CHAPTER XVIII

Representations of Finite Groups

The theory of group representations occurs in many contexts. First, it is developed for its own sake: determine all irreducible representations of a given group. See for instance Curtis-Reiner's *Methods of Representation Theory* (Wiley-Interscience, 1981). It is also used in classifying finite simple groups. But already in this book we have seen applications of representations to Galois theory and the determination of the Galois group over the rationals. In addition, there is an analogous theory for topological groups. In this case, the closest analogy is with compact groups, and the reader will find a self-contained treatment of the compact case entirely similar to §5 of this chapter in my book $\mathbf{SL_2(R)}$ (Springer Verlag), Chapter II, §2. Essentially, finite sums are replaced by integrals, otherwise the formalism is the same. The analysis comes only in two places. One of them is to show that every irreducible representation of a compact group is finite dimensional; the other is Schur's lemma. The details of these extra considerations are carried out completely in the above-mentioned reference. I was careful to write up §5 with the analogy in mind.

Similarly, readers will find analogous material on induced representations in $\mathbf{SL_2(R)}$, Chapter III, §2 (which is also self-contained).

Examples of the general theory come in various shapes. Theorem 8.4 may be viewed as an example, showing how a certain representation can be expressed as a direct sum of induced representations from 1-dimensional representations. Examples of representations of S_3 and S_4 are given in the exercises. The entire last section works out completely the simple characters for the group $GL_2(\mathbf{F})$ when $\mathbf{F}$ is a finite field, and shows how these characters essentially come from induced characters.

For other examples also leading into Lie groups, see W. Fulton and J. Harris, *Representation Theory*, Springer Verlag 1991.

S. Lang, *Algebra*

§1. REPRESENTATIONS AND SEMISIMPLICITY

Let R be a commutative ring and G a group. We form the group algebra $R[G]$. As explained in Chapter II, §3 it consists of all formal linear combinations

$$\sum_{\sigma \in G} a_\sigma \sigma$$

with coefficients $a_\sigma \in R$, almost all of which are 0. The product is taken in the natural way,

$$\left(\sum_{\sigma \in G} a_\sigma \sigma\right)\left(\sum_{\tau \in G} b_\tau \tau\right) = \sum_{\sigma, \tau} a_\sigma b_\tau \sigma\tau.$$

Let E be an R-module. Every algebra-homomorphism

$$R[G] \to \mathrm{End}_R(E)$$

induces a group-homomorphism

$$G \to \mathrm{Aut}_R(E),$$

and thus a representation of the ring $R[G]$ in E gives rise to a representation of the group. Given such representations, we also say that $R[G]$, or G, **operate** on E. We note that the representation makes E into a module over the ring $R[G]$.

Conversely, given a representation of the group, say $\rho : G \to \mathrm{Aut}_R(E)$, we can extend ρ to a representation of $R[G]$ as follows. Let $\alpha = \sum a_\sigma \sigma$ and $x \in E$. We define

$$\rho(\alpha)x = \sum a_\sigma \rho(\sigma)x.$$

It is immediately verified that ρ has been extended to a ring-homomorphism of $R[G]$ into $\mathrm{End}_R(E)$. We say that ρ is **faithful** on G if the map $\rho : G \to \mathrm{Aut}_R(E)$ is injective. The extension of ρ to $R[G]$ may not be faithful, however.

Given a representation of G on E, we often write simply σx instead of $\rho(\sigma)x$, whenever we deal with a fixed representation throughout a discussion.

An R-module E, together with a representation ρ, will be called a ***G*-module**, or ***G*-space**, or also a (G, R)-module if we wish to specify the ring R. If E, F are G-modules, we recall that a G-homomorphism $f : E \to F$ is an R-linear map such that $f(\sigma x) = \sigma f(x)$ for all $x \in E$ and $\sigma \in G$.

Given a G-homomorphism $f : E \to F$, we note that the kernel of f is a G-submodule of E, and that the R-factor module $F/f(E)$ admits an operation of G in a unique way such that the canonical map $F \to F/f(E)$ is a G-homomorphism.

By a **trivial** representation $\rho : G \to \mathrm{Aut}_R(E)$, we shall mean the representation such that $\rho(G) = 1$. A representation is trivial if and only if $\sigma x = x$ for all $x \in E$. We also say in that case that G **operates trivially**.

We make R into a G-module by making G act trivially on R.

We shall now discuss systematically the representations which arise from a given one, on Hom, the dual, and the tensor product. This pattern will be repeated later when we deal with induced representations.

First, $\mathrm{Hom}_R(E, F)$ is a G-module under the action defined for $f \in \mathrm{Hom}_R(E, F)$ by

$$([\sigma]f)(x) = \sigma f(\sigma^{-1}x).$$

The conditions for an operation are trivially verified. Note the σ^{-1} inside the expression. We shall usually omit parentheses, and write simply $[\sigma]f(x)$ for the left-hand side. We note that f is a G-homomorphism if and only if $[\sigma]f = f$ for all $\sigma \in G$.

We are particularly concerned when $F = R$ (so with trivial action), in which case $\mathrm{Hom}_R(E, R) = E^\vee$ is the dual module. In the terminology of representations, if $\rho\colon G \to \mathrm{Aut}_R(E)$ is a representation of G on E, then the action we have just described gives a representation denoted by

$$\rho^\vee : G \to \mathrm{Aut}_R(E^\vee),$$

and called the **dual representation** (also called contragredient (ugh!) in the literature).

Suppose now that the modules E, F are free and finite dimensional over R. Let ρ be representation of G on E. Let M be the matrix of $\rho(\sigma)$ with respect to a basis, and let $M^\vee$ be the matrix of $\rho^\vee(\sigma)$ with respect to the dual basis. Then it is immediately verified that

(1) $$M^\vee = {}^tM^{-1}.$$

Next we consider the tensor product instead of Hom. Let E, E' be (G, R)-modules. We can form their tensor product $E \otimes E'$, always taken over R. Then there is a unique action of G on $E \otimes E'$ such that for $\sigma \in G$ we have

$$\sigma(x \otimes x') = \sigma x \otimes \sigma x'.$$

Suppose that E, F are finite free over R. Then the R-isomorphism

(2) $$E^\vee \otimes F \approx \mathrm{Hom}_R(E, F)$$

of Chapter XVI, Corollary 5.5, is immediately verified to be a G-isomorphism.

Whether E is free or not, we define the G-**invariant** submodule of E to be $\mathrm{inv}_G(E)$ = R-submodule of elements $x \in E$ such that $\sigma x = x$ for all $\sigma \in G$. If E, F are free then we have an R-isomorphism

(3) $$\mathrm{inv}_G(E^\vee \otimes F) \approx \mathrm{Hom}_G(E, F).$$

If $\rho\colon G \to \mathrm{Aut}_R(E)$ and $\rho'\colon G \to \mathrm{Aut}_R(E')$ are representations of G on E and E' respectively, then we define their **sum** $\rho \oplus \rho'$ to be the representation on the direct sum $E \oplus E'$, with $\sigma \in G$ acting componentwise. Observe that G-isomorphism classes of representations have an additive monoid structure under this direct sum, and also have an associative multiplicative structure under the tensor product. With the notation of representations, we denote this product by $\rho \otimes \rho'$. This product is distributive with respect to the addition (direct sum).

If G is a finite group, and E is a G-module, then we can define the **trace** $\mathrm{Tr}_G\colon E \to E$ which is an R-homomorphism, namely

$$\mathrm{Tr}_G(x) = \sum_{\sigma \in G} \sigma x.$$

We observe that $\mathrm{Tr}_G(x)$ lies in $\mathrm{inv}_G(E)$, i.e. is fixed under the operation of all elements of G. This is because

$$\tau \,\mathrm{Tr}_G(x) = \sum_{\sigma \in G} \tau\sigma x,$$

and multiplying by τ on the left permutes the elements of G.

In particular, if $f\colon E \to F$ is an R-homomorphism of G-modules, then $\mathrm{Tr}_G(f)\colon E \to F$ is a G-homomorphism.

Proposition 1.1. *Let G be a finite group and let E', E, F, F' be G-modules. Let*

$$E' \xrightarrow{\varphi} E \xrightarrow{f} F \xrightarrow{\psi} F'$$

be R-homomorphisms, and assume that φ, ψ are G-homomorphisms. Then

$$\mathrm{Tr}_G(\psi \circ f \circ \varphi) = \psi \circ \mathrm{Tr}_G(f) \circ \varphi.$$

Proof. We have

$$\mathrm{Tr}_G(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} \sigma(\psi \circ f \circ \varphi) = \sum_{\sigma \in G} (\sigma\psi) \circ (\sigma f) \circ (\sigma\varphi)$$

$$= \psi \circ \left(\sum_{\sigma \in G} \sigma f\right) \circ \varphi = \psi \circ \mathrm{Tr}_G(f) \circ \varphi.$$

Theorem 1.2. (Maschke). *Let G be a finite group of order n, and let k be a field whose characteristic does not divide n. Then the group ring $k[G]$ is semisimple.*

Proof. Let E be a G-module, and F a G-submodule. Since k is a field, there exists a k-subspace F' such that E is the k-direct sum of F and F'. We let the k-linear map $\pi\colon E \to F$ be the projection on F. Then $\pi(x) = x$ for all $x \in F$.

Let

$$\varphi = \frac{1}{n}\operatorname{Tr}_G(\pi).$$

We have then two G-homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & F \arrow[r, shift left, "j"] & E \arrow[l, shift left, "\varphi"] \end{tikzcd}$$

such that j is the inclusion, and $\varphi \circ j = \mathrm{id}$. It follows that E is the G-direct sum of F and Ker φ, thereby proving that $k[G]$ is semisimple.

Except in §7 we denote by G a finite group, and we denote E, F finite dimensional k-spaces, where k is a field of characteristic not dividing $\#(G)$. We usually denote $\#(G)$ by n.

§2. CHARACTERS

Let $\rho : k[G] \to \operatorname{End}_k(E)$ be a representation. By the **character** χ_ρ of the representation, we shall mean the k-valued function

$$\chi_\rho : k[G] \to k$$

such that $\chi_\rho(\alpha) = \operatorname{tr} \rho(\alpha)$ for all $\alpha \in k[G]$. The trace here is the trace of an endomorphism, as defined in Chapter XIII, §3. If we select a basis for E over k, it is the trace of the matrix representing $\rho(\alpha)$, i.e., the sum of the diagonal elements. We have seen previously that the trace does not depend on the choice of the basis. We sometimes write χ_E instead of χ_ρ.

We also call E the **representation space** of ρ.

By the **trivial character** we shall mean the character of the representation of G on the k-space equal to k itself, such that $\sigma x = x$ for all $x \in k$. It is the function taking the value 1 on all elements of G. We denote it by χ_0 or also by 1_G if we need to specify the dependence on G.

We observe that characters are functions on G, and that the values of a character on elements of $k[G]$ are determined by its values on G (the extension from G to $k[G]$ being by k-linearity).

We say that two representations ρ, φ of G on spaces E, F are **isomorphic** if there is a G-isomorphism between E and F. We then see that if ρ, φ are isomorphic representations, then their characters are equal. (Put in another way, if E, F are G-spaces and are G-isomorphic, then $\chi_E = \chi_F$.) In everything that follows, we are interested only in isomorphism classes of representations.

If E, F are G-spaces, then their direct sum $E \oplus F$ is also a G-space, the operation of G being componentwise. If $x \oplus y \in E \oplus F$ with $x \in E$ and $y \in F$, then $\sigma(x \oplus y) = \sigma x \oplus \sigma y$.

