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 $\rho_1,\dots,\rho_n$ 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 $\rho_1,\dots,\rho_n$ 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 $v_1,\dots,v_n$ 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 $v_1,\dots,v_n$ 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 $\mathcal{F}$ 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 $f_{sv}\in V_{\widehat{\rho}}$ 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 $F\colon G\to \mathrm{Hom}_{\mathbb{C}}(V_\rho,V_\sigma)$ that satisfies (1.2), we define a function $\varphi\colon G\times G\to \mathrm{Hom}_{\mathbb{C}}(V_\rho, V_\sigma)$ by

$$\varphi(g_1,g_2) \coloneqq F\left(g_1g_2^{-1}\right). \tag{1.7}$$

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, $\mathcal{F}$ is isomorphic to F'_G.

For every $F\in\mathcal{F}$, 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

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

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

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

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

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

Clearly $|B| = (q-1)^2 q$. Straightforward calculations show that the matrix $w := \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$, 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

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

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

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

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

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

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

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

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

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

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 $\mathrm{Tr}(\alpha) \coloneqq \alpha + \overline{\alpha}$ and $\mathrm{N}(\alpha) \coloneqq \alpha\overline{\alpha}$, 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

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

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

$$\operatorname{Res}^P_U \operatorname{Ind}^P_U \psi \stackrel{?}{=} \bigoplus_{a \in A} \psi_a. \tag{2.2}$$

Indeed, for every $a \in A$, we define a function $f_a \in \operatorname{Ind}^P_U V_\psi$ 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

As a first step toward the determination of the irreducible representations of G, we investigate those that appear as components of $\operatorname{Ind}_B^G \mu$, where μ is a character of B. In order to shorten the notation, we make the convention

$$\widehat{\mu} := \operatorname{Ind}_B^G \mu$$

and stick to it for the rest of these notes. The dimension of $\widehat{\mu}$ is $q+1$. Our task in this section is to determine the connection between μ and $\widehat{\mu}$.

In order to do this, we have the following definition.

Definition 2.5 (Jacquet module)**.** We define the *Jacquet module* of a representation ρ of G as

$$J(V_\rho) := \{v \in V_\rho : \rho(u)v = v \text{ for every } u \in U\}.$$

The fact that U is normal in B implies that B acts on $J(V_\rho)$. Indeed, if $v \in J(V_\rho)$, $b \in B$, and $u \in U$, then $b^{-1}ub \in U$; hence

$$\rho(u)\rho(b)v = \rho(b)\rho\left(b^{-1}ub\right)v = \rho(b)v.$$

It might happen however that $J(V_\rho)$ is not a G-invariant subspace.

If ρ_1 and ρ_2 are two representations of ρ, then clearly

$$J\left(V_{\rho_1} \oplus V_{\rho_2}\right) = J\left(V_{\rho_1}\right) \oplus J\left(V_{\rho_2}\right).$$

In particular, we have the following lemma.

Lemma 2.6. If μ is a character of B, then $\dim J(V_{\widehat{\mu}}) = 2$.

Proof. By definition, $J(V_{\widehat{\mu}})$ contains all functions $f\colon G \to \mathbb{C}$ that satisfy

$$f(bg) = \mu(B)f(g) \qquad \text{and} \qquad f(bu) = f(b)$$

for all $b \in B$, $g \in G$, and $u \in U$. In particular,

$$f(b) = \mu(b)f(1) \qquad \text{and} \qquad f(bwu) = \mu(b)f(w).$$

Using the Bruhat decomposition $G = B \sqcup BwU$, this implies that f is determined by its values in 1 and in w. It follows that $\dim J(V_{\widehat{\mu}}) = 2$, and a canonical basis for $J(V_{\widehat{\mu}})$ is the two functions f_1 and f_2 satisfying

$$\begin{cases} f_1(1) = 1, \\ f_1(w) = 0, \end{cases} \qquad \text{and} \qquad \begin{cases} f_2(1) = 0, \\ f_2(w) = 1. \end{cases} \tag{2.8}$$

This completes the proof. ∎

A supplement to Lemma 2.6 is the following.

Lemma 2.7. If μ is a character of B, then B operating on $J(\mu_{\widehat{\mu}})$ has two eigenvectors f_1 and f_2 (defined by (2.8)) that correspond to the eigenvalues μ and μ_w, respectively. In detail,

$$\widehat{\mu}(b)f_1 = \mu(b)f_1 \qquad \text{and} \qquad \widehat{\mu}(b)f_2 = \mu_w(b)f_2 \tag{2.9}$$

for every $b \in B$.

Proof. We have only to prove that both sides of the equalities (2.9) coincide in 1 and in w.

Indeed, for f_1, we have $(\widehat{\mu}(b)f_1)(1) = f_1(b) = \mu(b)f_1(1)$. Also, by the Bruhat decomposition, there exists for every $b \in B$ elements $b_1 \in B$ and $u \in U$ such that $wb = b_1wu$. Hence,

$$(\widehat{\mu}(b)f_1)(w) = f_1(wb) = f_1(b_1wu) = \mu(b_1)f_1(w) = 0 = \mu(b)f_1(w).$$

For f_2, we have

$$(\widehat{\mu}(b)f_2)(1) = f_2(b) = \mu(b)f_2(1) = 0 = \mu_w(b)f_2(1).$$

A difficulty arises in calculating $(\widehat{\mu}(b)f_2)(w)$. We overcome this by first considering $d \in D$. Then

$$(\widehat{\mu}(d)f_2)(w) = f_2(wd) = f_2(wdww) = \mu(wdw)f_2(w) = \mu_w(d)f_2(w). \tag{2.10}$$

In general, we know from Lemma 2.6 that f_1 and f_2 generate $J(V_{\widehat{\mu}})$. Hence, for every $b \in B$, there exist $\alpha_1(b), \alpha_2(b) \in \mathbb{C}$ such that

$$\widehat{\mu}(b)f_2 = \alpha_1(b)f_1 + \alpha_2(b)f_2. \tag{2.11}$$

Calculating both sides of (2.11) at 1, we obtain $\alpha_1(b) = 0$; hence, $\widehat{\mu}(b)f_2 = \alpha_2(b)f_2$. It follows that $\alpha_2(b_1b_2) = \alpha_2(b_1)\alpha_2(b_2)$ for $b_2, b_2 \in B$; i.e., $\alpha - 2$ is a character of B. Hence, if

$$b := \begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix} \qquad \text{and} \qquad d := \begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix},$$

then

$$(\widehat{\mu}(b)f_2)(w) = \alpha_2(b)f_2(w) = \alpha_2(d)f_2(w) = (\widehat{\mu}(d)f_2)(w) = \mu_w(d)f_2(w) = \mu_w(b)f_2(w),$$

which completes the proof. ■

The importance of the Jacquet modules for our investigation lies in the following lemma.

Lemma 2.8. Let ρ be a representation of G. Then $J(V_\rho) \neq 0$ if and only if there exists character μ of B such that $(\rho, \widehat{\mu}) \neq 0$.

Proof. Suppose $J(V_\rho) \neq 0$. Then $J(V_\rho)$ can be considered as a nontrivial B/U-space via ρ. But B/U is abelian; hence $J(V_\rho)$ splits into a direct sum of one-dimensional B/U-subspaces. It follows that there exists a character μ of B and a nonzero element $v \in J(V_\rho)$ such that $\rho(b)v = \mu(b)v$ for every $b \in B$. Hence, $\left(\mathrm{Res}_B^G \rho, \mu\right) \neq 0$. By the Frobenius reciprocity theorem, $(\rho, \widehat{\mu}) \neq 0$, and half of the lemma is thus proved.

Now, suppose that $(\rho, \widehat{\mu}) \neq 0$. Then arguing backwards we find that there exists a nonzero element $v \in V_\rho$ such that $\rho(b)v = \mu(b)v$ for every $b \in B$. Now, μ is trivial on U because U is the commutator of B. Hence, $v \in J(V_\rho)$, which is therefore not zero. ■

Corollary 2.9. Let ρ be an irreducible representation of G. Then $J(V_\rho) \neq 0$ if and only if there exists a character μ of B such that $\rho \leq \widehat{\mu}$.

Proof. Immediate from Lemma 2.8. ■

Corollary 2.10. If μ is a character of B, then $\widehat{\mu}$ has at most two irreducible components.

Proof. Let $\widehat{\mu} = \rho_1 \oplus \cdots \oplus \rho_r$ be a decomposition of $\widehat{\mu}$ into irreducible components. Then

$$J(V_{\widehat{\mu}}) = J(V_{\rho_1}) \oplus \cdots \oplus J(V_{\rho_r}).$$

By Corollary 2.9, $J(V_{\rho_i}) \neq 0$ for $i = 1, \ldots, r$. Hence, the dimension of the right-hand side is $\geq r$. On the other hand, $\dim J(V_{\widehat{\mu}}) = 2$ by Lemma 2.6. Hence, $r \leq 2$. ■

The next few lemmas give the exact information about the possible two components of $\widehat{\mu}$.

Lemma 2.11. If μ is a character of B and $\mu = \mu_w$, then $\widehat{\mu}$ has a one-dimensional component.

Proof. The assumption implies that μ corresponds to a pair (μ_1, μ_1) of characters $K^\times$; i.e., if

$$b := \begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix},$$

then $\mu(b) = \mu_1(\alpha)\mu_1(\delta)$. It follows that $\mu(b) = \mu_2(\det b)$. Now, define a function $f\colon G \to \mathbb{C}$ by $f(g) := \mu_1(\deg g)$. Then $f(bg) = \mu(b)f(g)$, that is, f belongs to $V_{\widehat{\mu}}$. Moreover,

$$\left(\widehat{\mu}(s)f\right)(g) = f(gs) = \mu_1(\det s)f(g)$$

for $s, g \in G$. It follows that f is an eigenvector of G that belongs to the eigenvalue $\mu_1 \circ \det$. ■

Lemma 2.12. If μ is a character of B, then $\widehat{\mu}$ has at most one one-dimensional component.

Proof. Assume that $\widehat{\mu}$ has two distinct one-dimensional components, χ_1 and χ_2. Then by Corollary 2.10 they are all the components of $\widehat{\mu}$; i.e., $\widehat{\mu} = \chi_1 \oplus \chi_2$. It follows that $q + 1 = \dim \widehat{\mu} = 2$, which is a contradiction. ■

Lemma 2.13. If μ is a character of B, then

$$\operatorname{Res}_P V_{\widehat{\mu}} = \operatorname{Res}_P J(V_{\widehat{\mu}}) \oplus V_\pi.$$

Proof. Note $J(V_{\widehat{\mu}})$ is a two-dimensional B-subspace of $V_{\widehat{\mu}}$; in particular, $J(V_{\widehat{\mu}})$ is a P-subspace of $V_{\widehat{\mu}}$. Let V be a P-complement to $J(V_{\widehat{\mu}})$ in $V_{\widehat{\mu}}$. Then $\dim V = q - 1$. Further, V has no one-dimensional P-subspace; indeed otherwise, there would exist a nonzero element $v \in V$ and a character χ of P such that $\widehat{\mu}(p)v = \chi(p)v$ for every $p \in P$. In particular, we would have for $u \in U$ that $\widehat{\mu}(u)v = v$ since $U = P'$. It follows that $v \in J\left(V_{\widehat{\mu}}\right)$; hence $v = 0$, which is a contradiction. Therefore, by Theorem 2.1, V cannot have irreducible P-subspaces of dimension less than $q - 1$. Hence, V is irreducible and isomorphic to the unique P-representation V_π of dimension $q - 1$. ■

Lemma 2.14. If μ is a character of B and $\widehat{\mu}$ is reducible, then the following are true.

