indeed, $\varphi\colon V_\rho \to V_{\rho'}$ is fixed by $g \in G$ if and only if

$$\rho(g) \circ \varphi \circ \rho'(g)^{-1} = \varphi$$

for all $g \in G$, which rearranges to $\rho(g) \circ \varphi = \varphi \circ \rho'(g)$.

Definition A.9. Fix G-representations ρ and ρ'. Then $V_\rho \otimes_{\mathbb{C}} V_{\rho'}$ has the structure of G-representation by defining

$$g(v \otimes v') := gv \otimes gv'.$$

One can check directly that this provides $\mathbb{C}[G]$-module structure.

Here is a quick sanity check that our definitions have been set up correctly.

Lemma A.10. Fix G-representations ρ and ρ'. Then $\operatorname{Hom}_{\mathbb{C}}(V_\rho, V_{\rho'}) \cong V_\rho^\vee \otimes_{\mathbb{C}} V_{\rho'}$.

Proof. There is a natural map

$$\eta\colon V_\rho^\vee \otimes_{\mathbb{C}} V_{\rho'} \to \operatorname{Hom}_{\mathbb{C}}(V_\rho, V_{\rho'})$$

by extending $\eta(\varphi \otimes v')\colon v \mapsto \varphi(v)v'$; further, η is G-linear because

$$\begin{aligned}
(g\eta(\varphi \otimes v'))(v) &= \rho'(g) \circ \eta(\varphi \otimes v')\left(\rho(g)^{-1}v\right) \\
&= \rho'(g)\varphi\left(\rho(g)^{-1}v\right)v' \\
&= (g\varphi)(v)(\rho'(g)v') \\
&= \eta(g\varphi \otimes gv')(v).
\end{aligned}$$

It remains to show η is bijective. Well, the domain and codomain of η both have dimension $(\dim\rho)(\dim\rho')$, so it suffices to show η is surjective. As such, fix bases $\{v_1,\ldots,v_n\}$ and $\{v_1',\ldots,v_{n'}'\}$ of V and V', respectively. For any linear map $\psi\colon V_\rho\to V_{\rho'}$, we let $\{a_{ii'}\}_{i,i'}$ be the associated matrix. Then we define $\varphi_i\colon V_\rho\to\mathbb{C}$ by extending $v_j\mapsto 1_{i=j}$ linearly, and we see

$$\psi(v_i)=\sum_{j'=1}^{n'}a_{ij'}v_{j'}=\sum_{j'=1}^{n}a_{ij'}\varphi_i(v_i)v_{j'}=\sum_{j=1}^{n}\sum_{j'=1}^{n}a_{jj'}\varphi_j(v_i)v_{j'}$$

for each v_i. Thus, we see

$$\psi=\eta\left(\sum_{j=1}^{n}\sum_{j'=1}^{n}\varphi_j\otimes a_{jj'}v_{j'}\right),$$

finishing. ■

A.2 Decomposing Representations

We are going to decompose representations into irreducible ones.

Definition A.11 (irreducible)**.** A G-representation ρ is *irreducible* if and only if it is nonzero and has no nonzero proper subrepresentations.

We are going to want to decompose general representations into irreducible ones. It will be productive to discuss inner products.

Definition A.12 (unitary)**.** A G-representation ρ is *unitary* for a Hermitian inner product $\langle\cdot,\cdot\rangle$ on V_ρ if and only if

$$\langle gv,gw\rangle=\langle v,w\rangle$$

for any $v,w\in V_\rho$.

It is a remarkable fact that we can think about any given representation as being unitary.

Proposition A.13 (Weyl)**.** Let G be a finite group. For any representation ρ, there exists a Hermitian inner product $\langle\cdot,\cdot\rangle$ on V_ρ for which ρ is unitary.

Proof. Because V_ρ is a finite-dimensional $\mathbb{C}$-vector space, we can choose a basis of V to yield an isomorphism $V_\rho\cong\mathbb{C}^n$ where $n=\dim\rho$. Then we can certainly give V_ρ some inner product $\langle\cdot,\cdot\rangle_0$ in the form of the usual one on $\mathbb{C}^n$. To fix the G-invariance of this inner product, we define

$$\langle v,w\rangle:=\frac{1}{\#G}\sum_{g\in G}\langle\rho(g)v,\rho(g)w\rangle_0.$$

A linear combination of Hermitian inner products remains conjugate-symmetric, bilinear, and positive, so $\langle\cdot,\cdot\rangle$ is conjugate-symmetric, bilinear, and positive. In fact, we can also see that $\langle\cdot,\cdot\rangle$ is non-degenerate: if $\langle v,w\rangle=0$, then we must have $\langle\rho(g)v,\rho(g)w\rangle_0=0$ for each $g\in G$, so $v=w$ follows by setting g to be the identity. Lastly, we see that $\langle\cdot,\cdot\rangle$ makes ρ unitary because

$$\langle\rho(g')v,\rho(g')w\rangle=\frac{1}{\#G}\sum_{g\in G}\langle\rho(gg')v,\rho(gg')w\rangle_0=\frac{1}{\#G}\sum_{g\in G}\langle\rho(g)v,\rho(g)w\rangle_0=\langle v,w\rangle$$

for any $v,w\in V_\rho$ and $g'\in G$. ■

The following result explains why we care about being unitary.