Similarly, the tensor product $E \otimes_k F = E \otimes F$ is a G-space, the operation of G being given by $\sigma(x \otimes y) = \sigma x \otimes \sigma y$.

Proposition 2.1. *If E, F are G-spaces, then*

$$\chi_E + \chi_F = \chi_{E \oplus F} \quad \textit{and} \quad \chi_E \chi_F = \chi_{E \otimes F}.$$

If $\chi^\vee$ denotes the character of the dual representation on $E^\vee$, then

$$\begin{aligned} \chi^\vee(\sigma) &= \chi(\sigma^{-1}) \\ &= \overline{\chi(\sigma)} \textit{ if } k = \mathbf{C}. \end{aligned}$$

Proof. The first relation holds because the matrix of an element σ in the representation $E \oplus F$ decomposes into blocks corresponding to the representation in E and the representation in F. As to the second, if $\{v_i\}$ is a basis of E and $\{w_j\}$ is a basis of F over k, then we know that $\{v_i \otimes w_j\}$ is a basis of $E \otimes F$. Let $(a_{i\nu})$ be the matrix of σ with respect to our basis of E, and $(b_{j\mu})$ its matrix with respect to our basis of F. Then

$$\begin{aligned} \sigma(v_i \otimes w_j) = \sigma v_i \otimes \sigma w_j &= \sum_\nu a_{i\nu} v_\nu \otimes \sum_\mu b_{j\mu} w_\mu \\ &= \sum_{\nu, \mu} a_{i\nu} b_{j\mu} v_\nu \otimes w_\mu. \end{aligned}$$

By definition, we find

$$\chi_{E \otimes F}(\sigma) = \sum_i \sum_j a_{ii} b_{jj} = \chi_E(\sigma)\chi_F(\sigma),$$

thereby proving the statement about tensor products. The statement for the character of the dual representation follows from the formula for the matrix ${}^tM^{-1}$ given in §1. The value given as the complex conjugate in case $k = \mathbf{C}$ will be proved later in Corollary 3.2.

So far, we have defined the notion of character associated with a representation. It is now natural to form linear combinations of such characters with more general coefficients than positive integers. Thus by a **character** of G we shall mean a function on G which can be written as a linear combination of characters of representations with arbitrary integer coefficients. The characters associated with representations will be called **effective characters**. Everything we have defined of course depends on the field k, and we shall add **over *k*** to our expressions if we need to specify the field k.

We observe that the characters form a ring in view of Proposition 2.1. For most of our work we do not need the multiplicative structure, only the additive one.

By a **simple** or **irreducible character** of G one means the character of a simple representation (i.e., the character associated with a simple $k[G]$-module).

Taking into account Theorem 1.2, and the results of the preceding chapter concerning the structure of simple and semisimple modules over a semisimple ring (Chapter XVII, §4) we obtain:

Theorem 2.2. *There are only a finite number of simple characters of G (over k). The characters of representations of G are the linear combinations of the simple characters with integer coefficients $\geqq 0$.*

We shall use the direct product decomposition of a semisimple ring. We have

$$k[G] = \prod_{i=1}^{s} R_i$$

where each R_i is simple, and we have a corresponding decomposition of the unit element of $k[G]$:

$$1 = e_1 + \cdots + e_s,$$

where e_i is the unit element of R_i, and $e_i e_j = 0$ if $i \neq j$. Also, $R_i R_j = 0$ if $i \neq j$. *We note that $s = s(k)$ depends on k.*

If L_i denotes a typical simple module for R_i (say one of the simple left ideals), we let χ_i be the character of the representation on L_i.

We observe that $\chi_i(\alpha) = 0$ for all $\alpha \in R_j$ if $i \neq j$. This is a fundamental relation of orthogonality, which is obvious, but from which all our other relations will follow.

Theorem 2.3. *Assume that k has characteristic 0. Then every effective character has a unique expression as a linear combination*

$$\chi = \sum_{i=1}^{s} n_i \chi_i, \qquad n_i \in \mathbf{Z},\ n_i \geqq 0,$$

where $\chi_1, \ldots, \chi_s$ are the simple characters of G over k. Two representations are isomorphic if and only if their associated characters are equal.

Proof. Let E be the representation space of χ. Then by Theorem 4.4 of Chapter XVII,

$$E \approx \bigoplus_{i=1}^{s} n_i L_i.$$

The sum is finite because we assume throughout that E is finite dimensional. Since e_i acts as a unit element on L_i, we find

$$\chi_i(e_i) = \dim_k L_i.$$

We have already seen that $\chi_i(e_j) = 0$ if $i \neq j$. Hence

$$\chi(e_i) = n_i \dim_k L_i.$$

Since $\dim_k L_i$ depends only on the structure of the group algebra, we have recovered the multiplicities $n_1, \dots, n_s$. Namely, n_i is the number of times that L_i occurs (up to an isomorphism) in the representation space of χ, and is the value of $\chi(e_i)$ divided by $\dim_k L_i$ (we are in characteristic 0). This proves our theorem.

As a matter of definition, in Theorem 2.3 we call n_i the **multiplicity** of χ_i in χ. In both corollaries, we continue to assume that k has characteristic 0.

Corollary 2.4. *As functions of G into k, the simple characters*

$$\chi_1, \dots, \chi_s$$

are linearly independent over k.

Proof. Suppose that $\sum a_i\chi_i = 0$ with $a_i \in k$. We apply this expression to e_j and get

$$0 = (\textstyle\sum a_i\chi_i)(e_j) = a_j \dim_k L_j.$$

Hence $a_j = 0$ for all j.

In characteristic 0 we define the **dimension** of an effective character to be the dimension of the associated representation space.

Corollary 2.5. *The function* dim *is a homomorphism of the monoid of effective characters into* **Z**.

Example. Let G be a cyclic group of order equal to a prime number p. We form the group algebra $\mathbf{Q}[G]$. Let σ be a generator of G. Let

$$e_1 = \frac{1 + \sigma + \sigma^2 + \cdots + \sigma^{p-1}}{p}, \qquad e_2 = 1 - e_1.$$

Then $\tau e_1 = e_1$ for any $\tau \in G$ and consequently $e_1^2 = e_1$. It then follows that $e_2^2 = e_2$ and $e_1 e_2 = 0$. The field $\mathbf{Q}e_1$ is isomorphic to $\mathbf{Q}$. Let $\omega = \sigma e_2$. Then $\omega^p = e_2$. Let $\mathbf{Q}_2 = \mathbf{Q}e_2$. Since $\omega \neq e_2$, and satisfies the irreducible equation

$$X^{p-1} + \cdots + 1 = 0$$

over $\mathbf{Q}_2$, it follows that $\mathbf{Q}_2(\omega)$ is isomorphic to the field obtained by adjoining a primitive p-th root of unity to the rationals. Consequently, $\mathbf{Q}[G]$ admits the direct product decomposition

$$\mathbf{Q}[G] \approx \mathbf{Q} \times \mathbf{Q}(\zeta)$$

where ζ is a primitive p-th root of unity.

As another example, let G be any finite group, and let

$$e_1 = \frac{1}{n} \sum_{\sigma \in G} \sigma.$$

Then for any $\tau \in G$ we have $\tau e_1 = e_1$, and $e_1^2 = e_1$. If we let $e_1' = 1 - e_1$ then $e_1'^2 = e_1'$, and $e_1' e_1 = e_1 e_1' = 0$. Thus for any field k (whose characteristic does not divide the order of G according to conventions in force), we see that

$$k[G] = ke_1 \times k[G]e_1'$$

is a direct product decomposition. In particular, the representation of G on the group algebra $k[G]$ itself contains a 1-dimensional representation on the component ke_1, whose character is the trivial character.

§3. 1-DIMENSIONAL REPRESENTATIONS

By abuse of language, even in characteristic $p > 0$, we say that a **character is 1-dimensional** if it is a homomorphism $G \to k^*$.

Assume that E is a 1-dimensional vector space over k. Let

$$\rho : G \to \mathrm{Aut}_k(E)$$

be a representation. Let $\{v\}$ be a basis of E over k. Then for each $\sigma \in G$, we have

$$\sigma v = \chi(\sigma) v$$

for some element $\chi(\sigma) \in k$, and $\chi(\sigma) \neq 0$ since σ induces an automorphism of E. Then for $\tau \in G$,

$$\tau\sigma v = \chi(\sigma)\tau v = \chi(\sigma)\chi(\tau)v = \chi(\sigma\tau)v.$$

We see that $\chi : G \to k^*$ is a homomorphism, and that our 1-dimensional character is the same type of thing that occurred in Artin's theorem in Galois theory.

Conversely, let $\chi : G \to k^*$ be a homomorphism. Let E be a 1-dimensional k-space, with basis $\{v\}$, and define $\sigma(av) = a\chi(\sigma)v$ for all $a \in k$. Then we see at once that this operation of G on E gives a representation of G, whose associated character is χ.

Since G is finite, we note that

$$\chi(\sigma)^n = \chi(\sigma^n) = \chi(1) = 1.$$

Hence the values of 1-dimensional characters are n-th roots of unity. The 1-dimensional characters form a group under multiplication, and when G is a finite abelian group, we have determined its group of 1-dimensional characters in Chapter I, §9.

Theorem 3.1. *Let G be a finite abelian group, and assume that k is algebraically closed. Then every simple representation of G is 1-dimensional. The simple characters of G are the homomorphisms of G into k^*.*

Proof. The group ring $k[G]$ is semisimple, commutative, and is a direct product of simple rings. Each simple ring is a ring of matrices over k (by Corollary 3.6 Chapter XVII), and can be commutative if and only if it is equal to k.

For every 1-dimensional character χ of G we have

$$\chi(\sigma)^{-1} = \chi(\sigma^{-1}).$$

If k is the field of complex numbers, then

$$\overline{\chi(\sigma)} = \chi(\sigma)^{-1} = \chi(\sigma^{-1}).$$

Corollary 3.2. *Let k be algebraically closed. Let G be a finite group. For any character χ and $\sigma \in G$, the value $\chi(\sigma)$ is equal to a sum of roots of unity with integer coefficients (i.e. coefficients in $\mathbf{Z}$ or $\mathbf{Z}/p\mathbf{Z}$ depending on the characteristic of k).*

Proof. Let H be the subgroup generated by σ. Then H is a cyclic subgroup. A representation of G having character χ can be viewed as a representation for H by restriction, having the same character. Thus our assertion follows from Theorem 3.1.

§4. THE SPACE OF CLASS FUNCTIONS

By a **class function** of G (over k, or with values in k), we shall mean a function $f : G \to k$ such that $f(\sigma\tau\sigma^{-1}) = f(\tau)$ for all σ, $\tau \in G$. It is clear that characters are class functions, because for square matrices M, M' we have

$$\operatorname{tr}(MM'M^{-1}) = \operatorname{tr}(M').$$

Thus a class function may be viewed as a function on conjugacy classes.

We shall always extend the domain of definition of a class function to the group ring, by linearity. If

$$\alpha = \sum_{\sigma \in G} a_\sigma \sigma,$$

and f is a class function, we define

$$f(\alpha) = \sum_{\sigma \in G} a_\sigma f(\sigma).$$

Let $\sigma_0 \in G$. If $\sigma \in G$, we write $\sigma \sim \sigma_0$ if σ is conjugate to σ_0, that is, if there exists an element τ such that $\sigma_0 = \tau\sigma\tau^{-1}$. An element of the group ring of type

$$\gamma = \sum_{\sigma \sim \sigma_0} \sigma$$

will also be called a **conjugacy class**.