(a) $\widehat{\mu}$ has a one-dimensional component.

(b) $\mu = \mu_w$.

Proof. Here we go.

(a) Let $V_{\widehat{\mu}} = V \oplus V'$ be a nontrivial G-decomposition of V. By Lemma 2.13, we can assume, without loss of generality, that $V_\pi \cap V \neq 0$. Then $V_\pi \subseteq V$ because V_π is an irreducible P-representation. On the other hand, by Lemma 2.8, $J(V) \subseteq J(V_{\widehat{\mu}}) \cap V$ is nonempty, so V is not an irreducible P-representation. Hence, $V_\pi \neq V$. It follows that $\dim V = q$ and hence $\dim V' = 1$.

(b) We have proved that there exists a character χ of G and a nonzero function $f\colon G \to \mathbb{C}$ such that

$$f(bg) = \mu(b)f(g) \qquad \text{and} \qquad f(gs) = \chi(s)f(g)$$

for every $b \in B$ and $g, s \in G$.

We claim $f(1) \neq 0$. Indeed, assume that $f(1) = 0$ and let $g \in G$. Then there exists a positive integer n such that $g^n = 1$. Hence,

$$0 = f(1) = f\left(g \cdot g^{n-1}\right) = \chi\left(g^{n-1}\right) f(g).$$

It follows that $f(g)=0$ because $\chi\left(g^{n-1}\right)\neq 0$. This is a contradiction.

Now, let $d\in D$; then $\mu(d)f(q)=f(d)=\chi(d)f(1)$. Hence, $\mu(d)=\chi(d)$. It follows that

$$\mu_w(d)=\mu(wdw)=\chi(wdw)=\chi\left(w^2\right)\chi(d)=\mu(d).$$

Hence, $\mu_w=\mu$. ∎

Lemma 2.15. Let μ and μ' be two distinct characters of B. Then $(\widehat{\mu},\widehat{\mu}')\neq 0$ if and only if $\mu'=\mu_w$.

Proof. Suppose first that $(\widehat{\mu},\widehat{\mu}')\neq 0$. Then there exists an irreducible representation ρ of G such that $\rho\leq\widehat{\mu}$ and $\rho\leq\widehat{\mu}'$. It follows from Corollary 2.9 that $J(V_\rho)\neq 0$. By the proof of Lemma 2.8, we know that B operating on $J(V_\rho)$ has an eigenvalue χ. In addition, by Lemma 2.7, we know that B operating on $J(V_{\widehat{\mu}})$ has exactly two eigenvalues μ and μ_w. It follows that $\chi=\mu$ or $\chi=\mu_w$ because $J(V_\rho)\subseteq J(V_{\widehat{\mu}})$. Similarly, $\chi=\mu'$ or $\chi=\mu'_w$, but $\mu\neq\mu'$; hence, $\mu=\mu_w$.

Conversely, suppose that $\mu'=\mu_w$. Then arguing backwards we have that $\left(\mu',\operatorname{Res}_B^G\widehat{\mu}\right)\neq 0$. Hence, by the Frobenius reciprocity theorem $(\widehat{\mu}',\widehat{\mu})\neq 0$. ∎

Lemma 2.16. Let μ and μ' be two distinct characters of B. Then $\widehat{\mu}=\widehat{\mu}'$ if and only if $\mu'=\mu_w$.

Proof. Suppose that $\mu'=\mu_w$. Then $\mu\neq\mu_w$ and $\mu'=\mu'_w$. It follows that $\widehat{\mu}$ and $\widehat{\mu}'$ are irreducible by Lemma 2.14. Also, $(\widehat{\mu},\widehat{\mu}')\neq 0$ by Lemma 2.15. Hence, $\widehat{\mu}=\widehat{\mu}'$.

The other direction of the lemma follows directly from Lemma 2.15. ∎

Summing up the lemmas in this section, we obtain the theorem.

Theorem 2.17. Let μ and μ' be characters of B and let $\widehat{\mu}:=\operatorname{Ind}_B^G\mu$ and $\widehat{\mu}':=\operatorname{Ind}_B^G\mu'$.

(a) $\dim\widehat{\mu}=q+1$.

(b) $\widehat{\mu}$ has at most two irreducible components.

(c) $\widehat{\mu}$ is irreducible if and only if $\mu\neq\mu_w$.

(d) If $\widehat{\mu}$ is reducible, it decomposes into a direct sum of a one-dimensional and q-dimensional representation.

(e) $\widehat{\mu}'=\widehat{\mu}$ if and only if $\mu'=\mu$ or $\mu'=\mu_w$.

Proof. Note (a) is clear. Corollary 2.10 gives (b). Lemmas 2.11 and 2.14 give (c). Lemma 2.11 and (b) give (d). Lastly, Lemma 2.16 gives (e). ∎

Now, consider a character μ of B that corresponds to the pair of characters (μ_1,μ_2) of $K^\times$. There are two possibilities.

(a) $\mu=\mu_w$; i.e., $\mu_1=\mu_2$. In this case, $\widehat{\mu}$ is the direct sum of a one-dimensional representation $\rho'_{(\mu_1,\mu_2)}$ and an irreducible q-dimensional representation $\rho_{(\mu_1,\mu_2)}$. $K^\times$ has $q-1$ characters; hence, in this way we obtain $q-1$ characters of G and $q-1$ different q-dimensional irreducible representations of G.

(b) $\mu\neq\mu_w$; i.e., $\mu_1\neq\mu_2$. In this case, $\widehat{\mu}$ is an irreducible representation of dimension $q+1$, and we denote it by $\rho_{(\mu_1,\mu_2)}$. The number of these μ is equal to the number of characters of B, i.e., $(q-1)^2$, minus the characters of type (a), i.e. $q-1$. Further, μ and μ_w induce the same representation. Hence, in this way we obtain $\frac{1}{2}(q-1)(q-2)$ irreducible representations of G of dimension $q-1$.

We have therefore proved the following theorem.

Theorem 2.18. The irreducible representations of G, which are components of induced representations of the form $\operatorname{Ind}_B^G \mu$ where μ is a character of B, split up in the following classes.

(a) $q-1$ different 1-dimensional representations $\rho'_{(\mu_1,\mu_1)}$.

(b) $q-1$ different q-dimensional representations $\rho_{(\mu_1,\mu_2)}$.

(c) $\frac{1}{2}(q-1)(q-2)$ distinct $(q+1)$-dimensional representations, $\rho_{(\mu_1,\mu_2)}$.

If χ is a character of G, then χ is a component of $\operatorname{Ind}_B^G \operatorname{Res}_B^G \chi$. It follows by Theorem 2.18 that G has exactly $q-1$ characters. Hence, $[G : G^c] = q-1$. The subgroup $\mathrm{SL}(2,K) = \{g \in G : \deg g = 1\}$ is normal and $G/\mathrm{SL}(2,K) \cong K^\times$. Hence, we have the following corollary.

Corollary 2.19. $\mathrm{SL}(2,K)$ is the commutator subgroup of $\mathrm{GL}(2,K)$.

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

Let μ be a character of B, and let $\widehat{\mu} := \operatorname{Ind}_B^G \mu$. Bruhat's decomposition of G implies that $|B\backslash G/B| = 2$. Hence, by Corollary 1.2, $(\widehat{\mu},\widehat{\mu}) \leq 2$. Because $(\widehat{\mu},\widehat{\mu}) \geq 1$, there are only two possibilities: either $(\widehat{\mu},\widehat{\mu}) = 1$, in which case $\widehat{\mu}$ is irreducible; or $(\widehat{\mu},\widehat{\mu}) = 2$. We also know that if $\widehat{\mu} = \bigoplus_{i=1}^r n_i p_i$ is the canonical decomposition of $\widehat{\mu}$, then

$$(\widehat{\mu},\widehat{\mu}) = \sum_{i=1}^r n_i^2.$$

Because 2 can be decomposed into a sum of squares only in the form $2 = 1^2 + 1^2$, it follows that $(\widehat{\mu},\widehat{\mu}) = 2$ implies that $\widehat{\mu}$ decomposes into a direct sum of two non-isomorphic representations. We have therefore proved the following theorem.

Theorem 2.20. Let μ be a character of B and let $\widehat{\mu} := \operatorname{Ind}_B^G \mu$. Then either $(\widehat{\mu},\widehat{\mu}) = 1$, in which case $\widehat{\mu}$ is irreducible, or $(\widehat{\mu},\widehat{\mu}) = 2$, in which case $\widehat{\mu}$ decomposes into a direct sum of two non-isomorphic representations.

Obviously, Theorem 2.20 is also a consequence of Theorem 2.17. However, the proof given above is independent of Theorem 2.17.

2.5 The dimension of cuspidal representations

Irreducible representations of G that are not components of $\widehat{\mu}$, with μ a character of B, are said to be *cuspidal*. By Corollary 2.9, an irreducible representation ρ of G is cuspidal if and only if $J(V_\rho) = 0$. Comparing Proposition 1.3 with Theorem 2.18, we find that G has $\frac{1}{2}\left(q^2 - q\right)$ cuspidal representations, exactly the same as the number of conjugacy classes of the form $c_4(\alpha)$.

We delay a further explanation of this phenomenon to section 2.10 and concentrate in this section on proving that all cuspidal representations have dimension $q-1$. The first toward this goal is as follows.

Lemma 2.21. Let ρ be a cuspidal representation of G. Then $\operatorname{Res}_P^G \rho = r\pi$ for some positive integer r. In particular, $\dim \rho = r(q-1)$ is a multiple of $q-1$.

Proof. The P-representation $\operatorname{Res}_P^G V_\rho$ cannot have one-dimensional components. Indeed, otherwise, there would exist a nonzero vector $v \in V_\rho$ and a character χ of P such that $\rho(p)v = \chi(p)v$ for every $p \in P$. In particular, we would have $\rho(u)v = v$ for every $u \in U$; i.e., $v \in J(V_\rho)$; thus, $J(V_\rho) \neq 0$, contrary to the assumption that ρ is cuspidal (see also the proof of Lemma 2.13). By Theorem 2.1, $\operatorname{Res}_P^G \rho$ must be a multiple of π. ■

Proposition 2.22. The following are true.

(a) Let ρ be a cuspidal representation. Then $\operatorname{Res}_P^G \rho = \pi$ and $\dim \rho = q+1$.

(b) Conversely, if ρ is a representation of G such that $\operatorname{Res}_P^G \rho = \pi$, then ρ is cuspidal.

Proof. Here we go.

(a) Using the formula $|G| = \sum_\sigma (\dim \sigma)^2$ where σ runs over the irreducible representations of G, and by Theorem 2.18, we have

$$(q-1)^2 q(q+1) \geq (q-1)\cdot 1^2 + (q-1)\cdot q^2 + \frac{1}{2}(q-1)(q-2)\cdot(q+1)^2 + \sum_{\sigma \text{ cuspidal}} (\dim \sigma)^2.$$

By Lemma 2.21, there exists for every σ a positive integer $r(\sigma)$ such that $\dim \sigma = (q-1)r(\sigma)$. Hence,

$$\frac{1}{2}\left(q^2-q\right) \geq \sum_{\sigma \text{ cuspidal}} r(\sigma).$$

The number of the summands on the right-hand side is equal to $\frac{1}{2}\left(q^2-q\right)$. Hence, $r(\sigma)=1$, and (a) follows from Lemma 2.21.

(b) The representation π is irreducible; hence ρ is irreducible too. Also, if μ is a character of B, then by Theorem 2.18, the components of $\widehat{\mu}$ have the dimensions 1, q, or $q=1$. However, $\dim \rho = \dim \pi = q-1$; hence, ρ is not equal to any of them (i.e., ρ is cuspidal). ■

The proof of Proposition 2.22(a) relies heavily on the fact that K is a finite field. We now give another proof that will be independent of this fact.