Lemma A.14. Fix a G-representation ρ unitary for $\langle\cdot,\cdot\rangle$. If $W \subseteq V_\rho$ is a G-invariant subspace, then the orthogonal complement

$$W^\perp := \{v \in V : \langle v, w\rangle = 0 \text{ for all } w \in W\}$$

is also a G-invariant subspace, and $V_\rho \cong W \oplus W^\perp$ as G-representations.

Proof. To see that $W^\perp$ is G-invariant, we note that $v \in W^\perp$ implies that

$$\langle gv, w\rangle = \langle v, g^{-1}w\rangle = 0$$

for any $g \in G$ and $w \in W$; notably, we are using the fact that $g^{-1}w \in W$ as well. To see that $V_\rho \cong W \oplus W^\perp$, we define the map $\varphi\colon W \oplus W^\perp \to V_\rho$ by $\varphi\colon (w, w') \mapsto w + w'$. This map is G-linear, and it describes the usual orthogonal decomposition of a vector space (recall V_ρ is finite-dimensional), so it is an isomorphism of representations. ■

Theorem A.15 (Maschke)**.** Any G-representation ρ is a direct sum of finitely many irreducible representations.

Proof. We induct on $\dim\rho$. If $\dim\rho = 0$, then ρ is the zero representation, which is the direct sum of no irreducible representations. Otherwise, given ρ with $\dim\rho > 0$, we have two cases.

- If ρ is irreducible, then we are done.
- If ρ is not irreducible, then ρ has a nonzero proper G-invariant subspace $W \subsetneq V_\rho$. Then Proposition A.13 combined with Lemma A.14 allows us to decompose ρ as a direct sum of two proper subrepresentations arising from $W, W^\perp \subseteq V_\rho$. Thus, $\dim W, \dim W^\perp < \dim\rho$, so we may induct to finish. ■

Theorem A.15 lets us define the "isotypical decomposition."

Definition A.16 (isotypical decomposition)**.** Fix a G-representation ρ. Let $\rho_1, \ldots, \rho_k$ denote distinct irreducible representations of G. Then the *isotypical decomposition* of ρ consists of the nonnegative integers $n_1, \ldots, n_k$ such that

$$\rho \cong \bigoplus_{i=1}^k \rho_i^{n_i}.$$

Note that we have not yet shown that the isotypical decomposition is unique, only that it exists. This requires a bit more machinery; we will wait until Corollary A.33 to provide a proof.

A.3 Morphisms Between Representations

An advantage to working with "simple" objects is that their morphisms are relatively controlled.

Theorem A.17 (Schur's lemma)**.** Fix an irreducible G-representation ρ. Any G-invariant map $\varphi\colon V_\rho \to V_\rho$ is multiplication by a scalar.

Proof. Note φ is a linear operator on a $\mathbb{C}$-vector space, so it has an eigenvalue λ. Thus, $\ker(\varphi - \lambda\mathrm{id}_V)$ contains a nonzero vector, so it has a nonzero subrepresentation of V_ρ. Because V_ρ is irreducible, it follows that

$$\ker(\varphi - \lambda\mathrm{id}_V) = V_\rho,$$

so $\varphi(v) = \lambda v$ for all $v \in V_\rho$. ■

Theorem A.17 has a number of important corollaries.

Example A.18. Let G be a finite abelian group. We claim that all irreducible representations are one-dimensional. Indeed, for any G-representation ρ, we note that $\rho(g)\colon V_\rho \to V_\rho$ is a G-invariant map because G is abelian: we compute

$$\rho(g)(\rho(g')v) = \rho(gg')v = \rho(g'g)v = \rho(g')(\rho(g)v).$$

Thus, Theorem A.17 implies that $\rho(g)$ must equal a scalar λ_g. In particular, any one-dimensional subspace of V_ρ is a nonzero G-invariant subspace of V_ρ, so if ρ is irreducible, then $\dim V_\rho = 1$ is forced.

Corollary A.19. Fix irreducible G-representations ρ and ρ'. Then

$$\dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) = \begin{cases} 1 & \text{if } V_\rho \cong V_{\rho'}, \\ 0 & \text{else.} \end{cases}$$

Proof. We deal with the two cases separately.

- If $V_\rho \cong V_{\rho'}$, then after fixing such an isomorphism, we are computing

  $$\dim \operatorname{End}_{\mathbb{C}[G]}(V_\rho).$$

  Of course, scalars in $\mathbb{C}$ are morphisms, and these are distinct morphisms because ρ is irreducible and hence nonzero. However, Theorem A.17 tells us that these are the only morphisms, so $\dim \operatorname{End}_{\mathbb{C}[G]}(V_\rho) = \dim \mathbb{C} = 1$.

- If $V_\rho \not\cong V_{\rho'}$, we show $\operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) = 0$. Well, any morphism $\varphi\colon V_\rho \to V_{\rho'}$ is either not injective or not surjective. If φ is not injective, then $\ker\varphi \subseteq V_\rho$ is a nontrivial subrepresentation, so the irreducibility enforces $\ker\varphi = V_\rho$, so $\varphi = 0$.

  On the other hand, if φ is not surjective, then $\operatorname{im}\varphi \subseteq V_{\rho'}$ is a proper subrepresentation, so irreducibility enforces $\operatorname{im}\varphi = 0$, so $\varphi = 0$. ■

For the next corollaries, we want the following lemma. Roughly speaking, the symmetry of the statement in Corollary A.19 in ρ and ρ' can be extended to arbitrary representations, which we will use to great profit.