Proposition 4.1. *An element of $k[G]$ commutes with every element of G if and only if it is a linear combination of conjugacy classes with coefficients in k.*

Proof. Let $\alpha = \sum_{\sigma \in G} a_\sigma \sigma$ and assume $\alpha\tau = \tau\alpha$ for all $\tau \in G$. Then

$$\sum_{\sigma \in G} a_\sigma \tau\sigma\tau^{-1} = \sum_{\sigma \in G} a_\sigma \sigma.$$

Hence $a_{\sigma_0} = a_\sigma$ whenever σ is conjugate to σ_0, and this means that we can write

$$\alpha = \sum_{\gamma} a_\gamma \gamma$$

where the sum is taken over all conjugacy classes γ.

Remark. We note that the conjugacy classes in fact form a basis of the center of $\mathbf{Z}[G]$ over $\mathbf{Z}$, and thus play a universal role in the theory of representations.

We observe that the conjugacy classes are linearly independent over k, and form a basis for the center of $k[G]$ over k.

Assume for the rest of this section that k is algebraically closed. Then

$$k[G] = \prod_{i=1}^{s} R_i$$

is a direct product of simple rings, and each R_i is a matrix algebra over k. In a direct product, the center is obviously the product of the centers of each factor. Let us denote by k_i the image of k in R_i, in other words,

$$k_i = ke_i,$$

where e_i is the unit element of R_i. Then the center of $k[G]$ is also equal to

$$\prod_{i=1}^{s} k_i$$

which is s-dimensional over k.

If L_i is a typical simple left ideal of R_i, then

$$R_i \approx \operatorname{End}_k(L_i).$$

We let

$$d_i = \dim_k L_i.$$

Then

$$\boxed{d_i^2 = \dim_k R_i \quad \text{and} \quad \sum_{i=1}^{s} d_i^2 = n.}$$

We also have the direct sum decomposition

$$R_i \approx L_i^{(d_i)}$$

as a (G, k)-space.

The above notation will remain fixed from now on.

We can summarize some of our results as follows.

Proposition 4.2. *Let k be algebraically closed. Then the number of conjugacy classes of G is equal to the number of simple characters of G, both of these being equal to the number s above. The conjugacy classes $\gamma_1, \dots, \gamma_s$ and the unit elements $e_1, \dots, e_s$ form bases of the center of $k[G]$.*

The number of elements in γ_i will be denoted by h_i. The number of elements in a conjugacy class γ will be denoted by h_γ. We call it the **class number**. The center of the group algebra will be denoted by $Z_k(G)$.

We can view $k[G]$ as a G-module. Its character will be called the **regular character**, and will be denoted by χ_{reg} or r_G if we need to specify the dependence on G. The representation on $k[G]$ is called the**regular representation**. From our direct sum decomposition of $k[G]$ we get

$$\boxed{\chi_{\mathrm{reg}} = \sum_{i=1}^{s} d_i \chi_i.}$$

We shall determine the values of the regular character.

Proposition 4.3. *Let χ_{reg} be the regular character. Then*

$$\chi_{\mathrm{reg}}(\sigma) = 0 \quad \textit{if} \quad \sigma \in G, \sigma \neq 1$$

$$\chi_{\mathrm{reg}}(1) = n.$$

Proof. Let $1 = \sigma_1, \dots, \sigma_n$ be the elements of G. They form a basis of $k[G]$ over k. The matrix of 1 is the unit $n \times n$ matrix. Thus our second assertion follows. If $\sigma \neq 1$, then multiplication by σ permutes $\sigma_1, \dots, \sigma_n$, and it is immediately clear that all diagonal elements in the matrix representing σ are 0. This proves what we wanted.

We observe that we have two natural bases for the center $Z_k(G)$ of the group ring. First, the conjugacy classes of elements of G. Second, the elements $e_1, \dots, e_s$ (i.e. the unit elements of the rings R_i). We wish to find the relation between these, in other words, we wish to find the coefficients of e_i when expressed in terms of the group elements. The next proposition does this. The values of these coefficients will be interpreted in the next section as scalar products. This will clarify their mysterious appearance.

Proposition 4.4. *Assume again that k is algebraically closed. Let*

$$e_i = \sum_{\tau \in G} a_\tau \tau, \qquad a_\tau \in k.$$

Then

$$a_\tau = \frac{1}{n} \chi_{\mathrm{reg}}(e_i \tau^{-1}) = \frac{d_i}{n} \chi_i(\tau^{-1}).$$

Proof. We have for all $\tau \in G$:

$$\chi_{\mathrm{reg}}(e_i \tau^{-1}) = \chi_{\mathrm{reg}}\left(\sum_{\sigma \in G} a_\sigma \sigma \tau^{-1} \right) = \sum_{\sigma \in G} a_\sigma \chi_{\mathrm{reg}}(\sigma \tau^{-1}).$$

By Proposition 4.3, we find

$$\chi_{\text{reg}}(e_i\tau^{-1}) = na_\tau.$$

On the other hand,

$$\chi_{\text{reg}}(e_i\tau^{-1}) = \sum_{j=1}^{s} d_j\chi_j(e_i\tau^{-1}) = d_i\chi_i(e_i\tau^{-1}) = d_i\chi_i(\tau^{-1}).$$

Hence

$$d_i\chi_i(\tau^{-1}) = na_\tau$$

for all $\tau \in G$. This proves our proposition.

Corollary 4.5. *Each e_i can be expressed in terms of group elements with coefficients which lie in the field generated over the prime field by m-th roots of unity, if m is an exponent for G.*

Corollary 4.6. *The dimensions d_i are not divisible by the characteristic of k.*

Proof. Otherwise, $e_i = 0$, which is impossible.

Corollary 4.7. *The simple characters $\chi_1, \dots, \chi_s$ are linearly independent over k.*

Proof. The proof in Corollary 2.4 applies, since we now know that the characteristic does not divide d_i.

Corollary 4.8. *Assume in addition that k has characteristic 0. Then $d_i | n$ for each i.*

Proof. Multiplying our expression for e_i by n/d_i, and also by e_i, we find

$$\frac{n}{d_i} e_i = \sum_{\sigma \in G} \chi_i(\sigma^{-1})\sigma e_i.$$

Let ζ be a primitive m-th root of unity, and let M be the module over $\mathbf{Z}$ generated by the finite number of elements $\zeta^\nu \sigma e_i$ ($\nu = 0, \dots, m-1$ and $\sigma \in G$). Then from the preceding relation, we see at once that multiplication by n/d_i maps M into itself. By definition, we conclude that n/d_i is integral over $\mathbf{Z}$, and hence lies in $\mathbf{Z}$, as desired.

Theorem 4.9. *Let k be algebraically closed. Let $Z_k(G)$ be the center of $k[G]$, and let $X_k(G)$ be the k-space of class functions on G. Then $Z_k(G)$ and $X_k(G)$ are the dual spaces of each other, under the pairing*

$$(f, \alpha) \mapsto f(\alpha).$$

The simple characters and the unit elements $e_1, \dots, e_s$ form orthogonal bases to each other. We have

$$\chi_i(e_j) = \delta_{ij} d_i.$$

Proof. The formula has been proved in the proof of Theorem 2.3. The two spaces involved here both have dimension s, and $d_i \neq 0$ in k. Our proposition is then clear.

§5. ORTHOGONALITY RELATIONS

Throughout this section, we assume that k is algebraically closed.

If R is a subring of k, we denote by $X_R(G)$ the R-module generated over R by the characters of G. It is therefore the module of functions which are linear combinations of simple characters with coefficients in R. If R is the prime ring (i.e. the integers **Z** or the integers mod p if k has characteristic p), then we denote $X_R(G)$ by $X(G)$.

We shall now define a bilinear map on $X(G) \times X(G)$. If $f, g \in X(G)$, we define

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma) g(\sigma^{-1}).$$

Theorem 5.1. *The symbol $\langle f, g \rangle$ for $f, g \in X(G)$ takes on values in the prime ring. The simple characters form an orthonormal basis for $X(G)$, in other words*

$$\langle \chi_i, \chi_j \rangle = \delta_{ij}.$$

For each ring $R \subset k$, the symbol has a unique extension to an R-bilinear form $X_R(G) \times X_R(G) \to R$, given by the same formula as above.

Proof. By Proposition 4.4, we find

$$\chi_j(e_i) = \frac{d_i}{n} \sum_{\sigma \in G} \chi_i(\sigma^{-1}) \chi_j(\sigma).$$

If $i \neq j$ we get 0 on the left-hand side, so that χ_i and χ_j are orthogonal. If $i = j$ we get d_i on the left-hand side, and we know that $d_i \neq 0$ in k, by Corollary 4.6. Hence $\langle \chi_i, \chi_i \rangle = 1$. Since every element of $X(G)$ is a linear combination of simple characters with integer coefficients, it follows that the values of our bilinear map are in the prime ring. The extension statement is obvious, thereby proving our theorem.

Assume that k has characteristic 0. Let m be an exponent for G, and let R contain the m-th roots of unity. If R has an automorphism of order 2 such that its effect on a root of unity is $\zeta \mapsto \zeta^{-1}$, then we shall call such an automorphism a **conjugation**, and denote it by $a \mapsto \bar{a}$.

Theorem 5.2. *Let k have characteristic 0, and let R be a subring containing the m-th roots of unity, and having a conjugation. Then the bilinear form on $X(G)$ has a unique extension to a hermitian form*

$$X_R(G) \times X_R(G) \to R,$$

given by the formula

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma)\overline{g(\sigma)}.$$

The simple characters constitute an orthonormal basis of $X_R(G)$ with respect to this form.

Proof. The formula given in the statement of the theorem gives the same value as before for the symbol $\langle f, g \rangle$ when f, g lie in $X(G)$. Thus the extension exists, and is obviously unique.

We return to the case when k has arbitrary characteristic.

Let $Z(G)$ denote the additive group generated by the conjugacy classes $\gamma_1, \dots, \gamma_s$ over the prime ring. It is of dimension s. We shall define a bilinear map on $Z(G) \times Z(G)$. If $\alpha = \sum a_\sigma \sigma$ has coefficients in the prime ring, we denote by α^- the element $\sum a_\sigma \sigma^{-1}$.

Proposition 5.3. *For $\alpha, \beta \in Z(G)$, we can define a symbol $\langle \alpha, \beta \rangle$ by either one of the following expressions, which are equal:*

$$\langle \alpha, \beta \rangle = \frac{1}{n} \chi_{\text{reg}}(\alpha\beta^-) = \frac{1}{n} \sum_{\nu=1}^{s} \chi_\nu(\alpha)\chi_\nu(\beta^-).$$

The values of the symbol lie in the prime ring.

Proof. Each expression is linear in its first and second variable. Hence to prove their equality, it will suffice to prove that the two expressions are equal when we replace α by e_i and β by an element τ of G. But then, our equality is equivalent to

$$\chi_{\text{reg}}(e_i \tau^{-1}) = \sum_{\nu=1}^{s} \chi_\nu(e_i)\chi_\nu(\tau^{-1}).$$

Since $\chi_v(e_i) = 0$ unless $v = i$, we see that the right-hand side of this last relation is equal to $d_i\chi_i(\tau^{-1})$. Our two expressions are equal in view of Proposition 4.4.