Let $\widehat{\pi} := \operatorname{Ind}_B^G = \operatorname{Ind}_U^G \psi$. Then by Proposition 1.1, $\operatorname{End}_{\mathbb{C}[G]} V_{\widehat{\pi}}$ is isomorphic to the algebra A of all functions $F\colon G \to \mathbb{C}$ satisfying

$$F(u_1 g u_2) = \psi(u_1 u_2) F(g) \qquad \text{for } u_1, u_2 \in U \text{ and } g \in G,$$

where multiplication between two functions $F_1, F_2 \in A$ is given by the formula

$$(F_1 * F_2)(g) = \frac{1}{[G:U]} \sum_{s\in G} F_1\left(gs^{-1}\right) F_2(s)$$

(see (1.8)). We will show that A is abelian. This implies that $\widehat{\pi}$ has no multiple components (see section 1.1). If ρ is a cuspidal representation, then by Lemma 2.21 there exists a positive integer r such that $\left(\operatorname{Res}_P^G \rho, \pi\right) = r$ and $\dim \rho = r(q-1)$. Hence, by the Frobenius reciprocity theorem, $r = (\rho, \widehat{\pi}) = 1$, and our contention is proved.

Our method of proving that A is abelian is indirect. We shall define an involution on A; i.e., a map $F \mapsto F'$ such that $(F_1 * F_2)' = F_2' * F_1'$. We further prove that $F = F'$ for every $F \in A$. Hence, $F_1 * F_2 = F_2 * F_1$.

We start by defining an involution $g \mapsto g'$ on G: if $g = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, we let $g' := \begin{bmatrix} \delta & \beta \\ \gamma & \alpha \end{bmatrix}$. Then $(g_1 g_2)' = g_2' g_1'$, $g'' = g$, and $g = g'$ if g is symmetric with respect to the second diagonal. In particular, $u' = u$ for every $u \in U$. We continue by defining for an element $F \in A$ a function $F'\colon G \to \mathbb{C}$ by $F'(g) := F(g')$. Then F' belongs to A. In order prove that $F = F'$, it suffices to show that F and F' coincide on representatives of the double classes $U\backslash G/U$. Indeed, by Bruhat's decomposition $G = B \sqcup BwU$ and because $B = UD$, we have that the above representations are either of the form

$$\text{(a) } \begin{bmatrix} 0 & \beta \\ \gamma & 0 \end{bmatrix}, \qquad \text{or of the form (b) } \begin{bmatrix} \alpha & 0 \\ 0 & \delta \end{bmatrix}.$$

Clearly, F and F' coincide on the matrices (a) and on the matrices (b) in case $\alpha = \delta$. In order to prove that F and F' coincide also on the matrices (b) in case $\alpha \neq \delta$, it suffices to show that F (and hence also F') vanishes on them. Indeed, acting with F on both sides of the identity

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

we have

$$\psi(\beta)F\left(\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix}\right) = F\left(\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix}\right)\psi\left(\alpha^{-1}\delta\beta\right).$$

If $F\left(\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix}\right) \neq 0$, then $\psi(\beta) = \psi\left(\alpha^{-1}\delta\beta\right)$; hence, $\psi\left(\beta\left(1-\alpha^{-1}\delta\right)\right) = 1$ for every $\beta \in K$. It follows that ψ is the unit character of K^+, which is a contradiction.

This completes the alternative proof of Proposition 2.22(a). Note that we have actually also proved the following proposition.

Proposition 2.23. The representation $\mathrm{Ind}_U^G \psi$ has no multiple components.

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

We need this for an explicit description of the cuspidal representations. Let

$$w' := \begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}, \qquad z := \begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}, \qquad \text{and} \qquad s := w'z.$$

Then we have the following relations between w' and the elements of B:

$$w'\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix}(w')^{-1} = \begin{bmatrix}\beta & 0\\ 0 & \alpha\end{bmatrix}, \tag{2.12}$$

$$(w')^2 = \begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix} \tag{2.13}$$

$$s^3 = 1. \tag{2.14}$$

Proposition 2.24. The group $\mathrm{GL}(2, K)$ is the free group generated by B and w' with (2.12), (2.13), and (2.14) as the defining relations.

Proof. Denote by G the free group generated by B and w' with the above defining relations. Then there exists a unique epimorphism θ of G onto $\mathrm{GL}(2, K)$ which is the identity on B and maps w' onto itself. We have to prove that its kernel consists of 1.

We claim that for every $b \in B \setminus D$, there exists $b_1, b_2 \in B$ such that $w'bw' = b_1w'b_2$. Indeed, if

$$b := \begin{bmatrix}\alpha & \beta\\ 0 & \delta\end{bmatrix}$$

and $\beta \neq 0$, then

$$b = \begin{bmatrix}1 & 0\\ 0 & \delta\beta^{-1}\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix} = d'zd'';$$

also $w'zw'zw'z = 1$ by (2.14); hence,

$$w'zw' = z^{-1}(w')^{-1}z^{-1} = z^{-1}\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}w'z^{-1}$$

by (2.13). It follows that

$$w'bw' = \left(w'd'(w')^{-1}\right) w'zw' \left((w')^{-1}d''w'\right) = \left(w'd'(w')^{-1}\right) z^{-1} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} w'z^{-1} \left((w')^{-1}d''w'\right) = b_1 w' b_2,$$

by (2.12). This completes the proof of the claim.

Next, note that if $d \in D$, then $w'dw' = \left(w'd(w')^{-1}\right)(w')^2 \in B$ by (2.12) and (2.13). Now, let $g \neq 1$ be in the kernel of θ. Then $g \notin B$; hence, g can be written, for example, as $g = b_0 w' b_1 \cdots w' b_r$, where $b_i \in B$. If $r \geq 2$, then either $w'b_1w' = b_1' \in B$, if $b_1 \in D$, or $w'b_1w' = b_1'w'b_2'$ with $b_1', b_2' \in D$ if $b_1 \in B \setminus D$. In any case one can rewrite g as $g = b_2''w' \ldots w'b_r$. By a repeated application of this procedure, one finally proves that $g \in Bw'B$; i.e.,

$$g = \begin{bmatrix} \alpha' & \beta' \\ 0 & \delta' \end{bmatrix} w' \begin{bmatrix} \alpha & \beta \\ 0 & \delta \end{bmatrix}.$$

The right-hand side is mapped by θ to an element

$$\begin{bmatrix} * & * \\ -\delta'\alpha & * \end{bmatrix}$$

of $\mathrm{GL}(2,K)$. But g is mapped to 1. Hence, $\delta'\alpha = 0$, which is a contradiction. ■

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

We have denoted by L the unique quadratic extension of K. It has q^2 elements. If α is an element of L, then $\overline{\alpha}$ denotes its unique conjugate over K. Then the function $\mathrm{N}\,\alpha := \alpha\overline{\alpha}$ is the norm map from L to K. It is multiplicative.

Lemma 2.25. The function N is surjective.

Proof. The Galois group of L over K is generated by the Frobenius automorphism $\alpha \mapsto \alpha^q$. Hence, $\mathrm{N}\,\alpha = \alpha^{q+1}$. The restriction of N to $L^\times$ is a homomorphism to $K^\times$. It follows that the kernel E of this homomorphism consists of $q+1$ elements. Hence, its image consists of $\frac{q^2-1}{q+1} = q-1$ elements, exactly as many elements as $K^\times$ has. ■

We note that Lemma 2.25 also follows from the fact that the Brauer group of K is trivial. The proof of the lemma is not so elementary as the one we gave, but it is independent of counting elements.

Corollary 2.26 (Hilbert's Satz 90)**.** If β is an element of $L^\times$ such that $\mathrm{N}\,\beta = 1$, then there exists an $\alpha \in L$ such that $\alpha\overline{\alpha}^{-1} = \beta$.

Proof. Let $E := \ker \mathrm{N}$. The map $h\colon L^\times \to E$ defined by $h(\alpha) := \alpha\overline{\alpha}^{-1}$ is a homomorphism. Its kernel is $K^\times$. Hence, the image of h as $\left(q^2-1\right)(q-1)^{-1}$ elements, exactly as many as E has. ■

Definition 2.27 (decomposable)**.** Let χ be a character of $K^\times$. Composing χ with the norm map N from $L^\times$ to $K^\times$, we obtain a character $\widetilde{\chi}$ of $L^\times$ by

$$\widetilde{\chi}(\alpha) := \chi(\mathrm{N}\,\alpha) \qquad \text{for } \alpha \in L^\times. \tag{2.15}$$

Here, $\widetilde{\chi}$ is said to be *decomposable.*

Notation 2.28. If ν is an arbitrary character of $L^\times$, then $\overline{\nu}$ denotes its conjugate over K; i.e., $\overline{\nu}(\alpha) := \nu(\overline{\alpha})$ for $\alpha \in L^\times$.

Lemma 2.29. A character ν of $L^\times$ is decomposable if and only if $\nu = \overline{\nu}$.

Proof. If there exists a character χ of $K^\times$ such that $\nu = \widetilde{\chi}$, then certainly $\nu(\alpha) = \nu(\overline{\alpha})$ for every $\alpha \in K^\times$. Conversely, if $\nu = \overline{\nu}$, then we define $\chi(\mathrm{N}\,\alpha) := \nu(\alpha)$ for $\alpha \in L^\times$. If $\beta \in L^\times$ is such that $\mathrm{N}\,\alpha = \mathrm{N}\,\beta$, then by Corollary 2.26, there exists a $\gamma \in L^\times$ such that $\alpha\beta^{-1} = \gamma\overline{\gamma}^{-1}$; hence, $\nu(\alpha) = \nu(\beta)$, and therefore $\chi(\mathrm{N}\,\alpha)$ is well-defined. The fact that N is surjective now extends the domain of definition of χ to $K^\times$. Hence, χ is a character of $K^\times$ and ν is therefore decomposable. ■

Lemma 2.30. If ν is a non-decomposable character of $L^\times$, then

$$\sum_{\mathrm{N}\,x=\alpha} \nu(x) = 0$$

for every $\alpha \in K^\times$.

Proof. By the proof of Lemma 2.29, there exists a $\lambda \in L^\times$ such that $\mathrm{N}\,\lambda = 1$ and $\nu(\lambda) \neq 1$. Hence,

$$\sum_{\mathrm{N}\,x=\alpha} \nu(x) = \sum_{\mathrm{N}\,x=\alpha} \nu(\lambda x) = \nu(\lambda) \sum_{\mathrm{N}\,x=\alpha} \nu(x),$$

and our claim follows. ■

We shall need the analogue to Lemma 2.25 for the trace function $\mathrm{Tr}\colon L^+ \to K^+$ defined by $\mathrm{Tr}\,x := x + \overline{x}$.

Lemma 2.31. The function Tr is surjective.

Proof. The trace function is a homomorphism. Its kernel consists of those x in L that satisfy $x + x^q = 0$. It contains therefore q elements. Therefore, Tr is surjective. ■

Corollary 2.32. If $\alpha \in L^\times$, then for every $\beta \in K$, there exists an $x \in L$ such that $\alpha x + \overline{\alpha x} = \beta$.

Proof. This follows from Lemma 2.31. ■

2.8 Assigning cuspidal reps. to non-decomposable characters

Let ν be a non-decomposable character. We are going to define a representation $\rho = \rho_\nu$ of G that will turn out to be a cuspidal representation. In order to define ρ on G, it suffices by Proposition 2.24 to define ρ as a map from $B \cup \{w'\}$ into the automorphism group of an appropriate vector space B such that the restriction of ρ to B is a homomorphism and such that ρ preserves the relation (2.12), (2.13), and (2.14). The dimension of ρ should be $q-1$ by Proposition 2.22. Hence, it is convenient to take V as the vector space of all functions $K^\times \to \mathbb{C}$.