Lemma A.20. Fix a group G. Let $\rho_1, \ldots, \rho_k$ be irreducible representations, and fix nonnegative integers $n_1, \ldots, n_k$ and $n_1, \ldots, n_k'$. Then any morphism

$$\varphi\colon \bigoplus_{i=1}^k \rho_i^{\oplus n_i} \to \bigoplus_{i=1}^k \rho_i^{\oplus n_i'}$$

is the sum of the induced maps $\rho_i^{\oplus n_i} \to \rho_i^{\oplus n_i'}$. Thus,

$$\operatorname{Hom}_{\mathbb{C}[G]}\left(\bigoplus_{i=1}^k V_{\rho_i}^{\oplus n_i}, \bigoplus_{i=1}^k V_{\rho_i}^{\oplus n_i'}\right) \cong \bigoplus_{i=1}^k \operatorname{Hom}_{\mathbb{C}[G]}\left(V_{\rho_i}^{\oplus n_i}, V_{\rho_i}^{\oplus n_i'}\right).$$

Proof. Composing φ with inclusion and projection, for any indices a and b, we have induced maps

$$V_a^{\oplus n_a} \to \bigoplus_{i=1}^k \rho_i^{\oplus n_i} \xrightarrow{\varphi} \bigoplus_{i=1}^k \rho_i^{\oplus n_i'} \to V_b^{\oplus n_b'}.$$

Call this composite $\varphi_{b,a}$. It follows that we may write

$$\varphi(v_1, \ldots, v_k) = \left(\sum_{i=1}^{k} \varphi_{1,i}(v_i), \ldots, \sum_{i=1}^{k} \varphi_{k,i}(v_i) \right)$$

If $a \neq b$, then any G-invariant map $V_a \to V_b$ must vanish by Corollary A.19, so the above sum actually collapses into

$$\varphi(v_1, \ldots, v_k) = (\varphi_{1,1} v_1, \ldots, \varphi_{k,k} v_k).$$

To show the last sentence, we note that there is a natural map η from the right to left by sending a k-tuple of maps $(\varphi_1, \ldots, \varphi_k)$ to the map

$$\eta(\varphi_1, \ldots, \varphi_k) \colon (v_1, \ldots, v_k) \mapsto (\varphi_1 v_1, \ldots, \varphi_k v_k).$$

A direct computation shows that η is G-linear. Now, η is injective because if $\eta(\varphi_1, \ldots, \varphi_k)$ vanishes, then it must vanish in each coordinate, forcing $(\varphi_1, \ldots, \varphi_k) = (0, \ldots, 0)$. Further, the above proof establishes that η is surjective, so η is an isomorphism. ■

Corollary A.21. Fix a G-representations ρ and ρ' with isotypical decompositions $\rho \cong \bigoplus_{i=1}^{k} \rho_i^{\oplus n_i}$ and $\rho' \cong \bigoplus_{i=1}^{k} \rho_i^{\oplus n_i'}$. Then

$$\dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) = \sum_{i=1}^{k} n_i n_i'.$$

Proof. By Lemma A.20, we see

$$\operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) \cong \operatorname{Hom}_{\mathbb{C}[G]} \left(\bigoplus_{i=1}^{k} V_{\rho_i}^{\oplus n_i}, \bigoplus_{i=1}^{k} V_{\rho_i}^{\oplus n_i'} \right) \cong \bigoplus_{i=1}^{k} \operatorname{Hom}_{\mathbb{C}[G]} \left(V_{\rho_i}^{\oplus n_i}, V_{\rho_i}^{\oplus n_i'} \right).$$

Now, for each i, a morphism $V_{\rho_i}^{\oplus n_i} \to V_{\rho_i}^{\oplus n_i'}$ is an $n_i' \times n_i$ matrix of morphisms $V_{\rho_i} \to V_{\rho_i'}$ by tracking what happens to each coordinate, so we actually have

$$\operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) \cong \bigoplus_{i=1}^{k} \operatorname{Hom}_{\mathbb{C}[G]}(V_{\rho_i}, V_{\rho_i})^{\oplus n_i n_i'}.$$

Taking dimensions and applying Corollary A.19 finishes. ■

Remark A.22. Note that the form $(\cdot, \cdot)$ defined on finite-dimensional G-representations by $(\rho, \rho') := \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'})$ is automatically bilinear with respects to direct sums. (This is because Hom commutes with direct sums and products.) Here are some other properties.

- Corollary A.21 tells us that this form is symmetric.
- If ρ and ρ' are irreducible, then by Corollary A.19, we see (ρ, ρ') is 1 if $\rho \cong \rho'$ and 0 otherwise.
- If ρ has $(\rho, \rho') = 0$ for all ρ', then we claim $\rho = 0$. Indeed, give ρ an isotypical decomposition $\bigoplus_{i=1}^{k} \rho_i^{\oplus n_i}$. But then computing $(\rho, \rho_i) = n_i$ by Corollary A.21 for each i enforces $n_i = 0$ always, so $\rho = 0$.

Corollary A.23. Fix a G-representation ρ with isotypical decomposition $\rho \cong \bigoplus_{i=1}^k \rho_i^{\oplus n_i}$. Then

$$\operatorname{End}_{\mathbb{C}[G]}(V_\rho) \cong \bigoplus_{i=1}^k M_{n_i}(\mathbb{C}),$$

where $M_{n_i}(\mathbb{C})$ is the matrix algebra.