The fact that the values lie in the prime ring follows from Proposition 4.3: The values of the regular character on group elements are equal to 0 or n, and hence in characteristic 0, are integers divisible by n.

As with $X_R(G)$, we use the notation $Z_R(G)$ to denote the R-module generated by $\gamma_1, \ldots, \gamma_s$ over an arbitrary subring R of k.

Lemma 5.4. *For each ring R contained in k, the pairing of Proposition 5.3 has a unique extension to a map*

$$Z_R(G) \times Z(G) \to R$$

which is R-linear in its first variable. If R contains the m-th roots of unity, where m is an exponent for G, and also contains $1/n$, then $e_i \in Z_R(G)$ for all i. The class number h_i is not divisible by the characteristic of k, and we have

$$e_i = \sum_{\nu=1}^{s} \langle e_i, \gamma_\nu \rangle \frac{1}{h_\nu} \gamma_\nu .$$

Proof. We note that h_i is not divisible by the characteristic because it is the index of a subgroup of G (the isotropy group of an element in γ_i when G operates by conjugation), and hence h_i divides n. The extension of our pairing as stated is obvious, since $\gamma_1, \ldots, \gamma_s$ form a basis of $Z(G)$ over the prime ring. The expression of e_i in terms of this basis is only a reinterpretation of Proposition 4.4 in terms of the present pairing.

Let E be a free module over a subring R of k, and assume that we have a bilinear symmetric (or hermitian) form on E. Let $\{v_1, \ldots, v_s\}$ be an orthogonal basis for this module. If

$$v = a_1 v_1 + \cdots + a_s v_s$$

with $a_i \in R$, then we call $a_1, \ldots, a_s$ the **Fourier coefficients** of v with respect to our basis. In terms of the form, these coefficients are given by

$$a_i = \frac{\langle v, v_i \rangle}{\langle v_i, v_i \rangle}$$

provided $\langle v_i, v_i \rangle \neq 0$.

We shall see in the next theorem that the expression for e_i in terms of $\gamma_1, \ldots, \gamma_s$ is a Fourier expansion.

Theorem 5.5. *The conjugacy classes $\gamma_1, \ldots, \gamma_s$ constitute an orthogonal basis for $Z(G)$. We have $\langle \gamma_i, \gamma_i \rangle = h_i$. For each ring R contained in k, the bilinear map of Proposition 5.3 has a unique extension to a R-bilinear map*

$$Z_R(G) \times Z_R(G) \to R.$$

Proof. We use the lemma. By linearity, the formula in the lemma remains valid when we replace R by k, and when we replace e_i by any element of $Z_k(G)$, in particular when we replace e_i by γ_i. But $\{\gamma_1, \dots, \gamma_s\}$ is a basis of $Z_k(G)$, over k. Hence we find that $\langle \gamma_i, \gamma_i \rangle = h_i$ and $\langle \gamma_i, \gamma_j \rangle = 0$ if $i \neq j$, as was to shown.

Corollary 5.6. *If G is commutative, then*

$$\frac{1}{n} \sum_{\nu=1}^{n} \chi_\nu(\sigma)\chi_\nu(\tau^{-1}) = \begin{cases} 0 & \text{if } \sigma \text{ is not equal to } \tau \\ 1 & \text{if } \sigma \text{ is equal to } \tau. \end{cases}$$

Proof. When G is commutative, each conjugacy class has exactly one element, and the number of simple characters is equal to the order of the group.

We consider the case of characteristic 0 for our $Z(G)$ just as we did for $X(G)$. Let k have characteristic 0, and R be a subring of k containing the m-th roots of unity, and having a conjugation. Let $\alpha = \sum_{\sigma \in G} a_\sigma \sigma$ with $a_\sigma \in R$. We define

$$\bar{\alpha} = \sum_{\sigma \in G} \bar{a}_\sigma \sigma^{-1}.$$

Theorem 5.7. *Let k have characteristic 0, and let R be a subring of k, containing the m-th roots of unity, and having a conjugation. Then the pairing of Proposition 5.3 has a unique extension to a hermitian form*

$$Z_R(G) \times Z_R(G) \to R$$

given by the formulas

$$\langle \alpha, \beta \rangle = \frac{1}{n} \chi_{\text{reg}}(\alpha\bar{\beta}) = \frac{1}{n} \sum_{\nu=1}^{s} \chi_\nu(\alpha)\overline{\chi_\nu(\beta)}.$$

The conjugacy classes $\gamma_1, \dots, \gamma_s$ form an orthogonal basis for $Z_R(G)$. If R contains $1/n$, then $e_1, \dots, e_s$ lie in $Z_R(G)$ and also form an orthogonal basis for $Z_R(G)$. We have $\langle e_i, e_i \rangle = d_i^2/n$.

Proof. The formula given in the statement of the theorem gives the same value as the symbol $\langle \alpha, \beta \rangle$ of Proposition 5.3 when α, β lie in $Z(G)$. Thus the extension exists, and is obviously unique. Using the second formula in Proposition 5.3, defining the scalar product, and recalling that $\chi_\nu(e_i) = 0$ if $\nu \neq i$, we see that

$$\langle e_i, e_i \rangle = \frac{1}{n} \chi_i(e_i)\overline{\chi_i(e_i)},$$

whence our assertion follows.

We observe that the Fourier coefficients of e_i relative to the basis $\gamma_1, \ldots, \gamma_s$ are the same with respect to the bilinear form of Theorem 5.5, or the hermitian form of Theorem 5.7. This comes from the fact that $\gamma_1, \ldots, \gamma_s$ lie in $Z(G)$, and form a basis of $Z(G)$ over the prime ring.

We shall now reprove and generalize the orthogonality relations by another method. Let E be a finite dimensional (G, k)-space, so we have a representation

$$G \to \mathrm{Aut}_k(E).$$

After selecting a basis of E, we get a representation of G by $d \times d$ matrices. If $\{v_1, \ldots, v_d\}$ is the basis, then we have the dual basis $\{\lambda_1, \ldots, \lambda_d\}$ such that $\lambda_i(v_j) = \delta_{ij}$. If an element σ of G is represented by a matrix $(\rho_{ij}(\sigma))$, then each coefficient $\rho_{ij}(\sigma)$ is a function of σ, called the **ij-coefficient function**. We can also write

$$\rho_{ij}(\sigma) = \lambda_j(\sigma v_i).$$

But instead of indexing elements of a basis or the dual basis, we may just as well work with any functional λ on E, and any vector v. Then we get a function

$$\sigma \mapsto \lambda(\sigma v) = \rho_{\lambda, v}(\sigma),$$

which will also be called a **coefficient function**. In fact, one can always complete $v = v_1$ to a basis such that $\lambda = \lambda_1$ is the first element in the dual basis, but using the notation $\rho_{\lambda, v}$ is in many respects more elegant.

We shall constantly use:

Schur's Lemma. *Let E, F be simple (G, k)-spaces, and let*

$$\varphi : E \to F$$

be a homomorphism. Then either $\varphi = 0$ or φ is an isomorphism.

Proof. Indeed, the kernel of φ and the image of φ are subspaces, so the assertion is obvious.

We use the same formula as before to define a scalar product on the space of all k-valued functions on G, namely

$$\langle f, g \rangle = \frac{1}{n} \sum_{\sigma \in G} f(\sigma) g(\sigma^{-1}).$$

We shall derive various orthogonality relations among coefficient functions.

Theorem 5.8. *Let E, F be simple (G, k)-spaces. Let λ be a k-linear functional on E, let $x \in E$ and $y \in F$. If E, F are not isomorphic, then*

$$\sum_{\sigma \in G} \lambda(\sigma x) \sigma^{-1} y = 0.$$

If μ is a functional on F then the coefficient functions $\rho_{\lambda,x}$ and $\rho_{\mu,y}$ are orthogonal, that is

$$\sum_{\sigma \in G} \lambda(\sigma x)\mu(\sigma^{-1}y) = 0.$$

Proof. The map $x \mapsto \sum \lambda(\sigma x)\sigma^{-1}y$ is a G-homomorphism of E into F, so Schur's lemma concludes the proof of the first statement. The second comes by applying the functional μ.

As a corollary, we see that if χ, ψ are distinct irreducible characters of G over k, then

$$\langle \chi, \psi \rangle = 0,$$

that is the characters are orthogonal. Indeed, the character associated with a representation ρ is the sum of the diagonal coefficient functions,

$$\chi = \sum_{i=1}^{d} \rho_{ii},$$

where d is the dimension of the representation. Two distinct characters correspond to non-isomorphic representations, so we can apply Proposition 5.8.

Lemma 5.9. *Let E be a simple (G, k)-space. Then any G-endomorphism of E is equal to a scalar multiple of the identity.*

Proof. The algebra $\mathrm{End}_{G,k}(E)$ is a division algebra by Schur's lemma, and is finite dimensional over k. Since k is assumed algebraically closed, it must be equal to k because any element generates a commutative subfield over k. This proves the lemma.

Lemma 5.10. *Let E be a representation space for G of dimension d. Let λ be a functional on E, and let $x \in E$. Let $\varphi_{\lambda,x} \in \mathrm{End}_k(E)$ be the endomorphism such that*

$$\varphi_{\lambda,x}(y) = \lambda(y)x.$$

Then $\mathrm{tr}(\varphi_{\lambda,x}) = \lambda(x)$.

Proof. If $x = 0$ the statement is obvious. Let $x \neq 0$. If $\lambda(x) \neq 0$ we pick a basis of E consisting of x and a basis of the kernel of λ. If $\lambda(x) = 0$, we pick a basis of E consisting of a basis for the kernel of λ, and one other element. In either case it is immediate from the corresponding matrix representing $\varphi_{\lambda,x}$ that the trace is given by the formula as stated in the lemma.

Theorem 5.11. *Let $\rho: G \to \mathrm{Aut}_k(E)$ be a simple representation of G, of dimension d. Then the characteristic of k does not divide d. Let $x, y \in E$. Then for any functionals λ, μ on E,*

$$\sum_{\sigma \in G} \lambda(\sigma x)\mu(\sigma^{-1}y) = \frac{n}{d}\lambda(y)\mu(x).$$

Proof. It suffices to prove that

$$\sum_{\sigma \in G} \lambda(\sigma x)\sigma^{-1} y = \frac{n}{d} \lambda(y)x.$$

For fixed y the map

$$x \mapsto \sum_{\sigma \in G} \lambda(\sigma x)\sigma^{-1} y$$

is immediately verified to be a G-endomorphism of E, so is equal to cI for some $c \in k$ by Lemma 5.9. In fact, it is equal to

$$\sum_{\sigma \in G} \rho(\sigma^{-1}) \circ \varphi_{\lambda, y} \circ \rho(\sigma).$$

The trace of this expression is equal to $n \cdot \mathrm{tr}(\varphi_{\lambda, y})$ by Lemma 5.10, and also to dc. Taking λ, y such that $\lambda(y) = 1$ shows that the characteristic does not divide d, and then we can solve for c as stated in the theorem.

Corollary 5.12. *Let χ be the character of the representation of G on the simple space E. Then*

$$\langle \chi, \chi \rangle = 1.$$

Proof. This follows immediately from the theorem, and the expression of χ as

$$\chi = \rho_{11} + \cdots + \rho_{dd}.$$

We have now recovered the fact that the characters of simple representations are orthonormal. We may then recover the idempotents in the group ring, that is, if $\chi_1, \ldots, \chi_s$ are the simple characters, we may now *define*

$$e_i = \frac{d_i}{n} \sum_{\sigma \in G} \chi_i(\sigma)\sigma^{-1}.$$

Then the orthonormality of the characters yields the formulas:

Corollary 5.13. $\chi_i(e_j) = \delta_{ij} d_i$ *and* $\chi_{\mathrm{reg}} = \sum_{i=1}^{s} d_i \chi_i$.