The definition of $\mathrm{Res}^G_P\,\rho$ is motivated by the fact proved in Proposition 2.22 that it should be equal to π. Identifying the subgroup A of P with $K^\times$ and using the identity

$$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha & \beta \\ 0 & 1 \end{bmatrix},$$

we are led to define

$$\left(\rho\left(\begin{bmatrix} \alpha & \beta \\ 0 & 1 \end{bmatrix}\right) f\right)(x) = \psi(\beta x) f(\alpha x).$$

Further, we would like to define that ρ coincides with ν on D:

$$\left(\rho\left(\begin{bmatrix}\delta & 0\\ 0 & \delta\end{bmatrix}\right) f\right)(x) = \nu(\delta) f(x).$$

It follows that we must define ρ on B by

$$\left(\rho\left(\begin{bmatrix}\alpha & \beta\\ 0 & \delta\end{bmatrix}\right) f\right)(x) := \nu(\delta)\psi\left(\beta\delta^{-1}x\right) f\left(\alpha\delta^{-1}x\right). \tag{2.16}$$

A straightforward calculation shows that ρ is indeed a homomorphism of B into $\operatorname{Aut} V$.

In order to define $\rho(w')$, we define a function $j\colon K^\times \to \mathbb{C}$ by

$$j(u) := \frac{1}{q} \sum_{\substack{\mathrm{N}\, t = u\\ t\in L^\times}} \psi\left(t + \bar{t}\right) \nu(t) \tag{2.17}$$

and prove that it satisfies the following two identities.

Lemma 2.33. For $u \in K^\times$,

$$\sum_{v\in K^\times} j(uv) j(v) \nu\left(v^{-1}\right) = \begin{cases} \nu(-1) & \text{if } u = 1,\\ 0 & \text{if } u \neq 1.\end{cases}$$

Proof. We start from the left-hand side. Letting $L(u)$ denote the left-hand side,

$$\begin{aligned} L(u) &= \sum_{v\in K^\times} j(uv) j(v)\nu\left(v^{-1}\right)\\ &= \sum_{v\in K^\times} q^{-2} \sum_{\substack{\mathrm{N}\, t = uv\\ \mathrm{N}\, s = v}} \psi\left(t + \bar{t} + s + \bar{s}\right)\nu(ts)\nu\left(v^{-1}\right)\\ &= q^{-2} \sum_{v\in K^\times} \sum_{\substack{\mathrm{N}\, t = u \,\mathrm{N}\, s\\ \mathrm{N}\, s = v}} \psi\left(t + \bar{t} + s + \bar{s}\right)\nu\left(ts\,\mathrm{N}\, s^{-1}\right)\\ &= q^{-2} \sum_{s\in L^\times} \sum_{\mathrm{N}\, t = u\,\mathrm{N}\, s} \psi\left(t + \bar{t} + s + \bar{s}\right)\nu\left(t\bar{s}^{-1}\right). \end{aligned} \tag{2.18}$$

Let $\lambda := t\bar{s}^{-1}$. Then substituting $t = \bar{s}\lambda$ in (2.18), we have

$$\begin{aligned} L(u) &= q^{-2} \sum_{s\in L^\times} \sum_{\mathrm{N}\,\lambda = u} \psi\left(s(1+\lambda) + \bar{s}(1+\bar{\lambda})\right)\nu(\lambda)\\ &= q^{-2} \sum_{\mathrm{N}\,\lambda = u} \nu(\lambda) \sum_{s\in L^\times} \psi\left(s(1+\lambda) + \bar{s}(1+\bar{\lambda})\right). \end{aligned} \tag{2.19}$$

For a fixed λ, the function $\psi\left(s(1+\lambda) + \bar{s}(1+\bar{\lambda})\right)$ is a character of L^+. If $\lambda \neq -1$, then this is not the unit character, because by Corollary 2.32 the map $s \mapsto s(1+\lambda) + \bar{s}(1+\bar{\lambda})$ maps L onto K and ψ is not the unit character. It follows that

$$\sum_{s\in L^\times} \psi\left(s(1+\lambda) + \bar{s}(1+\bar{\lambda})\right) = -1.$$

If $\lambda = -1$, we have

$$\sum_{s\in L^\times} \psi\left(s(1+\lambda) + \bar{s}(1+\bar{\lambda})\right) = q^2 - 1.$$

We now distinguish between the two cases and suppose first that $u = 1$. Then (2.19) is equal to

$$L(u) = q^{-2} \sum_{\substack{\mathrm{N}\,\lambda=1 \\ \lambda\neq-1}} \nu(\lambda) \sum_{s\in L^\times} \psi\left(s(1+\lambda) + \overline{s}(1+\overline{\lambda})\right) + q^{-2}\nu(-1)\left(q^2-1\right) \tag{2.20}$$

$$= q^{-2} \sum_{\substack{\mathrm{N}\,\lambda=1 \\ \lambda\neq-1}} (-\nu(\lambda)) + \nu(-1)q^{-2}\left(q^2+1\right). \tag{2.21}$$

Using Lemma 2.30, we may continue this chain of equalities by

$$L(u) = q^{-2}\nu(-1) + \nu(-1)q^{-2}\left(q^2+1\right) = \nu(-1),$$

as desired.

Now suppose that $u \neq 1$. Then $\mathrm{N}\,\lambda = u$ implies $\lambda \neq -1$. Hence, (2.19) is equal in this case to

$$q^{-2} \sum_{\mathrm{N}\,\lambda=u} (-\nu(\lambda)) = 0$$

by Lemma 2.30, as desired. ∎

Lemma 2.34. For $x, y \in K^\times$,

$$\sum_{v\in K^\times} j(xv)j(yv)\nu\left(v^{-1}\right)\psi(v) = \nu(-1)\psi(-x-y)j(xy).$$

Proof. We start again from the left-hand side. Let $x, y \in K^\times$; then letting $L(x, y)$ denote the left-hand side,

$$\begin{aligned} L(x,y) &= \sum_{v\in K^\times} j(xv)j(yv)\nu\left(v^{-1}\right)\psi(v) \\ &= q^{-2} \sum_{v\in K^\times} \sum_{\substack{\mathrm{N}\,t=xv \\ \mathrm{N}\,s=yv}} \psi\left(t+\overline{t}+s+\overline{s}\right)\nu(ts)\nu\left(v^{-1}\right)\psi(v) \\ &= q^{-2} \sum_{v\in K^\times} \sum_{\substack{\mathrm{N}\,t=xv \\ \mathrm{N}\,s=yv}} \psi\left(t+\overline{t}+s+\overline{s}+v\right)\nu\left(tsv^{-1}\right). \end{aligned} \tag{2.22}$$

The condition $\mathrm{N}\,s = yv$ implies that $tsv^{-1} = yt\overline{s}^{-1}$. Define therefore $\lambda := yt\overline{s}^{-1}$. In addition, $\mathrm{N}\,t = xv$ implies $\mathrm{N}\,\lambda = xy$. Also,

$$t+\overline{t}+s+\overline{s}+v = y^{-1}(s+y+\lambda)\overline{(s+y+\lambda)} - y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)}.$$

Substituting this all in (2.22) gives

$$\begin{aligned} L(x,y) &= q^{-2} \sum_{v\in K^\times} \sum_{\substack{\mathrm{N}\,s=yv \\ \mathrm{N}\,\lambda=xy}} \psi\left(y^{-1}(s+y+\lambda)\overline{(s+y+\lambda)} - y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)}\right)\nu(\lambda) \\ &= q^{-2} \sum_{s\in L^\times} \sum_{\mathrm{N}\,\lambda=xy} \psi\left(y^{-1}(s+y+\lambda)\overline{(s+y+\lambda)} - y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)}\right)\nu(\lambda) \\ &= q^{-2} \sum_{\mathrm{N}\,\lambda=xy} \psi\left(-y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)}\right)\nu(\lambda) \sum_{s\in L^\times} \psi\left(y^{-1}(s+y+\lambda)\overline{(s+y+\lambda)}\right). \end{aligned} \tag{2.23}$$

Let us develop the inner sums

$$\begin{aligned}
\sum_{s\in L^\times} \psi\left(y^{-1}(s+y+\lambda)\overline{(s+y+\lambda)}\right) &= \sum_{\substack{r\in L\\ r\neq y+\lambda}} \psi\left(y^{-1}r\overline{r}\right)\\
&= \sum_{r\in L^\times} \psi\left(y^{-1}r\overline{r}\right) + 1 - \psi\left(y^{-1}(y+\lambda)\overline{(y+\lambda)}\right)\\
&= (q+1)\sum_{u\in K^\times} \psi\left(y^{-1}u\right) + 1 - \psi\left(y^{-1}(y+\lambda)(y+\overline{\lambda})\right)\\
&= -(q+1) + 1 - \psi\left(y^{-1}(y+\lambda)(y+\overline{\lambda})\right).
\end{aligned}$$

We have used the fact that $\ker \mathrm{N}$ consists of $q+1$ elements. Substituting this into (2.23), we obtain that (2.23) is equal to

$$\begin{aligned}
L(x,y) &= q^{-2}\sum_{\mathrm{N}\,\lambda=xy} \psi\left(-y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)}\right)\nu(\lambda)\left(-q-\psi\left(y^{-1}(y+\lambda)(y+\overline{\lambda})\right)\right)\\
&= q^{-1}\sum_{\mathrm{N}\,\lambda=xy} \psi\left(-y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)}\right)\nu(\lambda)\\
&\quad - q^{-2}\sum_{\mathrm{N}\,\lambda=xy} \psi\left(-y\left(1+y^{-1}\lambda\right)\overline{\left(1+y^{-1}\lambda\right)} + y^{-1}(y+\lambda)(y+\overline{\lambda})\right).
\end{aligned} \tag{2.24}$$

In order to compute the two sums, note that under the assumption $\lambda\overline{\lambda} = xy$ we have

$$-y\left(1+y^{-1}\lambda\right)\left(1+y^{-1}\overline{\lambda}\right) = -y - x - (\lambda+\overline{\lambda}),$$

and

$$-y\left(1+y^{-1}\lambda\right)\left(1+y^{-1}\overline{\lambda}\right) + y^{-1}(y+\lambda)(y+\overline{\lambda}) = 0.$$

Hence, (2.24) is equal to

$$\begin{aligned}
L(x,y) &= -q^{-1}\psi(-x-y)\sum_{\mathrm{N}\,\lambda=xy}\psi\left(-\lambda-\overline{\lambda}\right)\nu(\lambda) - q^{-2}\sum_{\mathrm{N}\,\lambda=xy}\nu(\lambda)\\
&= -q^{-1}\psi(-x-y)\nu(-1)\sum_{\mathrm{N}\,\lambda=xy}\psi\left(\lambda+\overline{\lambda}\right)\nu(\lambda)\\
&= \nu(-1)\psi(-x-y)j(xy),
\end{aligned}$$

as desired. ■

Having proved the above identities, we consider an $f \in V$ and define $\rho(w')f$ by

$$\left(\rho(w')f\right)(y) := \sum_{x\in K^\times} \nu\left(x^{-1}\right) j(yx) f(x). \tag{2.25}$$

Our task now is to prove that this definition of $\rho(w')$ together with (2.16) is compatible with the identities (2.12), (2.13), and (2.14).