Proof. By Lemma A.20, we note that any G-invariant map $\varphi\colon V_\rho \to V_\rho$ is the sum of maps $\varphi_i\colon V_{\rho_i}^{\oplus n_i} \to V_{\rho_i}^{\oplus n_i}$, so we have an isomorphism

$$\bigoplus_{i=1}^k \operatorname{End}_{\mathbb{C}[G]}\left(V_{\rho_i}^{\oplus n_i}, V_{\rho_i}^{\oplus n_i}\right) \to \operatorname{End}_{\mathbb{C}[G]}(V_\rho)$$

of $\mathbb{C}[G]$-modules. Because this isomorphism merely sends $(\varphi_1, \ldots, \varphi_k)$ to the summed morphisms, we see that it is also compatible with the ring structures on both sides, so this is an isomorphism of $\mathbb{C}[G]$-algebras.

It remains to show $\operatorname{End}_{\mathbb{C}[G]}\left(V_{\rho_i}^{\oplus n_i}, V_{\rho_i}^{\oplus n_i}\right)$ is isomorphic to $M_{n_i}(\mathbb{C})$. Well, we see that any morphism $\varphi\colon V_{\rho_i}^{\oplus n_i} \to V_{\rho_i}^{\oplus n_i}$ can be written as

$$\varphi(v_1, \ldots, v_{n_i}) = \left(\sum_{j=1}^n \varphi_{1j}(v_j), \ldots, \sum_{j=1}^n \varphi_{n_ij}(v_j)\right)$$

where the maps $\varphi_{ab}\colon V_{\rho_i} \to V_{\rho_i}$ are defined by the inclusion to $V_{\rho_i}^{\oplus n_i}$ followed by φ followed by projection. However, Theorem A.17 tells us that each φ_{ab} is a scalar $\lambda_{ab} \in \mathbb{C}$, so the data of the above morphism φ is simply given by the matrix $(\lambda_{ab})_{a,b=1}^{n_i}$. ■

A.4 Characters

One difficulty in understanding representations is that they are inherently multidimensional objects. To fix this, we introduce characters.

Definition A.24 (character)**.** Fix a G-representation ρ. Then the *character* $\chi_\rho\colon G \to \mathbb{C}$ of ρ is defined as $\chi_\rho(g) \coloneqq \operatorname{tr} \rho(g)$.

For example, one can compute the trace by providing V_ρ with any basis and then summing along the diagonal entries of the matrix associated to $\rho(g)$. This construction does not depend on the basis because the trace of a matrix does not change when the basis changes.

Example A.25. Let $\rho\colon G \to \mathbb{C}[G]$ be the regular representation. Then we claim $\chi_\rho(g) = |G|1_{g=e}$. Indeed, note $\mathbb{C}[G]$ has the standard basis $\{h\}_{h\in G}$, and $\rho(g)$ acts by permuting them by left multiplication. Then, for any $g \in G$, the diagonal entry given by $h \in G$ is 1 if $gh = h$ (which is equivalent to $g = e$) and 0 otherwise. So $\chi_\rho(g) = \operatorname{tr} \rho(g) = |G|1_{g=e}$ follows.

Here are some basic properties.

Lemma A.26. Fix a G-representations ρ.

(a) If $\dim \rho = 1$, then $\rho = \chi_\rho$ after identifying V_ρ with $\mathbb{C}$.

(b) χ_ρ is defined up to conjugacy class.

(c) $\chi_\rho(1) = \dim \rho$.

(d) We have
$$\dim V^G = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g).$$

Proof. Here we go.

(a) For any $g \in G$, we note $\rho(g) \colon \mathbb{C} \to \mathbb{C}$ is a morphism of vector spaces, so it is equal to its trace.

(b) For any $g, h \in G$, we compute
$$\chi_\rho\left(ghg^{-1}\right) = \operatorname{tr}\left(\rho(h) \circ \rho(g) \circ \rho(h)^{-1}\right) = \operatorname{tr}\left(\rho(g) \circ \rho(h)^{-1} \circ \rho(g)\right) = \operatorname{tr} \rho(g) = \chi_\rho(g),$$
so $\chi(g)$ is defined up to conjugacy class of g.

(c) Note $\chi_\rho(1) = \operatorname{tr} \rho(1) = \operatorname{tr} \mathrm{id}_{V_\rho}$. This is $\dim V_\rho$ by summing along the diagonal of the identity matrix.

(d) Define the linear map $\pi \colon V \to V$ by
$$\pi := \frac{1}{|G|} \sum_{g \in G} \rho(g).$$
Notably, $\operatorname{tr} \pi = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g)$ by the linearity of tr. We claim that π is a projection onto V^G. We have two checks.

- Note $\pi(v) \in V^G$ for any $v \in V$: indeed, we compute
$$g' \pi(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g'g)v = \frac{1}{|G|} \sum_{g \in G} \rho(g)v = \pi(v)$$
for any $g' \in G$.
- Note $\pi(v) = v$ for any $v \in V^G$: indeed, we compute
$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} \rho(g)v = \frac{1}{|G|} \sum_{g \in G} v = v.$$

It now follows that $\operatorname{tr} \pi = \dim V^G$. To see this concretely, we set $d := \dim V^G$ and $n := \dim \rho$, and we give V a basis by extending a basis $\{v_1, \ldots, v_d\}$ of V^G to a basis $\{v_1, \ldots, v_n\}$ of V. Letting $\{\pi_{ij}\}_{i,j=1}^n$ be the associated matrix, we note that $\pi(v_i) = v_i$ for each $1 \le i \le d$ implies that $\pi_{ii} = 1$ if $1 \le i \le d$; otherwise, for each $i > d$, we see $\pi_{ii} = 0$ because $\pi(v_i) \in V^G$ is a linear combination of the v_j with $1 \le j \le d$, which has no v_i component. Thus, summing along the diagonal confirms $\operatorname{tr} \pi = \dim V^G$. ■

We can also describe how characters behave with our other constructions.