Proof. The first formula is a direct application of the orthonormality of the characters. The second formula concerning the regular character is obtained by writing

$$\chi_{\mathrm{reg}} = \sum_j m_j \chi_j$$

with unknown coefficients. We know the values $\chi_{\text{reg}}(1) = n$ and $\chi_{\text{reg}}(\sigma) = 0$ if $\sigma \neq 1$. Taking the scalar product of χ_{reg} with χ_i for $i = 1, \ldots, s$ immediately yields the desired values for the coefficients m_j.

Since a character is a class function, one sees directly that each e_i is a linear combination of conjugacy classes, and so is in the center of the group ring $k[G]$.

Now let E_i be a representation space of χ_i, and let ρ_i be the representation of G or $k[G]$ on E_i. For $\alpha \in k[G]$ we let $\rho_i(\alpha): E_i \to E_i$ be the map such that $\rho_i(\alpha)x = \alpha x$ for all $x \in E_i$.

Proposition 5.14. *We have*

$$\rho_i(e_i) = \text{id} \quad \textit{and} \quad \rho_i(e_j) = 0 \quad \textit{if } i \neq j.$$

Proof. The map $x \mapsto e_i x$ is a G-homomorphism of E_i into itself since e_i is in the center of $k[G]$. Hence by Lemma 5.9 this homomorphism is a scalar multiple of the identity. Taking the trace and using the orthogonality relations between simple characters immediately gives the desired value of this scalar.

We now find that

$$\sum_{i=1}^{s} e_i = 1$$

because the group ring $k[G]$ is a direct sum of simple spaces, possibly with multiplicities, and operates faithfully on itself.

The orthonormality relations also allow us to expand a function in a Fourier expression, relative to the characters if it is a class function, and relative to the coefficient functions in general. We state this in two theorems.

Theorem 5.15. *Let f be a class function on G. Then*

$$f = \sum_{i=1}^{s} \langle f, \chi_i \rangle \chi_i.$$

Proof. The number of conjugacy class is equal to the number of distinct characters, and these are linearly independent, so they form a basis for the class functions. The coefficients are given by the stated formula, as one sees by taking the scalar product of f with any character χ_j and using the orthonormality.

Theorem 5.16. *Let $\rho^{(i)}$ be a matrix representation of G on E_i relative to a choice of basis, and let $\rho^{(i)}_{\nu,\mu}$ be the coefficient functions of this matrix, $i = 1, \ldots, s$ and $\nu, \mu = 1, \ldots, d_i$. Then the functions $\rho^{(i)}_{\nu,\mu}$ form an orthogonal basis for the space of all functions on G, and hence for any function f on G we have*

$$f = \sum_{i=1}^{s} \sum_{\nu,\mu} \frac{1}{d_i} \langle f, \rho^{(i)}_{\nu,\mu} \rangle \rho^{(i)}_{\nu,\mu}.$$

Proof. That the coefficient functions form an orthogonal basis follows from Theorems 5.8 and 5.11. The expression of f in terms of this basis is then merely the standard Fourier expansion relative to any scalar product. This concludes the proof.

Suppose now for concreteness that $k = \mathbf{C}$ is the complex numbers. Recall that an **effective character** χ is an element of $X(G)$, such that if

$$\chi = \sum_{i=1}^{s} m_i \chi_i$$

is a linear combination of the simple characters with integral coefficients, then we have $m_i \geqq 0$ for all i. In light of the orthonormality of the simple characters, we get for all elements $\chi \in X(G)$ the relations

$$\|\chi\|^2 = \langle \chi, \chi \rangle = \sum_{i=1}^{s} m_i^2 \quad \text{and} \quad m_i = \langle \chi, \chi_i \rangle .$$

Hence we get (a) of the next theorem.

Theorem 5.17. **(a)** *Let χ be an effective character in $X(G)$. Then χ is simple over $\mathbf{C}$ if and only if $\|\chi\|^2 = 1$, or alternatively,*

$$\sum_{\sigma \in G} |\chi(\sigma)|^2 = \#(G).$$

(b) *Let χ, ψ be effective characters in $X(G)$, and let E, F be their representation spaces over $\mathbf{C}$. Then*

$$\langle \chi, \psi \rangle_G = \dim \operatorname{Hom}_G(E, F).$$

Proof. The first part has been proved, and for (b), let $\psi = \sum q_i \chi_i$. Then by orthonormality, we get

$$\langle \chi, \psi \rangle_G = \sum m_i q_i .$$

But if E_i is the representation space of χ_i over $\mathbf{C}$, then by Schur's lemma

$$\dim \operatorname{Hom}_G(E_i, E_i) = 1 \text{ and } \dim \operatorname{Hom}_G(E_i, E_j) = 0 \text{ for } i \neq j.$$

Hence $\dim \operatorname{Hom}_G(E, F) = \sum m_i q_i$, thus proving (b).

Corollary 5.18 *With the above notation and $k = \mathbf{C}$ for simplicity, we have:*
(a) *The multiplicity of 1_G in $E^\vee \otimes F$ is $\dim_k \operatorname{inv}_G(E^\vee \otimes F)$.*
(b) *The (G, k)-space E is simple if and only if 1_G has multiplicity 1 in $E^\vee \otimes E$.*

Proof. Immediate from Theorem 5.17 and formula (3) of §1.

Remark. The criterion of Theorem 5.17(a) is useful in testing whether a representation is simple. In practice, representations are obtained by inducing from 1-dimensional characters, and such induced representations do have a tendency to be irreducible. We shall see a concrete case in §12.

§6. INDUCED CHARACTERS

The notation is the same as in the preceding section. However, we don't need all the results proved there; all we need is the bilinear pairing on $X(G)$, and its extension to

$$X_R(G) \times X_R(G) \to R.$$

The symbol $\langle\ ,\ \rangle$ may be interpreted either as the bilinear extension, or the hermitian extension according to Theorem 5.2.

Let S be a subgroup of G. We have an R-linear map called the restriction

$$\mathrm{res}_S^G : X_R(G) \to X_R(S)$$

which to each class function on G associates its restriction to S. It is a ring-homomorphism. We sometimes let f_S denote the restriction of f to S.

We shall define a map in the opposite direction,

$$\mathrm{ind}_S^G : X_R(S) \to X_R(G),$$

which we call the **induction map**. If $g \in X_R(S)$, we extend g to g_S on G by letting $g_S(\sigma) = 0$ if $\sigma \notin S$. Then we define the **induced function**

$$g^G(\sigma) = \mathrm{ind}_S^G(g)(\sigma) = \frac{1}{(S:1)} \sum_{\tau \in G} g_S(\tau\sigma\tau^{-1}).$$

Then $\mathrm{ind}_S^G(g)$ is a class function on G. It is clear that ind_S^G is R-linear.

Since we deal with two groups S and G, we shall denote the scalar product by $\langle\ ,\ \rangle_S$ and $\langle\ ,\ \rangle_G$ when it is taken with these respective groups. The next theorem shows among other things that the restriction and transfer are adjoint to each other with respect to our form.

Theorem 6.1. *Let S be a subgroup of G. Then the following rules hold:*

(i) **(Frobenius reciprocity)** *For $f \in X_R(G)$, and $g \in X_R(S)$ we have*

$$\langle \mathrm{ind}_S^G(g), f\rangle_G = \langle g, \mathrm{Res}_S^G(f)\rangle_S.$$

(ii) $\mathrm{Ind}_S^G(g)f = \mathrm{ind}_S^G(gf_S)$.

(iii) *If $T \subset S \subset G$ are subgroups of G, then*

$$\mathrm{ind}_S^G \circ \mathrm{ind}_T^S = \mathrm{ind}_T^G.$$

(iv) *If $\sigma \in G$ and g^σ is defined by $g^\sigma(\tau^\sigma) = g(\tau)$, where $\tau^\sigma = \sigma^{-1}\tau\sigma$, then*

$$\mathrm{ind}_S^G(g) = \mathrm{ind}_{S^\sigma}^G(g^\sigma).$$

(v) *If ψ is an effective character of S then* $\mathrm{ind}_S^G(\psi)$ *is effective.*

Proof. Let us first prove (ii). We must show that $g^G f = (gf_S)^G$. We have

$$(g^G f)(\tau) = \frac{1}{(S:1)} \sum_{\sigma \in G} g_S(\sigma\tau\sigma^{-1}) f(\tau) = \frac{1}{(S:1)} \sum_{\sigma \in G} g_S(\sigma\tau\sigma^{-1}) f(\sigma\tau\sigma^{-1}).$$

The last expression just obtained is equal to $(gf_S)^G$, thereby proving (ii). Let us sum over τ in G. The only non-zero contributions in our double sum will come from those elements of S which can be expressed in the form $\sigma\tau\sigma^{-1}$ with $\sigma, \tau \in G$. The number of pairs (σ, τ) such that $\sigma\tau\sigma^{-1}$ is equal to a fixed element of G is equal to n (because for every $\lambda \in G$, $(\sigma\lambda, \lambda^{-1}\tau\lambda)$ is another such pair, and the total number of pairs is n^2). Hence our expression is equal to

$$(G:1) \frac{1}{(S:1)} \sum_{\lambda \in S} g(\lambda) f(\lambda).$$

Our first rule then follows from the definitions of the scalar products in G and S respectively.

Now let $g = \psi$ be an effective character of S, and let $f = \chi$ be a simple character of G. From (i) we find that the Fourier coefficients of g^G are integers $\geqq 0$ because $\mathrm{res}_S^G(\chi)$ is an effective character of S. Therefore the scalar product

$$\langle \psi, \mathrm{res}_S^G(\chi) \rangle_S$$

is $\geqq 0$. Hence ψ^G is an effective character of G, thereby proving (v).

In order to prove the transitivity property, it is convenient to use the following notation.

Let $\{c\}$ denote the set of *right* cosets of S in G. For each right coset c, we select a fixed coset representative denoted by $\bar{c}$. Thus if $\bar{c}_1, \ldots, \bar{c}_r$ are these representatives, then

$$G = \bigcup_c c = \bigcup_c S\bar{c} = \bigcup_{i=1}^{r} S\bar{c}_i.$$

Lemma 6.2. *Let g be a class function on S. Then*

$$\mathrm{ind}_S^G(g)(\xi) = \sum_{i=1}^{r} g_S(\bar{c}_i \xi \bar{c}_i^{-1}).$$

Proof. We can split the sum over all $\sigma \in G$ in the definition of the induced function into a double sum

$$\sum_{\sigma \in G} = \sum_{\sigma \in S} \sum_{i=1}^{r}$$

and observe that each term $g_S(\sigma\bar{c}\xi\bar{c}^{-1}\sigma^{-1})$ is equal to $g_S(\bar{c}\xi\bar{c}^{-1})$ if $\sigma \in S$, because g is a class function. Hence the sum over $\sigma \in S$ is enough to cancel the factor $1/(S : 1)$ in front, to give the expression in the lemma.

If $T \subset S \subset G$ are subgroups of G, and if

$$G = \bigcup S\bar{c}_i \quad \text{and} \quad S = \bigcup T\bar{d}_j$$

are decompositions into right cosets, then $\{\bar{d}_j\bar{c}_i\}$ form a system of representatives for the right cosets of T in G. From this the transitivity property (iii) is obvious. We shall leave (iv) as an exercise (trivial, using the lemma).