Indeed, it is convenient to write (2.12) in the form

$$w'\begin{bmatrix}\alpha & 0\\ 0 & \delta\end{bmatrix} = \begin{bmatrix}\delta & 0\\ 0 & \alpha\end{bmatrix} w'.$$

A straightforward calculation shows that the two automorphisms obtained by acting with ρ on both sides of the equation operate in the same way on every element $f \in V$.

In order to show that ρ preserves identity (2.13), we compute for an $f\in V$ that

$$\begin{aligned}(\rho(w')\rho(w')f)(z) &= \sum_{x\in K^\times}\nu\left(x^{-1}\right)j(zx)(\rho(w')f)(x)\\ &= \sum_{x\in K^\times}\nu\left(x^{-1}\right)j(zx)\sum_{y\in K^\times}\nu\left(y^{-1}\right)j(xy)f(x)\\ &= \sum_{y\in K^\times}\nu\left(y^{-1}\right)f(y)\sum_{x\in K^\times}j(xy)j(zx)\nu\left(x^{-1}\right). \end{aligned} \tag{2.26}$$

Changing variables by $zx=c$ and $xy=uv$, (2.26) is equal to

$$\sum_{u\in K^\times}\nu\left(y^{-1}\right)f(uz)\nu(z)\sum_{v\in K^\times}j(uv)j(v)\nu\left(v^{-1}\right)=\nu\left(z^{-1}\right)\nu(z)\nu(-1)f(z)=\left(\rho\left(\begin{bmatrix}-1&0\\0&-1\end{bmatrix}\right)f\right)(z)$$

by (2.16) and Lemma 2.33.

Finally, we have to prove that ρ preserves relation (2.14). This is done by rewriting it as

$$w'\begin{bmatrix}1&1\\0&1\end{bmatrix}w'=\begin{bmatrix}-1&1\\0&-1\end{bmatrix}w'\begin{bmatrix}1&-1\\0&1\end{bmatrix},$$

making the necessary computations as above, and using Lemma 2.34. The actual computations raise no significant problem, so we omit them.

We have thus proved that starting from a non-decomposable character ν of $L^\times$, there exists a representation $\rho=\rho_\nu$ of G that acts on B via (2.16) and on w' via (2.25). For later references, let us also describe the action of ρ on the element

$$g:=\begin{bmatrix}\alpha&\beta\\\gamma&\delta\end{bmatrix} \tag{2.27}$$

of G, where $\gamma\neq 0$. We use the identity

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

and apply (2.16) and (2.25) to compute the action of $\rho(g)$ on a function $f\colon K^\times\to\mathbb{C}$ as

$$\begin{aligned}(\rho(g)f)(y) &= \nu(-\gamma)\psi\left(\alpha\gamma^{-1}y\right)\left(\rho(w')\rho\left(\begin{bmatrix}1&\gamma^{-1}\delta\\0&1\end{bmatrix}\right)f\right)\left(\left(\beta-\alpha\gamma^{-1}\delta\right)(-\gamma)^{-1}y\right)\\ &= \nu(-\gamma)\psi\left(\alpha\gamma^{-1}y\right)\sum_{x\in K^\times}\nu\left(x^{-1}\right)j\left(\left(\alpha\gamma^{-1}\delta-\beta\right)\gamma^{-1}yx\right)\left(\rho\left(\begin{bmatrix}1&\gamma^{-1}\delta\\0&1\end{bmatrix}\right)f\right)(x)\\ &= \nu(-\gamma)\psi\left(\alpha\gamma^{-1}y\right)\sum_{x\in K^\times}\nu\left(x^{-1}\right)j\left(\gamma^{-2}yx\det g\right)\psi\left(\gamma^{-1}\delta x\right)f(x)\\ &= \nu(-\gamma)\psi\left(\alpha\gamma^{-1}y\right)\sum_{x\in K^\times}\nu\left(x^{-1}\right)\psi\left(\gamma^{-1}\delta x\right)f(x)\left(q^{-1}\right)\sum_{\substack{t\bar{t}=\gamma^{-2}yx\det g\\ t\in L^\times}}\psi\left(t+\bar{t}\right)\nu(t).\end{aligned}$$

Substituting $t=-\gamma^{-1}xu$,

$$(\rho(g)f)(y)=\sum_{x\in K^\times}\left[q^{-1}\psi\left(\frac{\alpha y+\delta x}{\gamma}\right)\sum_{\substack{u\bar{u}=yx^{-1}\det g\\ u\in L^\times}}\psi\left(-\frac{x}{\gamma}(u+\bar{u})\right)\nu(u)\right]f(x).$$

We have therefore proved that for an element g given by (2.27),

$$(\rho(g)f)(y)=\sum_{x\in K^\times}k(y,x;g)f(x),$$

where

$$k(y,x;g) := \frac{1}{q}\psi\left(\frac{\alpha y+\delta x}{\gamma}\right)\sum_{\substack{u\overline{u}=yx^{-1}\det g\\ u\in L^\times}}\psi\left(-\frac{x}{\gamma}(u+\overline{u})\right)\nu(u).$$

2.9 The correspondence between ν and ρ_ν

Proposition 2.35. The following are true.

(a) If ν is a non-decomposable character of $L^\times$, then the representation ρ_ν of G defined in section 2.8 is cuspidal.

(b) If ν and ν' are non-decomposable character of $L^\times$, then ρ_ν is isomorphic to $\rho_{\nu'}$ if and only if ν is conjugate to ν' over K.

Proof. Here we go.

(a) We have defined ρ_ν such that its restriction to P is equal to π.[2] Hence, ρ_ν is cuspidal by Proposition 2.22.

(b) Let $\rho := \rho_\nu$, $\rho' := \rho_{\nu'}$, $j := j_\nu$, and $j_{\nu'} := j'$. If ν' is conjugate to ν, then j' is equal to j, as follows from definition (2.17). Hence, $\rho = \rho'$.

Conversely, suppose that ρ' is isomorphic to ρ. Then there exists an automorphism θ of V (which is the vector space of all functions $f\colon K^\times \to \mathbb{C}$) such that

$$\rho'(g) = \theta\rho(g)\theta^{-1} \qquad \text{for all } g\in G. \tag{2.28}$$

In particular, (2.28) is valid for every $g \in P$. However, $\operatorname{Res}^G_P \rho = \pi = \operatorname{Res}^G_P \rho'$, and π is irreducible. Hence, by Schur's lemma, θ is multiplication by a scalar. In particular, θ commutes with every automorphism of V. Hence, (2.28) implies that $\rho'(g) = \rho(g)$ for every $g\in G$.

It follows that for every $\delta, y \in K^\times$ and $f\in V$,

$$\nu'(\delta)f\left(\delta^{-1}y\right) = \left(\rho'\left(\begin{bmatrix}1&0\\0&\delta\end{bmatrix}\right)f\right)(y) = \left(\rho\left(\begin{bmatrix}1&0\\0&\delta\end{bmatrix}\right)f\right)(y) = \nu(\delta)f\left(\delta^{-1}y\right).$$

Hence,

$$\nu'(\delta) = \nu(\delta) \qquad \text{for every } \delta\in K^\times. \tag{2.29}$$

Further, $\rho'(w') = \rho(w')$; hence,

$$\sum_{x\in K^\times}\nu'\left(x^{-1}\right)j(yx)f(x) = \sum_{x\in K^\times}\nu\left(x^{-1}\right)j'(yx)f(x)$$

for every $y\in K^\times$ and every $f\in V$. Using (2.29), this implies that $j'(u) = j(u)$ for every $u\in K^\times$. This means that

$$\sum_{\mathrm{N}\,t=u}\psi\left(t+\overline{t}\right)\nu'(t) = \sum_{\mathrm{N}\,t=u}\psi\left(t+\overline{t}\right)\nu(t). \tag{2.30}$$

Let $\delta\in K^\times$ and replace the variable t in (2.30) by δt. Using (2.29) to cancel $\nu(\delta)$ on both sides, we have

$$\sum_{t\overline{t}=v}\psi\left(\delta(t+\overline{t})\right)\nu'(t) = \sum_{t\overline{t}=v}\psi\left(\delta(t+\overline{t})\right)\nu(t)$$

[2] By definition, $\operatorname{Res}^G_U \rho_\nu = \psi$, so $\left(\operatorname{Res}^G_P \rho_\nu, \pi\right) = \left(\operatorname{Res}^G_P \rho_\nu, \operatorname{Ind}^P_U \psi\right) = \left(\operatorname{Res}^G_U \rho_\nu, \psi\right) = 1$. But $\dim \operatorname{Res}^G_P \rho_\nu = \dim \rho_\nu = q-1 = \dim \pi$, so we have equality.

for every $v,\delta\in K^\times$. This can be rewritten as

$$\sum_{t\bar{t}=v}{}' \left(\nu'(t)+\nu'(\bar{t})-\nu(t)-\nu(\bar{t})\right)\psi\left(\delta(t+\bar{t})\right)=0, \tag{2.31}$$

where the prime over the summation symbols indicates that for every $t\in L^\times$ such that $t\bar{t}=v$, only one pair out of the two $(t,\bar{t}),(\bar{t},t)$ contributes a summand to the summation.

Now let x be an element of K. Then there exists a $t\in L$ such that $t+\bar{t}=x$ and $t\bar{t}=v$. This element is a solution to the quadratic equation $X^2-xX+v=0$. (We repeat that L is the unique quadratic extension of K.) The other solution of the equation is obviously $\bar{t}$. The expression $a_x:=\nu'(t)+\nu'(\bar{t})-\nu(t)-\nu(\bar{t})$ is therefore well-defined, and (2.31) can be rewritten as

$$\sum_{t\bar{t}=v}{}' a_x\psi(\delta x)=0.$$

If $x_1\neq x_2$, then the characters $\delta\mapsto\psi(\delta x_1)$ and $\delta\mapsto\psi(\delta x_2)$ of K^+ are distinct. Hence, by Artin's lemma, $a_x=0$ for every $x\in K$. This means that

$$\nu'(t)+\nu'(\bar{t})=\nu(t)+\nu(\bar{t})\qquad\text{for all } t\in L^\times.$$

In addition,

$$\nu'(t)\nu'(\bar{t})=\nu(t)\nu(\bar{t})\qquad\text{for all } t\in L^\times$$

by (2.29). Hence, the pairs $\left(\nu'(t),\nu'(\bar{t})\right)$, $\left(\nu(t),\nu(\bar{t})\right)$ are the solutions of the same quadratic equation over K. Hence,

$$\left\{\nu'(t),\nu'(\bar{t})\right\}=\left\{\nu(t),\nu(\bar{t})\right\}\qquad\text{for all } t\in L^\times. \tag{2.32}$$

In particular, (2.32) is true for a generator t_0 of the cyclic group $L^\times$. Suppose, for example, that $\nu(t_0)=\nu'(t_0)$. Then $\nu(t)=\nu'(t)$ for every $t\in L^\times$. If $\nu'(t_0)=\nu(\overline{t_0})$, then $\nu'=\overline{\nu}$.

We have therefore proved that ν' is conjugate to ν over K. ■

At this point, we would like to indicate an interesting duality between conjugacy classes of G on one hand and irreducible representations of G on the other hand. The elements α of $K^\times$ correspond bijectively to the pair of conjugacy classes $(c_1(\alpha),c_2(\alpha))$ (see section 1.5), and there are $q-1$ of them. Dually, the characters μ_1 of $K^\times$ correspond bijectively to pairs $\left(\rho_{(\mu_1,\mu_1)},\rho'_{(\mu_1,\mu_1)}\right)$ of irreducible representations of dimensions q and 1 respectively (see Theorem 2.18), and there are $q-1$ of them. Further, the pairs of elements α,β of $K^\times$ with $\alpha\neq\beta$ correspond to the conjugacy classes $c_3(\alpha,\beta)$, and there are $\frac{1}{2}(q-1)(q-2)$ of them. Dually, the pairs of characters μ_1,μ_2 of $K^\times$ with $\mu_1\neq\mu_2$ correspond to the irreducible representations $\rho_{(\mu_1,\mu_2)}$ of G of dimension $q+1$, and there are also $\frac{1}{2}(q-1)(q-2)$ of them. Finally, the elements λ of $L^\times\setminus K^\times$ correspond to the conjugacy classes $c_4(\lambda)$, whereas the characters ν of $L^\times$ that do not come from characters of $K^\times$ (i.e., non-decomposable) correspond to the cuspidal representations ρ_ν of G. In both sets that are $\frac{1}{2}\left(q^2-q\right)$ elements.