Lemma A.27. Fix G-representations ρ and ρ'.

(a) $\chi_{\rho \oplus \rho'} = \chi_\rho + \chi_{\rho'}$.

(b) $\chi_{\rho \otimes \rho'} = \chi_\rho \cdot \chi_{\rho'}$.

(c) $\chi_{\rho^\vee}(g) = \chi_\rho\left(g^{-1}\right)$ for any g.

Proof. Here we go.

(a) For any $g \in G$, we compute

$$\chi_{\rho\oplus\rho'}(g) = \operatorname{tr}(\rho(g) \oplus \rho'(g)) \stackrel{*}{=} \operatorname{tr}\rho(g) + \operatorname{tr}\rho'(g) = \chi_\rho(g) + \chi_{\rho'}(g).$$

To see $\stackrel{*}{=}$ concretely, we note that we can give the underlying vector space $V_\rho \oplus V_{\rho'}$ a basis by concatenating the bases of V_ρ and $V_{\rho'}$, upon which the matrix associated to $\rho(g) \oplus \rho'(g)$ looks like

$$\begin{bmatrix} \rho(g) & 0 \\ 0 & \rho'(g) \end{bmatrix},$$

whose trace is the sum of the traces of $\rho(g)$ and $\rho'(g)$.

(b) For any $g \in G$, we compute

$$\chi_{\rho\otimes\rho'}(g) = \operatorname{tr}(\rho(g) \otimes \rho'(g)) \stackrel{*}{=} \operatorname{tr}\rho(g) \cdot \operatorname{tr}\rho'(g) = \chi_\rho(g) \cdot \chi_{\rho'}(g).$$

To see $\stackrel{*}{=}$ concretely needs some work. Give V_ρ and $V_{\rho'}$ bases $\{v_1, \ldots, v_n\}$ and $\{v'_1, \ldots, v'_{n'}\}$, respectively, and let the matrices associated to $\rho(g)$ and $\rho'(g)$ be $\{a_{ij}\}_{i,j=1}^n$ and $\{a'_{i'j'}\}_{i',j'=1}^n$, respectively. Now, $V_\rho \otimes V_{\rho'}$ has basis given by $v_i \otimes v'_{i'}$ where the i and i' vary, so we compute

$$(\rho(g) \otimes \rho'(g))(v_i \otimes v'_{i'}) = \rho(g)v_i \otimes \rho'(g)v'_{i'} = \left(\sum_{j=1}^n a_{ij}v_j\right) \otimes \left(\sum_{j'=1}^{n'} a'_{i'j'}v'_{j'}\right) = \sum_{j=1}^n \sum_{j'=1}^{n'} a_{ij}a'_{i'j'}(v_j \otimes v'_{j'}).$$

Thus, the diagonal entry (at (i, i')) here is $a_{ii}a_{i'i'}$. Summing over all diagonal entries, we conclude

$$\operatorname{tr}(\rho(g) \otimes \rho'(g)) = \sum_{i=1}^n \sum_{i'=1}^{n'} a_{ii}a_{i'i'} = \operatorname{tr}\rho(g) \cdot \operatorname{tr}\rho'(g).$$

(c) By Proposition A.13, we may give V_ρ an inner product $\langle\cdot,\cdot\rangle$ making ρ a unitary representation. Then

$$\chi_{\rho^\vee}(g) = \operatorname{tr}\left(\varphi \mapsto \varphi \circ \rho(g)^{-1}\right) \stackrel{*}{=} \operatorname{tr}\left(\rho(g)^{-\intercal}\right) = \operatorname{tr}\rho(g)^{-1} = \chi_\rho\left(g^{-1}\right),$$

where $\stackrel{*}{=}$ amounts to giving $V_\rho^\vee$ a dual basis. ■

A.5 Orthogonality Relations

Characters get most of their structure from having an inner product.

Notation A.28. For any functions $\varphi, \psi \colon G \to \mathbb{C}$, we define

$$\langle \varphi, \psi \rangle \coloneqq \frac{1}{|G|} \sum_{g \in G} \varphi(g)\psi\left(g^{-1}\right).$$

One can directly check that $\langle\cdot,\cdot\rangle$ is an inner product on the $\mathbb{C}$-vector space $\operatorname{Mor}(G, \mathbb{C})$ (though not Hermitian!).

Remark A.29. Fix a G-representation ρ. By Remark A.6, we see that $\rho(g)$ is diagonalizable, and we know that its eigenvalues are roots of unity (of order dividing $|G|$) and in particular have magnitude 1. Thus, $\rho\left(g^{-1}\right)$ has eigenvalues conjugate to the eigenvalues of $\rho(g)$, with the correct multiplicities, so

$$\chi_\rho(g) = \operatorname{tr}\rho(g) = \overline{\operatorname{tr}\rho\left(g^{-1}\right)} = \overline{\chi_\rho\left(g^{-1}\right)}.$$

Thus, our inner product does look Hermitian when we work with characters of representations.