§7. INDUCED REPRESENTATIONS

Let G be a group and S a subgroup of finite index. Let F be an S-module. We consider the category $\mathcal{C}$ whose objects are S-homomorphisms $\varphi : F \to E$ of F into a G-module E. (We note that a G-module E can be regarded as an S-module by restriction.) If $\varphi' : F \to E'$ is another object in $\mathcal{C}$, we define a morphism $\varphi' \to \varphi$ in $\mathcal{C}$ to be a G-homomorphism $\eta : E' \to E$ making the following diagram commutative:

$$\begin{tikzcd}
 & E' \arrow[dd, "\eta"] \\
F \arrow[ur, "\varphi'"] \arrow[dr, "\varphi"'] & \\
 & E
\end{tikzcd}$$

A universal object in $\mathcal{C}$ is determined up to a unique G-isomorphism. It will be denoted by

$$\operatorname{ind}_S^G : F \to \operatorname{ind}_S^G(F).$$

We shall prove below that a universal object always exists. If $\varphi : F \to E$ is a universal object, we call E **an induced module**. It is uniquely determined, up to a unique G-isomorphism making a diagram commutative. For convenience, we shall select one induced module such that φ is an inclusion. We shall then call this particular module $\operatorname{ind}_S^G(F)$ **the** G-module **induced** by F. In particular, given an S-homomorphism φ: $F \to E$ into a G-module E, there is a unique G-homomorphism φ_*: $\operatorname{ind}_S^G(F) \to E$ making the following diagram commutative:

$$\begin{tikzcd}
 & \operatorname{ind}_S^G(F) \arrow[dd, "\varphi_* = \operatorname{ind}_S^G(\varphi)"] \\
F \arrow[ur, "\operatorname{ind}_S^G"] \arrow[dr, "\varphi"'] & \\
 & E
\end{tikzcd}$$

The association $\varphi \mapsto \mathrm{ind}_S^G(\varphi)$ then induces an isomorphism

$$\boxed{\mathrm{Hom}_G(\mathrm{ind}_S^G(F), E) \approx \mathrm{Hom}_S(F, \mathrm{res}_S^G(E)),}$$

for an S-module F and a G-module E. We shall see in a moment that ind_S^G is a functor from Mod(S) to Mod(G), and the above formula may be described as saying that **induction is the adjoint functor of restriction**. One also calls this relation **Frobenius reciprocity for modules**, because Theorem 6.1(i) is a corollary.

Sometimes, if the reference to F as an S-module is clear, we shall omit the subscript S, and write simply

$$\mathrm{ind}^G(F)$$

for the induced module.

Let $f: F' \to F$ be an S-homomorphism. If

$$\varphi_S^G : F' \to \mathrm{ind}_S^G(F')$$

is a G-module induced by F', then there exists a unique G-homomorphism $\mathrm{ind}_S^G(F') \to \mathrm{ind}_S^G(F)$ making the following diagram commutative:

$$\begin{tikzcd}
F' \arrow[r, "\varphi_S^G"] \arrow[d, "f"'] \arrow[dr, dashed] & \mathrm{ind}_S^G(F') \arrow[d, "\mathrm{ind}_S^G(f)"] \\
F \arrow[r, "\varphi_S^G"'] & \mathrm{ind}_S^G(F)
\end{tikzcd}$$

It is simply the G-homomorphism corresponding to the universal property for the S-homomorphism $\varphi_G^S \circ f$, represented by a dashed line in our diagram. *Thus* ind_S^G *is a functor, from the category of S-modules to the category of G-modules.*

From the universality and uniqueness of the induced module, we get some formal properties:

ind_S^G *commutes with direct sums: If we have an S-direct sum* $F \oplus F'$, *then*

$$\mathrm{ind}_S^G(F \oplus F') \approx \mathrm{ind}_S^G(F) \oplus \mathrm{ind}_S^G(F'),$$

the direct sum on the right being a G-direct sum.

If $f, g : F' \to F$ *are S-homomorphisms, then*

$$\mathrm{ind}_S^G(f + g) = \mathrm{ind}_S^G(f) + \mathrm{ind}_S^G(g).$$

If $T \subset S \subset G$ *are subgroups of G, and F is a T-module, then*

$$\mathrm{ind}_S^G \circ \mathrm{ind}_T^S(F) \approx \mathrm{ind}_T^G(F).$$

In all three cases, the equality between the left member and the right member of our equations follows at once by using the uniqueness of the universal object. We shall leave the verifications to the reader.

To prove the existence of the induced module, we let $M_G^S(F)$ be the additive group of functions $f : G \to F$ satisfying

$$\sigma f(\xi) = f(\sigma\xi)$$

for $\sigma \in S$ and $\xi \in G$. We define an operation of G on $M_G^S(F)$ by letting

$$(\sigma f)(\xi) = f(\xi\sigma)$$

for $\sigma, \xi \in G$. It is then clear that $M_G^S(F)$ is a G-module.

Proposition 7.1. *Let $\varphi : F \to M_G^S(F)$ be such that $\varphi(x) = \varphi_x$ is the map*

$$\varphi_x(\tau) = \begin{cases} 0 & \text{if } \tau \notin S \\ \tau x & \text{if } \tau \in S. \end{cases}$$

Then φ is an S-homomorphism, $\varphi : F \to M_G^S(F)$ is universal, and φ is injective. The image of φ consists of those elements $f \in M_G^S(F)$ such that $f(\tau) = 0$ if $\tau \notin S$.

Proof. Let $\sigma \in S$ and $x \in F$. Let $\tau \in G$. Then

$$(\sigma\varphi_x)(\tau) = \varphi_x(\tau\sigma).$$

If $\tau \in S$, then this last expression is equal to $\varphi_{\sigma x}(\tau)$. If $\tau \notin S$, then $\tau\sigma \notin S$, and hence both $\varphi_{\sigma x}(\tau)$ and $\varphi_x(\tau\sigma)$ are equal to 0. Thus φ is an S-homomorphism, and it is immediately clear that φ is injective. Furthermore, if $f \in M_G^S(F)$ is such that $f(\tau) = 0$ if $\tau \notin S$, then from the definitions, we conclude that $f = \varphi_x$ where $x = f(1)$.

There remains to prove that φ is universal. To do this, we shall analyze more closely the structure of $M_G^S(F)$.

Proposition 7.2. *Let $G = \bigcup_{i=1}^{r} S\bar{c}_i$ be a decomposition of G into right cosets. Let F_1 be the additive group of functions in $M_G^S(F)$ having value 0 at elements $\xi \in G$, $\xi \notin S$. Then*

$$M_G^S(F) = \bigoplus_{i=1}^{r} \bar{c}_i^{-1} F_1,$$

the direct sum being taken as an abelian group.

Proof. For each $f \in M_G^S(F)$, let f_i be the function such that

$$f_i(\xi) = \begin{cases} 0 & \text{if } \xi \notin S\bar{c}_i \\ f(\xi) & \text{if } \xi \in S\bar{c}_i. \end{cases}$$

For all $\sigma \in S$ we have $f_i(\sigma \bar{c}_i) = (\bar{c}_i f_i)(\sigma)$. It is immediately clear that $\bar{c}_i f_i$ lies in F_1, and

$$f = \sum_{i=1}^{r} \bar{c}_i^{-1}(\bar{c}_i f_i).$$

Thus $M_G^S(F)$ is the sum of the subgroups $\bar{c}_i^{-1} F_1$. It is clear that this sum is direct, as desired.

We note that $\{\bar{c}_1^{-1}, \ldots, \bar{c}_r^{-1}\}$ form a system of representatives for the *left* cosets of S in G. The operation of G on $M_G^S(F)$ is defined by the presceding direct sum decomposition. We see that G permutes the factors transitively. The factor F_1 is S-isomorphic to the original module F, as stated in Proposition 7.1.

Suppose that instead of considering arbitrary modules, we start with a commutative ring R and consider only R-modules E on which we have a representation of G, i.e. a homomorphism $G \to \mathrm{Aut}_R(E)$, thus giving rise to what we call a (G, R)-module. Then it is clear that all our constructions and definitions can be applied in this context. Therefore if we have a representation of S on an R-module F, then we obtain an induced representation of G on $\mathrm{ind}_S^G(F)$. Then we deal with the category $\mathcal{C}$ of S-homomorphisms of an (S, R)-module into a (G, R)-module. To simplify the notation, we may write "G-module" to mean "(G, R)-module" when such a ring R enters as a ring of coefficients.

Theorem 7.3. *Let $\{\lambda_1, \ldots, \lambda_r\}$ be a system of left coset representatives of S in G. There exists a G-module E containing F as an S-submodule, such that*

$$E = \bigoplus_{i=1}^{r} \lambda_i F$$

is a direct sum (as R-modules). Let $\varphi : F \to E$ be the inclusion mapping. Then φ is universal in our category $\mathcal{C}$, i.e. E is an induced module.

Proof. By the usual set-theoretic procedure of replacing F_1 by F in $M_G^S(F)$, obtain a G-module E containing F as a S-submodule, and having the desired direct sum decomposition. Let $\varphi' : F \to E'$ be an S-homomorphism into a G-module E'. We define

$$h : E \to E'$$

by the rule

$$h(\lambda_1 x_1 + \cdots + \lambda_r x_r) = \lambda_1 \varphi'(x_1) + \cdots + \lambda_r \varphi'(x_r)$$

for $x_i \in F$. This is well defined since our sum for E is direct. We must show that h is a G-homomorphism. Let $\sigma \in G$. Then

$$\sigma \lambda_i = \lambda_{\sigma(i)} \tau_{\sigma, i}$$

where $\sigma(i)$ is some index depending on σ and i, and $\tau_{\sigma, i}$ is an element of S, also depending on σ, i. Then

$$h(\sigma\lambda_i x_i) = h(\lambda_{\sigma(i)}\tau_{\sigma,i}x_i) = \lambda_{\sigma(i)}\varphi'(\tau_{\sigma,i}x_i).$$

Since φ' is an S-homomorphism, we see that this expression is equal to

$$\lambda_{\sigma(i)}\tau_{\sigma,i}\varphi'(x_i) = \sigma h(\lambda_i x_i).$$

By linearity, we conclude that h is a G-homomorphism, as desired.

In the next proposition we return to the case when R is our field k.

Proposition 7.4. *Let ψ be the character of the representation of S on the k-space F. Let E be the space of an induced representation. Then the character χ of E is equal to the induced character ψ^G, i.e. is given by the formula*

$$\chi(\xi) = \sum_c \psi_0(\bar{c}\xi\bar{c}^{-1}),$$

where the sum is taken over the right cosets c of S in G, $\bar{c}$ is a fixed coset representative for c, and ψ_0 is the extension of ψ to G obtained by setting $\psi_0(\sigma) = 0$ if $\sigma \notin S$.

Proof. Let $\{w_1, \ldots, w_m\}$ be a basis for F over k. We know that

$$E = \bigoplus \bar{c}^{-1}F.$$

Let σ be an element of G. The elements $\{\overline{c\sigma}^{-1}w_j\}_{c,j}$ form a basis for E over k.