We summarize these data in the following table.

elements of $L^\times$	conj. classes	chars. of $L^\times, K^\times$	irr. repr. of G	dim. of repr.	no. of elements
$\alpha\in K^\times$	$c_1(\alpha)$	$\mu_1\in X(K^\times)$	$\rho'_{(\mu_1,\mu_1)}$	1	$q-1$
	$c_2(\alpha)$		$\rho_{(\mu_1,\mu_1)}$	q	$q-1$
$\alpha,\beta\in K^\times$ $\alpha\neq\beta$	$c_3(\alpha,\beta)$	$\mu_1,\mu_2\in X\left(K^\times\right)$ $\mu_1\neq\mu_2$	$\rho_{(\mu_1,\mu_2)}$	$q+1$	$\frac{1}{2}(q-1)(q-2)$
$\lambda\in L^\times\setminus K^\times$	$c_4(\lambda)$	$\nu\in X\left(L^\times\right)\setminus X\left(K^\times\right)$	ρ_ν	$q-1$	$\frac{1}{2}\left(q^2-q\right)$

2.10 The small Weil group and the small reciprocity law

Let F/E be a finite Galois extension. Its Galois group, $\mathrm{Gal}(F/E)$ acts on the multiplicative group $F^\times$ of F. Denote by $W(F/E):=\mathrm{Gal}(F/E)\ltimes F^\times$ the semi-direct product of $\mathrm{Gal}(F/E)$ by $F^\times$. It consists of all pairs

(x, σ) where $x \in F^\times$ and $\sigma \in \mathrm{Gal}(F/E)$. Multiplication is given by the formula

$$(x, \sigma) \cdot (y, \tau) \coloneqq (x \cdot \sigma y, \sigma\tau);$$

the one element is $(1, 1)$, and the inverse is given by

$$(x, \sigma)^{-1} \coloneqq \left(\sigma^{-1}x^{-1}, \sigma^{-1}\right).$$

The map $x \mapsto (x, 1)$ is an embedding of $F^\times$ in $W(F/E)$. We identify $F^\times$ with its image. Then $F^\times$ is normal in $W(F/E)$ and its index is equal to the degree $[F : E]$.

The group $W(F/E)$ is in general not abelian. A typical commutator is

$$(x, \sigma)(y, \tau)(x, \sigma)^{-1}(y, \tau)^{-1} = \left(x \cdot \sigma(y) \cdot \sigma\tau\sigma^{-1}\left(x^{-1}\right) \cdot \sigma\tau\sigma^{-1}\tau^{-1}\left(y^{-1}\right), \sigma\tau\sigma^{-1}\tau^{-1}\right).$$

If in addition $\mathrm{Gal}(F/E)$ is abelian, then this formula simplifies to

$$(x, \sigma)(y, \tau)(x, \sigma)^{-1}(y, \tau)^{-1} = \left(x \cdot \sigma(y) \cot\tau\left(x^{-1}\right) \cdot y, 1\right). \tag{2.33}$$

We now restrict our attention to the case where $E = K$ is our field with q elements and $F = L$ its unique quadratic extension. The Galois group $\mathrm{Gal}(L/K)$ consists of two elements, a conjugation, the action of which is denoted by a bar, and the identity automorphism. In this case, $W(L/K)$ is called the small Weil group of the extension L/K. It is a finite group having $w(q-1)$ elements, and it can be described as the free group generated by $L^\times$ and with the relations

$$\varphi^2 = 1 \qquad \text{and} \qquad x\varphi = \varphi\overline{x} \text{ for } x \in L^\times. \tag{2.34}$$

Now, $W(L/K)$ contains the abelian normal subgroup $L^\times$ of index 2. Hence, its irreducible representations are of degree ≤ 2.

We would like to establish a correspondence between the two-dimensional representations of $W(L/K)$ (not only the irreducible ones) and the higher-dimensional representations of G. As a first step toward this goal, let us compute the number of characters of $W(L/K)$. This number is equal to the index of the commutator subgroup $W(L/K)^c$ of $W(L/K)$. Indeed, applying (2.33) to the four possible pairs (σ, τ), one concludes that

$$W(L/K)^c = \left\{z\overline{z} : z \in L^\times\right\}. \tag{2.35}$$

By Corollary 2.26, the right-hand side is equal to $\{x \in L^\times : \mathrm{N}\, x = 1\}$; hence, $[W(L/K) : W(L/K)^c] = 2(q-1)$ by Lemma 2.25. We have therefore proved the following.

Lemma 2.36. The group $W(L/K)$ has $2(q-1)$ characters.

Consider now a two-dimensional representation τ of $W(L/K)$ its restriction to $L^\times$ decomposes into a direct sum of two characters. Let ν be one of them.

Lemma 2.37. Fix everything as above.

(a) If ν is non-decomposable, then $\mathrm{Res}_{L^\times} \tau = \nu \oplus \overline{\nu}$.

(b) ν is non-decomposable if and only if τ is irreducible.

Proof. By construction, there exists a vector $0 \neq v_1 \in V_\tau$ such that

$$\tau(x)v_1 = \nu(x)v_1 \qquad \text{for all } x \in L^\times. \tag{2.36}$$

Let $v_1' \coloneqq \tau(\varphi)v_1$. Then the relation $x\varphi = \varphi\overline{x}$ implies

$$\tau(x)v_1' = \nu(\overline{x})v_1' \qquad \text{for all } x \in L^\times. \tag{2.37}$$

Hence, $\overline{\nu}$ is also a component of $\mathrm{Res}_{L^\times} \tau$. If $\nu \neq \overline{\nu}$, then $\mathrm{Res}_{L^\times} \tau = \nu \oplus \overline{\nu}$, and (a) is proved.

In order to prove (b), suppose first that $\tau = \tau_1 \oplus \tau_2$ is reducible. Then the τ_i are characters of $W(L/K)$ and since $x\overline{x}^{-1} \in W(L/K)^c$ by (2.35), we have $\tau_i(x) = \tau_i(\overline{x})$. It follows that $\operatorname{Res}_{L^\times} \tau_i$ are decomposable characters of $L^\times$. Also, ν must be equal to one of them; hence, ν is also decomposable.

Conversely, suppose that $\nu = \overline{\nu}$. There are two possibilities. Either $\nu_1' = \nu(\varphi)v_1$ is a multiple of v_1, or v_1 and v_1' are linearly independent. In the first case, $\nu\colon L^\times \cup \{\varphi\} \to \mathbb{C}$ is a map which is multiplicative on $L^\times$ and agrees with the defining relations (2.34) of $W(L/K)$. Hence, ν can be extended to a character of $W(L/K)$ that happens to be a component of τ by (2.36) and because $v_1' = \tau(\varphi)v_1$. This implies that τ is reducible.

In the second case, v_1 and v_1' generate V_τ. Then (2.36) and (2.37) imply that $\tau(x)v = \nu(x)v$ for every $x \in L^\times$ and $v \in V_\tau$. Let ν_2 be an eigenvector of $\tau(\varphi)$. Then because $\tau(x)v_2 = \nu(x)v_2$, we prove as above that v_2 is an eigenvector of $W(L/K)$. This implies that τ is reducible. ∎

Now consider more closely the case where $\tau = \tau_1 \oplus \tau_2$ is a reducible representation of $W(L/K)$. By Lemma 2.37, there exist characters μ_1 and μ_2 of $K^\times$ such that $\tau_i(x) = \mu_i(\mathrm{N}\, x)$ for $i = 1, 2$ and for every $x \in L^\times$. We may therefore write $\tau = \tau_{(\mu_1,\mu_2)}$. The pair (μ_1, μ_2) defines a character μ of B (by (2.6)). If $\mu_1 = \mu_2$, then $\widehat{\mu} = \rho_{(\mu_1,\mu_1)} \oplus \rho'_{(\mu_1,\mu_1)}$. We correspond τ to $\rho_{(\mu_1,\mu_1)}$. If $\mu_1 \neq \mu_2$, then $\widehat{\mu} = \rho_{(\mu_1,\mu_2)}$. We correspond τ to $\rho_{(\mu_1,\mu_2)}$.

This correspondence is injective.[3] Indeed, starting from a pair of characters (μ_1, μ_2) of $K^\times$, we define characters τ_1, τ_2 of $W(L/K)$ by $\tau_i(x) := \mu_i(\mathrm{N}\, x)$ and $\tau_i(\varphi) = 1$. This definition makes sense because it is compatible with the relations (2.34). Then $\tau_{(\mu_1,\mu_2)} = \tau_1 \oplus \tau_2$ is a reducible two-dimensional representation of $W(L/K)$, and $\rho_{(\mu_1,\mu_2)}$ corresponds to $\tau_{(\mu_1,\mu_2)}$.

Finally, let ν be a non-decomposable character of $L^\times$. Define a two-dimensional representation τ_ν of $W(L/K)$ by

$$\tau_\nu(x) := \begin{bmatrix} \nu(x) & 0 \\ 0 & \nu(\overline{x}) \end{bmatrix} \text{ for } x \in L^\times, \qquad \text{and} \qquad \tau_\nu(\varphi) := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Then $\operatorname{Res}_{L^\times} \tau_\nu = \nu \oplus \overline{\nu}$; hence, τ_ν is irreducible. If ν' is an additional non-decomposable character of $L^\times$, then $\tau_\nu = \tau_{\nu'}$ if and only if ν' is conjugate to ν. It follows that $W(L/K)$ has exactly $\frac{1}{2}\left(q^2 - q\right)$ irreducible representations of the form τ_ν. Taking into account Lemma 2.37, we deduce from the identity

$$2\left(q^2 - 1\right) = 2^2 \cdot \frac{1}{2}\left(q^2 - 1\right) + 1^2 \cdot 2(q - 1)$$

that the τ_ν are all the irreducible representations of $W(L/K)$.

Adding Proposition 2.35 to the above arguments, we have proved the following reciprocity law.

Theorem 2.38. There exists an injective correspondence between the two-dimensional representations τ of the Weil group $W(L/K)$ and the higher-dimensional representations of $\mathrm{GL}(2, K)$.

Using the above notation, the correspondence may be described as follows.

(a) For reducible τ: if (μ_1, μ_2) is a pair of characters $K^\times$, then $\tau_{(\mu_1,\mu_2)}$ corresponds to $\rho_{(\mu_1,\mu_2)}$.

(b) For irreducible τ: if ν is a non-decomposable character of $L^\times$, then τ_ν corresponds to ρ_ν.

[3] Piatetski-Shapiro claims that this correspondence is bijective, but the following description of the inverse map only hits reducible representations τ with $\tau(\varphi) = 1$.