The following result explains how we will use this inner product to talk about representations.

Theorem A.30. Fix G-representations ρ and ρ'. Then $\langle \chi_\rho, \chi_{\rho'} \rangle = \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'})$.

Proof. We apply force. By Remark A.8 and Lemma A.10, we see

$$\dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) = \dim \operatorname{Hom}_{\mathbb{C}}(V_\rho, V_{\rho'})^G = \dim \left(V_\rho^\vee \otimes_{\mathbb{C}} V_{\rho'}\right)^G.$$

To relate to characters, we use Lemma A.26 and then use Lemma A.27 to compute

$$\dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) = \frac{1}{|G|} \sum_{g \in G} \chi_{\rho^\vee \otimes \rho'}(g) = \frac{1}{|G|} \sum_{g \in G} \chi_\rho\left(g^{-1}\right) \chi_{\rho'}(g).$$

Exchanging the roles of g and g^{-1} finishes the proof. ■

Corollary A.31. Fix a G-representations ρ and ρ' with isotypical decompositions $\rho \cong \bigoplus_{i=1}^k \rho_i^{\oplus n_i}$ and $\rho' \cong \bigoplus_{i=1}^k \rho_i^{\oplus n_i'}$. Then

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \sum_{i=1}^k n_i n_i'.$$

In particular, $\langle \chi_\rho, \chi_{\rho_i} \rangle = n_i$.

Proof. By Lemma A.26, we see

$$\chi_\rho = \sum_{i=1}^k n_i \chi_{\rho_i} \qquad \text{and} \qquad \chi_{\rho'} = \sum_{i=1}^k n_i' \chi_{\rho_i},$$

so the bilinearity of our inner product yields

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \sum_{i=1}^k \sum_{j=1}^k n_i n_j \langle \chi_{\rho_i}, \chi_{\rho_j} \rangle.$$

Now, Theorem A.30 tells us that $\langle \chi_{\rho_i}, \chi_{\rho_j} \rangle = \dim \operatorname{Hom}_{\mathbb{C}[G]}(V_{\rho_i}, V_{\rho_j})$, which is $1_{i=j}$ by Corollary A.19. So this collapses to

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \sum_{i=1}^k n_i n_i',$$

which is what we wanted. The last sentence now follows by giving ρ_i an isotypical decomposition "ρ_i." ■

Remark A.32. One can show Corollary A.31 in the form of

$$\dim \operatorname{Hom}_{\mathbb{C}[G]}(V_\rho, V_{\rho'}) = \sum_{i=1}^k n_i n_i'$$

directly by taking dimensions in Lemma A.20. In particular, one can prove suitable versions of Corollaries A.33 to A.37 without needing to talk about characters at all!

Corollary A.33. Fix a G-representation ρ. Then the isotypical decomposition of ρ is unique.

Proof. Suppose we have two isotypical decompositions of ρ. In other words, we may fix irreducible representations $\rho_1, \ldots, \rho_k$ and nonnegative integers $n_1, \ldots, n_k$ and $n_1', \ldots, n_k'$ such that

$$\bigoplus_{i=1}^{k} \rho_i^{\oplus n_i} \cong \rho \cong \bigoplus_{i=1}^{k} \rho_i^{\oplus n_i'}.$$

Then applying Corollary A.31 to each of our isotypical decompositions yields

$$n_i = \langle \chi_\rho, \chi_{\rho_i} \rangle = n_i'$$

for each i, finishing. ■

Corollary A.34. Fix a group G. Then a G-representation ρ is irreducible if and only if $\langle \chi_\rho, \chi_\rho \rangle = 1$.

Proof. Let $\rho \cong \bigoplus_{i=1}^{k} \rho_i^{\oplus n_i}$ be an isotypical decomposition of ρ. Then Corollary A.31 tells us

$$\langle \chi_\rho, \chi_\rho \rangle = \sum_{i=1}^{k} n_i^2.$$

If ρ is irreducible, then there is only one nonzero term in the above sum, and it is equal to $1^2 = 1$, so $\langle \chi_\rho, \chi_\rho \rangle = 1$. Conversely, if the above sum is 1, then we have $n_i^2 \leq 1$ for each i, and we have equality achieved exactly once, so $\rho \cong \rho_i$ for some irreducible representation ρ_i, which is what we wanted. ■

Corollary A.35. Fix a group G. Then a G-representation ρ is irreducible if and only if $\rho^\vee$ is irreducible.

Proof. We compute

$$\langle \chi_{\rho^\vee}, \chi_{\rho^\vee} \rangle = \sum_{g \in G} \chi_{\rho^\vee}(g) \chi_{\rho^\vee}\left(g^{-1}\right) \stackrel{*}{=} \sum_{g \in G} \chi_\rho\left(g^{-1}\right) \chi_\rho(g) = \langle \chi_\rho, \chi_\rho \rangle,$$

where we used Lemma A.27 in $\stackrel{*}{=}$. So the left-hand side equals 1 if and only if the right-hand side equals 1, from which Corollary A.34 finishes. ■

Corollary A.36 (First orthogonality relation). Fix a group G. Given irreducible representations ρ and ρ', we have

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \begin{cases} 1 & \text{if } \rho \cong \rho', \\ 0 & \text{else.} \end{cases}$$

Proof. One can see this by comparing isotypical decompositions of ρ and ρ' and applying Corollary A.31. Alternatively, one may use Theorem A.30 and then Corollary A.19. ■