We observe that $\bar{c}\sigma\overline{c\sigma}^{-1}$ is an element of S because

$$S\bar{c}\sigma = Sc\sigma = S\overline{c\sigma}.$$

We have

$$\sigma(\overline{c\sigma}^{-1}w_j) = \bar{c}^{-1}(\bar{c}\sigma\overline{c\sigma}^{-1})w_j.$$

Let

$$(\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}$$

be the components of the matrix representing the effect of $\bar{c}\sigma\overline{c\sigma}^{-1}$ on F with respect to the basis $\{w_1, \ldots, w_m\}$. Then the action of σ on E is given by

$$\begin{aligned}\sigma(\overline{c\sigma}^{-1}w_j) &= \bar{c}^{-1}\sum_\mu (\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}w_\mu \\ &= \sum_\mu (\bar{c}\sigma\overline{c\sigma}^{-1})_{\mu j}(\bar{c}^{-1}w_\mu).\end{aligned}$$

By definition,

$$\chi(\sigma) = \sum_{c\sigma = c}\sum_j (\bar{c}\sigma\overline{c\sigma}^{-1})_{jj}.$$

But $c\sigma = c$ if and only if $\bar{c}\sigma\bar{c}^{-1} \in S$. Furthermore,

$$\psi(\bar{c}\sigma\bar{c}^{-1}) = \sum_j (\bar{c}\sigma\bar{c}^{-1})_{jj}.$$

Hence

$$\chi(\sigma) = \sum_c \psi_0(\bar{c}\sigma\bar{c}^{-1}),$$

as was to be shown.

Remark. Having given an explicit description of the representation space for an induced character, we have in some sense completed the more elementary part of the theory of induced characters. Readers interested in seeing an application can immediately read §12.

Double cosets

Let G be a group and let S be a subgroup. To avoid superscripts we use the following notation. Let $\gamma \in G$. We write

$$[\gamma]S = \gamma S \gamma^{-1} \quad \text{and} \quad S[\gamma] = \gamma^{-1} S \gamma.$$

We shall suppose that S has finite index. We let H be a subgroup. A subset of G of the form $H\gamma S$ is called a **double coset**. As with cosets, it is immediately verified that G is a disjoint union of double cosets. We let $\{\gamma\}$ be a family of double coset representatives, so we have the disjoint union

$$G = \bigcup_\gamma H\gamma S.$$

For each γ we have a decomposition into ordinary cosets

$$H = \bigcup_{\tau_\gamma} \tau_\gamma [H \cap [\gamma]S),$$

where $\{\tau_\gamma\}$ is a finite family of elements of H, depending on γ.

Lemma 7.5. *The elements $\{\tau_\gamma \gamma\}$ form a family of left coset representatives for S in G; that is, we have a disjoint union*

$$G = \bigcup_{\gamma, \tau_\gamma} \tau_\gamma \gamma S.$$

Proof. First we have by hypothesis

$$G = \bigcup_\gamma \bigcup_{\tau_\gamma} \tau_\gamma (H \cap [\gamma]S)\gamma S,$$

and so every element of G can be written in the form

$$\tau_\gamma \gamma s_1 \gamma^{-1} \gamma s_2 = \tau_\gamma \gamma s \quad \text{with} \quad s_1, s_2, s \in S.$$

On the other hand, the elements $\tau_\gamma \gamma$ represent distinct cosets of S, because if $\tau_\gamma \gamma S = \tau_{\gamma'} \gamma' S$, then $\gamma = \gamma'$, since the elements γ represent distinct double cosets, whence τ_γ and $\tau_{\gamma'}$ represent the same coset of $\gamma S \gamma^{-1}$, and therefore are equal. This proves the lemma.

Let F be an S-module. Given $\gamma \in G$, we denote by $[\gamma]F$ the $[\gamma]S$-module such that for $\gamma s \gamma^{-1} \in [\gamma]S$, the operation is given by

$$\gamma s \gamma^{-1} \cdot [\gamma]x = [\gamma]sx.$$

This notation is compatible with the notation that if F is a submodule of a G-module E, then we may form γF either according to the formal definition above, or according to the operation of G. The two are naturally isomorphic (essentially equal). We shall write

$$[\gamma] : F \to \gamma F \text{ or } [\gamma]F$$

for the above isomorphism from the S-module F to the $[\gamma]S$-module γF. If S_1 is a subgroup of S, then by restriction F is also an S_1-module, and we use $[\gamma]$ also in this context, especially for the subgroup $H \cap [\gamma]S$ which is contained in $[\gamma]S$.

Theorem 7.6. *Applied to the S-module F, we have an isomorphism of H-modules*

$$\operatorname{res}_H^G \circ \operatorname{ind}_S^G \approx \bigoplus_\gamma \operatorname{ind}_{H\cap[\gamma]S}^H \circ \operatorname{res}_{H\cap[\gamma]S}^{[\gamma]S} \circ [\gamma]$$

where the direct sum is taken over double coset representatives γ.

Proof. The induced module $\operatorname{ind}_S^G(F)$ is simply the direct sum

$$\operatorname{ind}_S^G(F) = \bigoplus_{\gamma, \tau_\gamma} \tau_\gamma \gamma F$$

by Lemma 7.5, which gives us coset representatives of S in G, and Theorem 7.3. On the other hand, for each γ, the module

$$\bigoplus_{\tau_\gamma} \tau_\gamma \gamma F$$

is a representation module for the induced representation from $H \cap [\gamma]S$ on γF to H. Taking the direct sum over γ, we get the right-hand side of the expression in the theorem, and thus prove the theorem.

Remark. The formal relation of Theorem 7.6 is one which occurred in Artin's formalism of induced characters and L-functions; *cf.* the exercises and [La 70], Chapter XII, §3. For applications to the cohomology of groups, see [La 96]. The formalism also emerged in Mackey's work [Ma 51], [Ma 53], which we shall now consider more systematically. The rest of this section is due to Mackey. For more extensive results and applications, see Curtis-Reiner [CuR 81], especially Chapter 1. See also Exercises 15, 16, and 17.

To deal more systematically with conjugations, we make some general functorial remarks. Let E be a G-module. Possibly one may have a commutative ring R such that E is a (G, R)-module. We shall deal systematically with the functors

Hom_G, $E^\vee$, and the tensor product. Let

$$\lambda : E \to \lambda E$$

by a R-isomorphism. Then interpreting elements of G as endomorphisms of E we obtain a group $\lambda G \lambda^{-1}$ operating on λE. We shall also write $[\lambda]G$ instead of $\lambda G \lambda^{-1}$. Let E_1, E_2 be (G, R)-modules. Let $\lambda_1 : E_i \to \lambda_i E_i$ be R-isomorphisms. Then we have a natural R-isomorphism

$$\text{(1)} \qquad \lambda_2 \mathrm{Hom}_G(E_1, E_2)\lambda_1^{-1} = \mathrm{Hom}_{\lambda_2 G \lambda_1^{-1}}(\lambda_1 E_1, \lambda_2 E_2),$$

and especially

$$[\lambda]\mathrm{Hom}_G(E, E) = \mathrm{Hom}_{[\lambda]G}(\lambda E, \lambda E).$$

As a special case of the general situation, let H, S be subgroups of G, and let F_1, F_2 be (H, R)- and (S, R)-modules respectively, and let σ, $\tau \in G$. *Suppose that* $\sigma^{-1}\tau$ lies in the double coset $D = H\gamma S$. Then we have an R-isomorphism

$$\text{(2)} \qquad \mathrm{Hom}_{[\sigma]H \cap [\tau]S}([\sigma]F_1, [\tau]F_2) \approx \mathrm{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2).$$

This is immediate by conjugation, writing $\tau = \sigma h \gamma s$ with $h \in H$, $s \in S$, conjugating first with $[\sigma h]^{-1}$, and then observing that for $s \in S$, and an S-module F, we have $[s]S = S$, and $[s^{-1}]F$ is isomorphic to F. In light of (2), we see that the R-module on the left-hand side depends only on the double coset. Let D be a double coset. We shall use the notation

$$M_D(F_1, F_2) = \mathrm{Hom}_{H \cap [\gamma]S}\,(F_1, [\gamma]F_2)$$

where γ represents the double coset D. With this notation we have:

Theorem 7.7. *Let H, S be subgroups of finite index in G. Let F_1, F_2 be (H, R) and (S, R)-modules respectively. Then we have an isomorphism of R-modules*

$$\mathrm{Hom}_G(\mathrm{ind}_H^G(F_1), \mathrm{ind}_S^G(F_2)) \approx \bigoplus_D M_D(F_1, F_2),$$

where the direct sum is taken over all double cosets $H\gamma S = D$.

Proof. We have the isomorphisms:

$$\begin{aligned}
\mathrm{Hom}_G(\mathrm{ind}_H^G(F_1), \mathrm{ind}_S^G(F_2)) &\approx \mathrm{Hom}_H(F_1, \mathrm{res}_H^G \circ \mathrm{ind}_S^G(F_2)) \\
&\approx \bigoplus_\gamma \mathrm{Hom}_H(F_1, \mathrm{ind}_{H \cap [\gamma]S}^H \circ \mathrm{res}_{H \cap [\gamma]S}^{[\gamma]S} \circ [\gamma]F_2) \\
&\approx \bigoplus_\gamma \mathrm{Hom}_{H \cap [\gamma]S}(F_1, [\gamma]F_2)
\end{aligned}$$

by applying the definition of the induced module in the first and third step, and applying Theorem 7.6 in the second step. Each term in the last expression is what we denoted by $M_D(F_1, F_2)$ if γ is a representative for the double coset D. This proves the theorem.

Corollary 7.8. *Let $R = k = \mathbf{C}$. Let S, H be subgroups of the finite group G. Let $D = H\gamma S$ range over the double cosets, with representatives γ. Let χ be an effective character of H and ψ an effective character of S. Then*

$$\langle \mathrm{ind}_H^G((\chi), \mathrm{ind}_S^G(\psi)\rangle_G = \sum_\gamma \langle \chi, [\gamma]\psi\rangle_{H\cap[\gamma]S}.$$

Proof. Immediate from Theorem 5.17(b) and Theorem 7.7, taking dimensions on the left-hand side and on the right-hand side.

Corollary 7.9. (Irreducibility of the induced character). *Let S be a subgroup of the finite group G. Let $R = k = \mathbf{C}$. Let ψ be an effective character of S. Then* $\mathrm{ind}_S^G(\psi)$ *is irreducible if and only if ψ is irreducible and*

$$\langle \psi, [\gamma]\psi\rangle_{S\cap[\gamma]S} = 0$$

for all $\gamma \in G$, $\gamma \notin S$.

Proof. Immediate from Corollary 7.8 and Theorem 5.17(a). It is of course trivial that if ψ is reducible, then so is the induced character.

Another way to phrase Corollary 7.9 is as follows. Let F, F' be representation spaces for S (over $\mathbf{C}$). We call F, F' **disjoint** if no simple S-space occurs both in F and F'. Then Corollary 7.9 can be reformulated:

Corollary 7.9′. *Let S be a subgroup of the finite group G. Let F be an (S, k)-space (with $k = \mathbf{C}$). Then* $\mathrm{ind}_S^G(F)$ *is simple if and only if F is simple and for all $\gamma \in G$ and $\gamma \notin S$, the $S \cap [\gamma]S$-modules F and $[\gamma]F$ are disjoint.*

Next we have the commutation of the dual and induced representations.