THEME 3

Γ-FUNCTIONS AND BESSEL FUNCTIONS

3.1 Whittaker models

Recall that we have fixed a non-unit character ψ of K^+, identified with a character of U and found that $\pi := \operatorname{Ind}_U^P$ is an irreducible representation of dimension $q-1$. If χ is a character of g, then by the Frobenius reciprocity theorem,

$$\left(\chi, \operatorname{Ind}_U^G \psi\right)_G = \left(\chi, \operatorname{Ind}_B^G \pi\right)_G = \left(\operatorname{Res}_B^G \chi, \pi\right)_B = 0.$$

Hence, all the irreducible components of $\operatorname{Ind}_U^G \psi$ are of dimension > 1. Each one of them appears in multiplicity 1 by Proposition 2.23. On the other hand, if we sum up the dimensions of all higher-dimensional representations of G, we find that it is equal to $\dim \operatorname{Ind}_U^G \psi = (q-1)^2(q+1)$. This follows from the table in section 2.9 and from the following identity:

$$\frac{1}{2}\left(q^2-q\right)(q-1) + (q-1)q + \frac{1}{2}(q-1)(q-2)(q+1) = (q-1)^2(q+1).$$

We conclude therefore the following.

Theorem 3.1. The representation $\operatorname{Ind}_U^G \psi$ is equal to the direct sum of all higher-dimensional irreducible representations of G, each with multiplicity 1.

Note that the same conclusion can be drawn from the following lemma, which his proved, however, without explicit use of the finiteness of K.

Lemma 3.2. Let ρ be an irreducible representation of G of dimension > 1. Then the following are true.

(a) $\operatorname{Res}_P^G V_\rho = \operatorname{Res}_P^B J(V_\rho) \oplus V_\pi$;

(b) $\dim J(V_\rho) = \dim \rho - (q-1)$;

(c) The multiplicity of ρ in $\operatorname{Ind}_U^G \psi$ is equal to 1.

Proof. If $\dim \rho = q-1$, i.e., if ρ is cuspidal, then $J(V_\rho) = 0$, and $\operatorname{Res}_P^G V_\rho = V_\pi$ by Proposition 2.22. Formula (a) is therefore true in this case.

If $\dim \rho \geq q$, i.e., if ρ is non-cuspidal, then $J(V_\rho) \neq 0$ and there exists a character μ of B and a representation ρ' of G such that $\widehat{\mu} = \operatorname{Ind}_P^G \mu = \rho' \oplus \rho$ and $\dim \rho' \leq 1$. Further, by Lemma 2.13, we have $\operatorname{Res}_P^G V_{\widehat{\mu}} = \operatorname{Res}_P^B J(V_{\widehat{\mu}}) \oplus V_\pi$; hence,

$$\operatorname{Res}_P^G V_{\rho'} \oplus \operatorname{Res}_P^G V_\rho = \operatorname{Res}_P^G J(V_{\rho'}) \oplus \operatorname{Res}_P^G J(V_\rho) \oplus V_\pi. \tag{3.1}$$

Now, V_π does not contain any one-dimensional P-modules because $\dim V_\pi = q - 1 > 1$ and V_π is P-irreducible. It follows that $V_\pi \subseteq \operatorname{Res}_P^G V_\rho$. Further, $\operatorname{Res}_P^G J(V_\rho)$ is certainly contained in V_ρ, and by Lemma 2.7, it decomposes into a direct sum of one-dimensional P-subspaces. Hence, $\operatorname{Res}_P^B V_\pi \cap \operatorname{Res}_P^B J(V_\rho) = 0$, and thus the right-hand side of (a) is contained in its left-hand side. If $\dim \rho = q$, then because the dimension of the right-hand side of (a) is $\geq 1 + (q-1)$, we may conclude the equality. If $\dim \rho = q+1$, then $\rho' = 0$, and (3.1) coincides with (a).

Note that we have also proved that the multiplicity of π in $\operatorname{Res}_P^G \rho$ is 1. Hence, by the Frobenius reciprocity theorem the multiplicity of ρ in $\operatorname{Ind}_U^G \psi = \operatorname{Ind}_B^G \pi$ is 1. ∎

Recall that $\operatorname{Ind}_U^G V_\psi$ can be identified with the space of all functions $F\colon G \to \mathbb{C}$ such that

$$F(ug) = \psi(u)F(g) \qquad \text{for all } u \in U \text{ and } g \in G.$$

The group G operates on $\operatorname{Ind}_U^G V_\psi$ by the following law:

$$(sF)(g) = F(gs).$$

If ρ is now an irreducible higher-dimensional representation of G, then V_ρ can be embedded in $\operatorname{Ind}_U^G V_\psi$. For every $v \in V_\rho$, there exist therefore a function $W_v\colon G \to \mathbb{C}$ called a *Whittaker function* of ρ such that the following rules hold:

$$\begin{aligned} W_v = 0 &\iff v = 0, \\ W_{c_1 v_1 + c_2 v_2} &= c_1 W_{v_1} + c_2 W_{v_2} && \text{for } c_1, c_2 \in \mathbb{C}, \\ W_v(ug) &= \psi(u) W_v(g) && \text{for } u \in U \text{ and } g \in G, \\ W_{\rho(s)v} &= W_v(gs) && \text{for } s, g \in G. \end{aligned}$$

The set of all functions W_v forms a G-subspace $W(\rho)$ of $\operatorname{Ind}_U^G V_\psi$ called the *Whittaker model* of ρ. By Theorem 3.1 or Lemma 3.2, this subspace is uniquely determined within $\operatorname{Ind}_U^G V_\psi$. Moreover, if ρ' is an additional higher-dimensional representation of G, then $W(\rho) \cap W(\rho') = 0$.

3.2 The Γ-function of a representation

Let ρ be a higher-dimensional irreducible representation of G. The P-decomposition

$$V_\rho = J(V_\rho) \oplus V_\pi \tag{3.2}$$

of V_ρ, obtained in Lemma 3.2, is also an A-decomposition, where we recall that

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

is the subgroup of P which is canonically isomorphic to $K^\times$. If $\dim \rho \geq$, then $\rho = \rho_{(\mu_1, \mu_2)}$ are characters of $K^\times$. By Lemma 2.7, they are the eigenvalues of A on $J(V_\rho)$. If $\dim \rho = q+1$, then $\mu_1 \neq \mu_2$ and $\dim J(V_\rho) = 2$. If $\dim \rho = q$, then $\mu_1 = \mu_2$ and $\dim J(V_\rho) = 1$. If $\dim \rho = q-1$, then $J(V_\rho) = 0$. In the first two cases we call μ_1^{-1}, μ_2^{-1}, and μ_1^{-1}, respectively, the *exceptional characters* for ρ. In the third case there are no exceptional characters. In any case, if the inverse of a character ω of $K^\times$ is not exceptional, then it is not an eigenvalue of A operating on $J(V_\rho)$ through ρ.

Lemma 3.3. If a character ω of $K^\times$ is not an exceptional character for ρ, then any two linear functionals ℓ_1 and ℓ_2 of V_ρ satisfying

$$\ell_i \left(\rho \left(\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix} \right) v \right) = \omega(x)^{-1} \ell_i(v) \qquad \text{for every } x \in K^\times \text{ and } v \in V_\rho$$

are linearly dependent.

Proof. Note $\operatorname{Res}_A^B V_\pi$ is isomorphic to the space of all functions $\varphi\colon K^\times \to \mathbb{C}$, and A acts on this space by the formula
$$\left(\rho\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)\varphi\right)(x) = \varphi(x\alpha).$$
Indeed, we may an $f \in V_\pi$ to the function φ defined by
$$\varphi(x) := f\left(\begin{bmatrix}x & 0\\ 0 & 1\end{bmatrix}\right).$$
On the other hand, the identity
$$\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix} = \begin{bmatrix}\alpha & \beta\\ 0 & 1\end{bmatrix}$$
implies that φ also determines f.

There exists now exactly one nonzero function φ (up to a multiplication by a scalar) such that $\varphi(x\alpha) = \omega(\alpha)^{-1}\varphi(x)$. This function is defined by $\varphi(x) = \omega(x)^{-1}\varphi(1)$. Using (3.2) and the assumption that the inverse ω is non-exceptional, this means that ω is an eigenvalue operating on V_ρ and the subspace of eigenvectors of A belonging to ω is one-dimensional.

Now let ζ be a generator of the cyclic group $K^\times$ and define a linear map $T\colon V_\rho \to V_\rho$ by
$$Tv = \rho\left(\begin{bmatrix}\zeta & 0\\ 0 & 1\end{bmatrix}\right)v - \omega(\zeta)^{-1}v.$$
Then
$$\ker T = \left\{v \in V_\rho : \rho\left(\begin{bmatrix}x & 0\\ 0 & 1\end{bmatrix}\right)v = \omega(x)^{-1}v \text{ for all } x \in K^\times\right\}$$
is the subspace of eigenvectors belonging to ω^{-1}. We proved that $\dim\ker T = 1$. Hence, $\dim T(V_\rho) = \dim\rho - 1$. However, $T(V) \subseteq \ker\ell_i$, and $\dim\ker\ell_i = \dim\rho - 1$. Hence, $\ker\ell_1 = T(V) = \ker\ell_2$. It follows that ℓ_1 and ℓ_2 are linearly dependent. ■

Theorem 3.4. Let ρ be a higher-dimensional irreducible representation of G, and let ω be a character of $K^\times$ which is not exceptional for ρ. Then there exists a complex number $\Gamma_\rho(\omega)$ such that for every Whittaker function W_v W_v of ρ, we have
$$\Gamma_\rho(\omega)\sum_{x\in K^\times} W_v\left(\begin{bmatrix}x & 0\\ 0 & 1\end{bmatrix}\right)\omega(x) = \sum_{x\in K^\times} W_v\left(\begin{bmatrix}0 & 1\\ x & 0\end{bmatrix}\right)\omega(x).$$

Proof. Define linear functionals ℓ_i, $i = 1, 2$ of V_ρ by
$$\ell_1(v) := \sum_{x\in K^\times} W_v\left(\begin{bmatrix}x & 0\\ 0 & 1\end{bmatrix}\right) \qquad \text{and} \qquad \ell_2(v) := \sum_{x\in K^\times} W_v\left(\begin{bmatrix}0 & 1\\ x & 0\end{bmatrix}\right)\omega(x).$$
Then
$$\ell_i\left(\rho\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)v\right) = \omega(\alpha)^{-1}\ell_i(v) \qquad \text{for } i = 1, 2$$
for every $\alpha \in K^\times$ and every $v \in V_\rho$. For example,
$$\begin{aligned}\ell_2\left(\rho\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)v\right) &= \sum_{x\in K^\times} W_{\rho\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)v}\left(\begin{bmatrix}0 & 1\\ x & 0\end{bmatrix}\right)\omega(x)\\ &= \sum_{x\in K^\times} W_v\left(\begin{bmatrix}0 & 1\\ x\alpha & 0\end{bmatrix}\right)\omega(x) = \omega(\alpha)^{-1}\sum_{y\in K^\times} W_v\left(\begin{bmatrix}0 & 1\\ y & 0\end{bmatrix}\right)\omega(y)\\ &= \omega(\alpha)^{-1}\ell_2(y).\end{aligned}$$

It follows from Lemma 3.3 that ℓ_2 is a multiple of ℓ_1 by a constant.[1] We denote this constant by $\Gamma_\rho(\omega)$. ■

The complex-valued function $\Gamma_\rho(\omega)$ defined for every non-exceptional character ω of $K^\times$ will play an important role in the computation of the character table of G.

3.3 Determination of ρ by Γ_ρ

Let ρ be a higher-dimensional representation of G. For every $v \in V_\rho$, let W_v be the corresponding Whittaker function of ρ, and let r be the homomorphism of V_ρ into the space $F(K^\times, \mathbb{C})$ of all functions $\varphi\colon K^\times \to \mathbb{C}$ defined by $r(v) := \mathrm{Res}_A^G W_v$. If we define an operation of $K^\times$ on $F(K^\times, \mathbb{C})$ by $(\alpha \cdot \varphi)(x) = \varphi(x\alpha)$ and identify A with $K^\times$, then r is also an A-homomorphism.