Corollary A.37. Fix a group G. There are only finitely many irreducible representations of G, and if they are $\rho_1, \ldots, \rho_k$, then

$$\sum_{i=1}^{k} (\dim \rho_i)^2 = |G|.$$

Proof. The point here is to compute the isotypical decomposition of the representation $\rho\colon G \to \mathbb{C}[G]$. Indeed, for any G-representation ρ', we see that

$$\langle \chi_\rho, \chi_{\rho'} \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \chi_{\rho'}\left(g^{-1}\right) = \frac{1}{|G|} \cdot |G| \chi_{\rho'}(1),$$

where we have used the computation in Example A.25. To finish, Lemma A.26 tells us $\chi_{\rho'}(1) = \dim \rho'$, so $\langle \chi_\rho, \chi_{\rho'} \rangle = \dim \rho'$.

Thus, if we let $\rho \cong \bigoplus_{i=1}^k \rho_i^{\oplus n_i}$ be the isotypical decomposition of $\mathbb{C}[G]$, Corollary A.31 tells us that $n_i = \langle \chi_\rho, \chi_{\rho_i} \rangle = \dim \rho_i$. Taking dimensions, we see

$$|G| = \dim \mathbb{C}[G] = \sum_{i=1}^k n_i \dim \rho_i = \sum_{i=1}^k (\dim \rho_i)^2.$$

We now show that $\rho_i, \ldots, \rho_k$ are all the irreducible representations. For any irreducible G-representation ρ, if $\rho \not\cong \rho_i$ for each i, then Corollary A.31 implies that $\dim \operatorname{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G], \rho) = 0$, which is false as shown above. ■

We are now ready to explain why we care so much about characters.

Corollary A.38. Fix G-representations ρ and ρ'. Then $\rho \cong \rho'$ if and only if $\chi_\rho = \chi_{\rho'}$.

Proof. There is nothing to say for the forward direction. In the reverse direction, let $\rho_1, \ldots, \rho_k$ denote the irreducible G-representations. Then we see

$$\langle \chi_\rho, \chi_{\rho_i} \rangle = \langle \chi_{\rho'}, \chi_{\rho_i} \rangle$$

for any i, so Corollary A.31 lets us give ρ and ρ' the same isotypical decomposition

$$\bigoplus_{i=1}^k \rho_i^{\oplus \langle \chi_\rho, \chi_{\rho_o} \rangle},$$

so $\rho \cong \rho'$ follows. ■

Corollary A.36 is the "first" orthogonality relation. We will prove the second one later.

A.6 Class Functions

Lemma A.26 motivates the following definition.

Definition A.39 (class function)**.** Fix a group G. Then a function $\varphi\colon G \to \mathbb{C}$ is a *class function* if and only if $\varphi\left(hgh^{-1}\right) = \varphi(g)$ for any $g, h \in G$. Note that the set of all class functions forms a $\mathbb{C}$-vector space.

It will turn out that characters of irreducible representations form an orthonormal basis of the vector space of all class functions. The key idea is the following lemma, which connects class functions back to representations.

Lemma A.40. Fix a group G, and let $\varphi\colon G \to \mathbb{C}$ be a function. Then the following are equivalent.

(a) φ is a class function.

(b) The element $e_\varphi := \sum_{g \in G} \varphi(g) \in \mathbb{C}[G]$ is in the center of $\mathbb{C}[G]$.

Proof. We have two implications to show. For any $h \in G$, we compute

$$he_\varphi h^{-1} = \sum_{g \in G} \varphi(g) hgh^{-1} = \sum_{g \in G} \varphi\left(hgh^{-1}\right) g.$$

Now, e_φ is in the center if and only if $he_\varphi h^{-1} = e_\varphi$ for all $h \in G$. (The forward implication is by definition; the reverse implication is because any element of $\mathbb{C}$ commutes with e_φ already.) But comparing the g-coordinate of $he_\varphi h^{-1}$ above and e_φ reveals that this is equivalent to $\varphi\left(hgh^{-1}\right) = \varphi(g)$ for any $g, h \in G$, which is equivalent to φ being a class function. ■

Proposition A.41. Fix a group G. Then the characters of irreducible representations form an orthonormal basis of the vector space of all class functions.

Proof. This is tricky. That these characters are orthonormal follows from Corollary A.36, so it remains to show that these span the vector space of class functions. Let $\rho_1, \ldots, \rho_k$ be the irreducible G-representaitons. Now, for any class function ψ, we define

$$\varphi \coloneqq \psi - \sum_{i=1}^{k} \langle \psi, \chi_{\rho_i} \rangle \chi_{\rho_i}$$

so that $\langle \varphi, \chi_{\rho_i} \rangle = 0$ for each i by the linearity of our inner product. We claim that φ vanishes, which will finish because it shows that ψ lives in the span of the χ_{ρ_i}.

We now apply a trick. As in Lemma A.40, define $e_\varphi \coloneqq \sum_{g \in G} \varphi(g) g$. For any G-representation ρ, we see from Lemma A.40 that multiplication by e_φ induces a G-invariant map $\rho_\varphi \colon V_\rho \to V_\rho$. In particular, if ρ is irreducible, then Theorem A.17 tells us that ρ_φ is equal to multiplication by a scalar. By providing V_ρ with a basis and writing out the matrix associated to ρ_φ, we see that

$$\rho_\varphi = \frac{\operatorname{tr} \rho_\varphi}{\dim V_\rho} = \frac{1}{\dim V} \sum_{g \in G} \varphi(g) \operatorname{tr} \rho(g) = \frac{1}{\dim V} \langle \varphi, \chi_{\rho^\vee} \rangle,$$

where we used Lemma A.27 in the last equality. But $\rho^\vee$ is also irreducible by Corollary A.35, so $\langle \varphi, \chi_\rho \rangle = 0$ by hypothesis on φ.