Lemma 3.5. The homomorphism r is surjective, and $\ker r = J(V_\rho)$.

Proof. We start by determining the kernel of r. Let $v \in J(V_\rho)$; then for every $\alpha \in K^\times$, we choose a $\beta \in K$ such that $\psi(\alpha\beta) \neq 0$. Then

$$\begin{aligned}
W_v\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) &= W_{\rho\left(\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\right)v}\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)\\
&= W_v\left(\begin{bmatrix}\alpha & \alpha\beta\\ 0 & 1\end{bmatrix}\right)\\
&= W_v\left(\begin{bmatrix}1 & \alpha\beta\\ 0 & 1\end{bmatrix}\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)\\
&= \psi(\alpha\beta) W_v\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right).
\end{aligned}$$

Hence, $W_v\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) = 0$; i.e., $v \in \ker r$.

To prove that $\ker r \subseteq J(V_\rho)$, recall again the P-decomposition $V = J(V_\rho) \oplus V_\pi$ (see Lemma 3.2). Then $V_\pi \cap \ker r$ is left-invariant by P. This follows from the decomposition $P = AU$ and from the following two computations: let $v \in V_\pi \cap \ker r$; then

$$\begin{aligned}
W_{\rho\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)v}\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) &= W_v\left(\begin{bmatrix}\alpha\alpha' & 0\\ 0 & 1\end{bmatrix}\right) = 0,\\
W_{\rho\left(\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\right)v}\left(\begin{bmatrix}\alpha & 1\\ 0 & 1\end{bmatrix}\right) &= \psi(\alpha\beta) W_v\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) = 0.
\end{aligned} \tag{3.3}$$

It follows that $V_\pi \cap \ker r = 0$ or $V_\pi \cap \ker r = V_\pi$ because V_π is P-irreducible.

Assume that $V_\pi \cap \ker r = V_\pi$. Then by the first part of the prof, $W_v(a) = 0$ for every $v \in V$ and every $a \in A$. Hence, if $g \in G$, then $W_v(G) = W_{\rho(g)v}(1) = 0$, i.e., $v = 0$, which is a contradiction. It follows that $V_\pi \cap \ker r = 0$; hence $\ker r = J(V_\rho)$. This fact implies that $\dim \operatorname{im} r = \dim V_\rho - \dim J(V_\rho) = q - 1 = \dim F(K^\times, \mathbb{C})$. Hence, $\operatorname{im} r = F(K^\times, \mathbb{C})$. ■

The center Z of G consists of the scalar matrices and is therefore canonically isomorphic to $K^\times$. The restriction of ρ to Z can therefore be identified with a character ω_P of $K^\times$, called the central character of ρ.

[1] Notably, ℓ_2 is nonzero (and hence ℓ_1 is nonzero): the proof of Lemma 3.3 gives $v \in V_\pi$ which is an eigenvector of A with eigenvalue ω^{-1}. Then we can compute $\ell_2(v) = (q-1)W_v(1)$, so $\ell_2(v) = 0$ implies $W_v(1) = 0$. However, this means $W_v(a) = W_{av}(1) = \omega^{-1}(a)W_v(1) = 0$ for any $a \in A$, so Lemma 3.5 below implies that $v \in J(V_\rho)$, so $v = 0$ because $v \in V_\pi$, which is a contradiction.

Proposition 3.6. A cuspidal representation ρ of G is uniquely determined by its Γ-function and its central character.

Proof. Let ρ and ρ' be two cuspidal representation of G. Then by Proposition 2.22, $\operatorname{Res}_P^G \rho = \pi = \operatorname{Res}_P^G \rho'$. If ρ and ρ' coincide on Z, then they coincide on B since $B = ZP$. Suppose in addition that $\Gamma_\rho = \Gamma_{\rho'}$. We have to prove that $\rho = \rho'$. The Bruhat decomposition $G = B \sqcup BwU$ implies that it suffices to show that $\rho(w) = \rho'(w)$.

Both representations ρ and ρ' are of dimension $q-1$. We can therefore assume that both of them act on the space V. For every $v \in V$, let W_v and W'_v be Whittaker functions of ρ and ρ', respectively. We know that $J(V_\rho) = J(V_{\rho'}) = 0$; hence, by Lemma 3.5 the maps $v \mapsto \operatorname{Res}_A^G W_v$ and $v \mapsto \operatorname{Res}_A^G W'_v$ are A-isomorphisms of V onto $F(K^\times, \mathbb{C})$. Hence, without loss of generality, we can assume that $\operatorname{Res}_A^G W_v = \operatorname{Res}_A^G W'_v$.[2]

Therefore, by Theorem 3.4, the assumption $\Gamma_\rho = \Gamma_{\rho'}$ implies that for every character ω of $K^\times$,

$$\sum_{x \in K^\times} W_v\left(\begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}\right) = \sum_{x \in K^\times} W'_v\left(\begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}\right).$$

This implies by Artin's lemma that

$$W_v\left(\begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}\right) = W'_v\left(\begin{bmatrix} 0 & 1 \\ x & 0 \end{bmatrix}\right) \qquad \text{for every } x \in K^\times.$$

Hence,

$$\begin{aligned}
W_{\rho(w)v}\left(\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}\right) &= W_v\left(\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) \\
&= W_v\left(\begin{bmatrix} 0 & 1 \\ x^{-1} & 0 \end{bmatrix}\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}\right) \\
&= W_{\rho\left(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}\right)v}\left(\begin{bmatrix} 0 & 1 \\ x^{-1} & 0 \end{bmatrix}\right) \\
&= W_{\rho'\left(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}\right)v}\left(\begin{bmatrix} 0 & 1 \\ x^{-1} & 0 \end{bmatrix}\right) \\
&= W'_{\rho'\left(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}\right)v}\left(\begin{bmatrix} 0 & 1 \\ x^{-1} & 0 \end{bmatrix}\right) \\
&= W'_{\rho'(w)}\left(\begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}\right).
\end{aligned}$$

Hence, by Lemma 3.5, $W_{\rho(w)v} = W'_{\rho'(w)v}$, and hence $\rho(w) = \rho'(w)$. ∎

3.4 The Bessel function of a representation

Let ρ be a higher-dimensional representation of G. Then $\dim V_\rho > 2 \geq \dim J(V_\rho)$ except in the case where $q = 3$ and $\dim \rho = 2$. In this case, ρ is however cuspidal and $J(V_\rho) = 0$. Therefore, $J(V_\rho) \neq V_\rho$ in all cases.

As U is an abelian group, $\operatorname{Res}_U^G \rho$ decomposes into a direct sum of characters. One of them must be different from the unit character. Indeed, otherwise we would have that

$$\rho\left(\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}\right) v = v$$

[2] I find this argument unsatisfactory. Here's an alternate: fix $v_0 \in V$ which is an A-eigenvector with eigenvalue ω, which implies $W_{v_0}(1), W'_{v_0}(1) \neq 0$ as explained previously. Scaling, we may assume $W_{v_0}(1) = W_{v_0}(1)$. Note $W_{v_0}(a) = W'_{v_0}(a)$ for any $a \in A$. Properties of Whittaker functions allow us to extend this to $W_{auv_0}(a') = \psi\left((aa')u(aa')^{-1}\right)\omega(aa')W_{v_0}(1) = W'_{auv_0}(a')$ for any $a, a' \in A$ and $u \in U$. Thus, $\operatorname{Res}_A^G W_v = \operatorname{Res}_A^G W'_v$ for any $v \in Pv_0$, but Pv_0 spans V because $\operatorname{Res}_P^G V = V_\pi$ is P-irreducible.

for every $\beta \in K$ and every $v \in V_\rho$. Then by (3.3),

$$W_v\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) = \psi(\alpha\beta) W_v\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right)$$

for every $\alpha \in K^\times$. Hence, $\operatorname{Res}^G_A W_v = 0$, and hence $v \in J(V_\rho)$ by Lemma 3.5. This contradicts the inequality $J(V_\rho) \neq V_\rho$. There exists therefore a non-unit character ψ_1 of K^+ and a nonzero vector $v_1' \in V_\rho$ such that

$$\rho\left(\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\right) v_w' = \psi_1(\beta) v_1' \qquad \text{for every } \beta \in K.$$

By section 2.1, there exists an $\alpha \in K^\times$ such that $\psi_1(\beta) = \psi(\alpha\beta)$. Using the identity

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

and replacing v_1' by $v_1 := \rho\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) v_1'$, we get that

$$\rho\left(\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\right) v_1 = \psi(\beta) v_1) \qquad \text{for every } \beta \in K. \tag{3.4}$$

It follows that if $\alpha \in K^\times$, then

$$\psi(\beta) W_{v_1}\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) = \psi(\alpha\beta) W_{v_1}\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right).$$

If $\alpha \neq 1$, then we may conclude that

$$W_{v_1}\left(\begin{bmatrix}\alpha & 0\\ 0 & 1\end{bmatrix}\right) = 0.$$

Further, (3.4) implies that $v_1 \notin J(V_\rho)$. Hence, $\operatorname{Res}_A W_{v_1} \neq 0$ by Lemma 3.5 and therefore $W_{v_1}(1) \neq 0$. The vector v_1 is said to be a *Bessel vector* for ρ.

If v_2 if an additional Bessel vector for ρ, then by the last paragraph, there exists a $\zeta \in \mathbb{C}$ such that $W_{v_1}(a) = \zeta W_{v_2}(a)$ for every $a \in A$. Using Lemma 3.5 once again, we conclude that $v_1 - \zeta v_2 \in J(V_\rho)$. Hence,

$$\psi(\beta)(v_1 - \zeta v_2) = \rho\left(\begin{bmatrix}1 & \beta\\ 0 & 1\end{bmatrix}\right)(v_1 - \zeta v_2) = v_1 - \zeta v_2 \qquad \text{for every } \beta \in K.$$

Hence, $v_1 = \zeta v_2$. Thus, up to a scalar multiple, there exists only one Bessel vector for ρ. We use this vector to define the *Bessel function* $J_\rho \colon G \to \mathbb{C}$ of ρ by

$$J_\rho(g) := \left(W_{v_1}\left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)\right)^{-1} W_{v_1}(g).$$

Clearly, $J_\rho(g)$ does not depend on the particular Bessel vector v_1 which is used in its definition. Note that J_ρ is also a Whittaker function for ρ. Therefore,

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

Also,

$$J_\rho(1) = 1 \qquad \text{and} \qquad J_\rho(a) = 0 \text{ if } a \neq 1 \text{ and } a \in A.$$

Therefore, if a character ω of $K^\times$ is not exceptional for ρ, we have by Theorem 3.4 that

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

One can use this formula to define $\Gamma_\rho(\omega)$ also for the exceptional characters. We shall use this formula in the next two sections in order to compute Γ_ρ.

3.5 A computation of $\Gamma_\rho(\omega)$ for a non-cuspidal ρ

3.6 A computation of $\Gamma_\rho(\omega)$ for a cuspidal ρ

3.7 The characters of G

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

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

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 $W \subseteq V_\rho$. 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

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

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

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

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 $\mathrm{End}_{\mathbb{C}[G]}\left(V_{\rho_i}^{\oplus n_i}, V_{\rho_i}^{\oplus n_i}\right)$ 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

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

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 $\chi_\rho(g) := \operatorname{tr}\rho(g)$.

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

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

To see $\overset{*}{=}$ 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

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

To see $\overset{*}{=}$ 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

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

where $\overset{*}{=}$ 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

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

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

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

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

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

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

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

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 $n_i^2 \le 1$ 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.