Now, decomposing the regular representation $\rho \colon G \to \mathbb{C}[G]$ as a sum of irreducible representations (via Theorem A.15) we again note that the multiplication-by-e_φ map $\rho_\varphi \colon \mathbb{C}[G] \to \mathbb{C}[G]$ must be the zero map because it is the zero map on each summand. Thus,

$$0 = e_\varphi \cdot 1 = \sum_{g \in G} \varphi(g) g,$$

so $\varphi(g) = 0$ for each $g \in G$. This completes the proof. ■

Corollary A.42. Fix a group G. Then the number of irreducible representations is equal to the number of conjugacy classes of G.

Proof. By Proposition A.41, characters of irreducible representations are distinct (by Corollary A.36) and form a basis of the space of all class functions. So the number of irreducible characters is the dimension of the space of all class functions. But letting $c_1, \ldots, c_r$ denote the conjugacy classes of G, we see that class functions are functions $\{c_1, \ldots, c_r\} \to \mathbb{C}$, and this space has dimension r. This finishes. ■

While we're here, we also prove the second orthogonality relation.

Corollary A.43 (Second orthogonality relation)**.** Fix a group G. Let $\rho_1, \ldots, \rho_r$ be the irreducible representations of G. For any $g \in G$, we let $[g]$ denote the conjugacy class of G. Then each $g, h \in G$ has

$$\sum_{i=1}^{r} \chi_{\rho_i}(g)\chi_{\rho_i}\left(h^{-1}\right) = \begin{cases} |G|/|[g]| & \text{if } [g]=[h], \\ 0 & \text{else.} \end{cases}$$

Proof. Let the conjugacy classes of G be represented as $[g_1], \ldots, [g_r]$; note that this is equal to the number of irreducible representations by Corollary A.42. The point here is to do linear algebra to achieve the result from Corollary A.36. Indeed, define the $r \times r$ matrix

$$M := \begin{bmatrix} \sqrt{\frac{|[g_1]|}{|G|}}\chi_1(g_1) & \cdots & \sqrt{\frac{|[g_r]|}{|G|}}\chi_1(g_r) \\ \vdots & \ddots & \vdots \\ \sqrt{\frac{|[g_1]|}{|G|}}\chi_r(g_1) & \cdots & \sqrt{\frac{|[g_r]|}{|G|}}\chi_r(g_r) \end{bmatrix}.$$

The main claim is that M is a unitary matrix. Notably, Remark A.29 tells us that

$$M^\dagger = \begin{bmatrix} \sqrt{\frac{|[g_1]|}{|G|}}\overline{\chi_1(g_1)} & \cdots & \sqrt{\frac{|[g_1]|}{|G|}}\overline{\chi_r(g_1)} \\ \vdots & \ddots & \vdots \\ \sqrt{\frac{|[g_r]|}{|G|}}\overline{\chi_1(g_r)} & \cdots & \sqrt{\frac{|[g_r]|}{|G|}}\overline{\chi_r(g_r)} \end{bmatrix} = \begin{bmatrix} \sqrt{\frac{|[g_1]|}{|G|}}\chi_1\left(g_1^{-1}\right) & \cdots & \sqrt{\frac{|[g_1]|}{|G|}}\chi_r\left(g_1^{-1}\right) \\ \vdots & \ddots & \vdots \\ \sqrt{\frac{|[g_r]|}{|G|}}\chi_1\left(g_r^{-1}\right) & \cdots & \sqrt{\frac{|[g_r]|}{|G|}}\chi_r\left(g_r^{-1}\right) \end{bmatrix}.$$

Thus, Corollary A.36 tells us that

$$(MM^\dagger)_{ik} = \sum_{j=1}^{r} M_{ij}M^\dagger_{jk} = \sum_{j=1}^{r} \frac{|[g_j]}{|G|}\chi_i(g_j)\chi_k\left(g_j^{-1}\right) = \frac{1}{|G|}\sum_{g\in G}\chi_i(g)\chi_k(g^{-1}) = 1_{i=k},$$

so $MM^\dagger$ is the identity matrix, as needed. In particular, $M^\dagger = M^{-1}$, so we also see that $M^\dagger M$ is the identity matrix, so

$$1_{i=k} = (M^\dagger M)_{ik} = \sum_{j=1}^{r} M^\dagger_{ij}M_{jk} = \frac{\sqrt{|[g_i]| \cdot |[g_k]|}}{|G|}\sum_{j=1}^{r}\chi_j(g_i^{-1})\chi_j(g_k).$$

Thus, if $i = k$, then we see the leftmost summation evaluates to $|G|/|[g_i]|$; otherwise, the leftmost summation vanishes. The summation can replace g_i and g_k with any representative of their respective conjugacy classes by Lemma A.26, so we complete the proof. ■

Remark A.44. The moral of the above proof is that the character table (which is the matrix $\{\chi_i([g_j])\}$) is "almost" unitary. Indeed, it becomes unitary after appropriately scaling the columns.