Theorem 7.10. *Let S be a subgroup of G and let F be a finite free R-module. Then there is a G-isomorphism*

$$\mathrm{ind}_S^G(F^\vee) \approx (\mathrm{ind}_S^G(F))^\vee .$$

Proof. Let $G = \bigcup \lambda_i S$ be a left coset decomposition. Then, as in Theorem 7.3, we can express the representation space for $\mathrm{ind}_S^G(F)$ as

$$\mathrm{ind}_S^G(F) = \bigoplus \lambda_i F.$$

We may select $\lambda_1 = 1$ (unit element of G). There is a unique R-homomorphism

$$f : F^\vee \to (\mathrm{ind}_S^G(F))^\vee$$

such that for $\varphi \in F^\vee$ and $x \in F$ we have

$$f(\varphi)(\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \varphi(x) & \text{if } i = 1, \end{cases}$$

which is in fact an R-isomorphism of $F^\vee$ on $(\lambda_1 F)^\vee$. We claim that it is an S-

homomorphism. This is a routine verification, which we write down. We have

$$f([\sigma]\varphi)(\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \sigma(\varphi(\sigma^{-1}x)) & \text{if } i = 1. \end{cases}$$

On the other hand, note that if $\sigma \in S$ then $\sigma^{-1}\lambda_1 \in S$ so $\sigma^{-1}\lambda_1 x \in \lambda_1 F$ for $x \in F$; but if $\sigma \notin S$, then $\sigma^{-1}\lambda_i \notin S$ for $i \neq 1$ so $\sigma^{-1}\lambda_i x \notin \lambda_1 F$. Hence

$$[\sigma](f(\varphi))(\lambda_1 x) = \sigma f(\varphi)(\sigma^{-1}\lambda_i x) = \begin{cases} 0 & \text{if } i \neq 1 \\ \sigma(\varphi(\sigma^{-1}x)) & \text{if } i = 1. \end{cases}$$

This proves that f commutes with the action of S.

By the universal property of the induced module, it follows that there is a unique (G, R)-homomorphism

$$\operatorname{ind}_S^G(f) : \operatorname{ind}_S^G(F^\vee) \to (\operatorname{ind}_S^G(F))^\vee,$$

which must be an isomorphism because f was an isomorphism on its image, the λ_1-component of the induced module. This concludes the proof of the theorem.

Theorems and definitions with Hom have analogues with the tensor product. We start with the analogue of the definition.

Theorem 7.11. *Let S be a subgroup of finite index in G. Let F be an S-module, and E a G-module (over the commutative ring R). Then there is an isomorphism*

$$\operatorname{ind}_S^G(\operatorname{res}_S(E) \otimes F) \approx E \otimes \operatorname{ind}_S^G(F).$$

Proof. The G-module $\operatorname{ind}_S^G(F)$ contains F as a summand, because it is the direct sum $\bigoplus \lambda_i F$ with left coset representatives λ_i as in Theorem 7.3. Hence we have a natural S-isomorphism

$$f : \operatorname{res}_S(E) \otimes F \xrightarrow{\approx} E \otimes \lambda_1 F \subset E \otimes \operatorname{ind}_S^G(F).$$

taking the representative λ_1 to be 1 (the unit element of G). By the universal property of induction, there is a G-homomorphism

$$\operatorname{ind}_S^G(f) : \operatorname{ind}_S^G(\operatorname{res}_S(E) \otimes F) \to E \otimes \operatorname{ind}_S^G(F),$$

which is immediately verified to be an isomorphism, as desired. (Note that here it only needed to verify the bijectivity in this last step, which comes from the structure of direct sum as R-modules.)

Before going further, we make some remarks on functorialities. Suppose we have an isomorphism $G \approx G'$, a subgroup H of G corresponding to a subgroup H' of G' under the isomorphism, and an isomorphism $F \approx F'$ from an H-module F to an H'-module F' commuting with the actions of H, H'. Then we get an isomorphism

$$\operatorname{ind}_H^G(F) \approx \operatorname{ind}_{H'}^{G'}(F').$$

In particular, we could take $\sigma \in G$, let $G' = [\sigma]G = G$, $H' = [\sigma]H$ and $F' = [\sigma]F$.

Next we deal with the analogue of Theorem 7.7. We keep the same notation as in that theorem and the discussion preceding it. With the two subgroups H and S, we may then form the tensor product

$$[\sigma]F_1 \otimes [\tau]F_2$$

with $\sigma, \tau \in G$. Suppose $\sigma^{-1}\tau \in D$ for some double coset $D = H\gamma S$. Note that $[\sigma]F_1 \otimes [\tau]F_2$ is a $[\sigma]H \cap [\tau]S$-module. By conjugation we have an isomorphism

$$(3) \qquad \operatorname{ind}^G_{[\sigma]H \cap [\tau]S}([\sigma]F_1 \otimes [\tau]F_2) \approx \operatorname{ind}^G_{H \cap [\gamma]S}(F_1 \otimes [\gamma]F_2).$$

Theorem 7.12. *There is a G-isomorphism*

$$\operatorname{ind}^G_H(F_1) \otimes \operatorname{ind}^G_S(F_2) \approx \bigoplus_\gamma \operatorname{ind}^G_{H \cap [\gamma]S}(F_1 \otimes [\gamma]F_2),$$

where the sum is taken over double coset representatives γ.

Proof. We have:

$$\operatorname{ind}^G_H(F_1) \otimes \operatorname{ind}^G_S(F_2) \approx \operatorname{ind}^G_H(F_1 \otimes \operatorname{res}_H \operatorname{ind}^G_S(F_2)) \qquad \text{by Theorem 7.11}$$

$$\approx \bigoplus_\gamma \operatorname{ind}^G_H(F_1 \otimes \operatorname{ind}^H_{H \cap [\gamma]S} \operatorname{res}^{[\gamma]S}_{H \cap [\gamma]S}([\gamma]F_2) \qquad \text{by Theorem 7.6}$$

$$\approx \bigoplus_\gamma \operatorname{ind}^G_H\left(\operatorname{ind}^H_{H \cap [\gamma]S}\left(\operatorname{res}^H_{H \cap [\gamma]S}(F_1) \otimes \operatorname{res}^{[\gamma]S}_{H \cap [\gamma]S}([\gamma]F_2)\right)\right) \qquad \text{by Theorem 7.7}$$

$$\approx \bigoplus_\gamma \operatorname{ind}^G_{H \cap [\gamma]S}(F_1 \otimes [\gamma]F_2) \qquad \text{by transitivity of induction}$$

where we view $F_1 \cap [\gamma]F_2$ as an $H \cap [\gamma]S$-module in this last line. This proves the theorem.

General comment. This section has given a lot of relations for the induced representations. In light of the cohomology of groups, each formula may be viewed as giving an isomorphism of functors in dimension 0, and therefore gives rise to corresponding isomorphisms for the higher cohomology groups H^q. The reader may see this developed further than the exercises in [La 96].

Bibliography

[CuR 81] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, John Wiley and Sons, 1981

[La 96] S. Lang, *Topics in cohomology of groups*, Springer Lecture Notes 1996

[La 70] S. Lang, *Algebraic Number Theory*, Addison-Wesley, 1970, reprinted by Springer Verlag, 1986

[Ma 51] G. Mackey, On induced representations of groups, *Amer. J. Math.* **73** (1951), pp. 576–592

[Ma 53] G. Mackey, Symmetric and anti-symmetric Kronecker squares of induced representations of finite groups, *Amer. J. Math.* **75** (1953), pp. 387–405

The next three sections, which are essentially independent of each other, give examples of induced representations. In each case, we show that certain representations are either induced from certain well-known types, or are linear combinations with integral coefficients of certain well-known types. The most striking feature is that we obtain all characters as linear combinations of induced characters arising from 1*-dimensional characters. Thus the theory of characters is to a large extent reduced to the study of* 1*-dimensional, or abelian characters.*

§8. POSITIVE DECOMPOSITION OF THE REGULAR CHARACTER

Let G be a finite group and let k be the complex numbers. We let 1_G be the trivial character, and r_G denote the regular character.

Proposition 8.1. *Let H be a subgroup of G, and let ψ be a character of H. Let ψ^G be the induced character. Then the multiplicity of 1_H in ψ is the same as the multiplicity of 1_G in ψ^G.*

Proof. By Theorem 6.1 (i), we have

$$\langle \psi, 1_H \rangle_H = \langle \psi^G, 1_G \rangle_G.$$

These scalar products are precisely the multiplicities in question.

Proposition 8.2. *The regular representation is the representation induced by the trivial character on the trivial subgroup of G.*

Proof. This follows at once from the definition of the induced character

$$\psi^G(\tau) = \sum_{\sigma \in G} \psi_H(\sigma\tau\sigma^{-1}),$$

taking $\psi = 1$ on the trivial subgroup.

Corollary 8.3. *The multiplicity of 1_G in the regular character r_G is equal to* 1.

We shall now investigate the character

$$u_G = r_G - 1_G.$$

Theorem 8.4. (Aramata). *The character nu_G is a linear combination with positive integer coefficients of characters induced by* 1*-dimensional characters of cyclic subgroups of G.*

The proof consists of two propositions, which give an explicit description of the induced characters. I am indebted to Serre for the exposition, derived from Brauer's.

If A is a cyclic group of order a, we define the function θ_A on A by the conditions:

$$\theta_A(\sigma) = \begin{cases} a & \text{if } \sigma \text{ is a generator of } A \\ 0 & \text{otherwise.} \end{cases}$$

We let $\lambda_A = \varphi(a)r_A - \theta_A$ (where φ is the Euler function), and $\lambda_A = 0$ if $a = 1$. The desired result is contained in the following two propositions.

Proposition 8.5. *Let G be a finite group of order n. Then*

$$nu_G = \sum \lambda_A^G,$$

the sum being taken over all cyclic subgroups of G.

Proof. Given two class functions χ, ψ on G, we have the usual scalar product:

$$\langle \psi, \chi \rangle_G = \frac{1}{n} \sum_{\sigma \in G} \psi(\sigma)\overline{\chi(\sigma)}.$$

Let ψ be any class function on G. Then:

$$\begin{aligned} \langle \psi, nu_G \rangle &= \langle \psi, nr_G \rangle - \langle \psi, n1_G \rangle \\ &= n\psi(1) - \sum_{\sigma \in G} \psi(\sigma). \end{aligned}$$

On the other hand, using the fact that the induced character is the transpose of the restriction, we obtain

$$\begin{aligned} \sum_A \langle \psi, \lambda_A^G \rangle &= \sum_A \langle \psi | A, \lambda_A \rangle \\ &= \sum_A \langle \psi | A, \varphi(a)r_A - \theta_A \rangle \\ &= \sum_A \varphi(a)\psi(1) - \sum_A \frac{1}{a} \sum_{\sigma \text{ gen } A} a\psi(\sigma) \\ &= n\psi(1) - \sum_{\sigma \in G} \psi(\sigma). \end{aligned}$$

Since the functions on the right and left of the equality sign in the statement of our proposition have the same scalar product with an arbitrary function, they are equal. This proves our proposition.

Proposition 8.6. *If $A \neq \{1\}$, the function λ_A is a linear combination of irreducible nontrivial characters of A with positive integral coefficients.*

Proof. If A is cyclic of prime order, then by Proposition 8.5, we know that $\lambda_A = nu_A$, and our assertion follows from the standard structure of the regular representation.

In order to prove the assertion in general, it suffices to prove that the Fourier coefficients of λ_A with respect to a character of degree 1 are integers $\geqq 0$. Let ψ be a character of degree 1. We take the scalar product with respect to A, and obtain:

$$\begin{aligned} \langle \psi, \lambda_A \rangle &= \varphi(a)\psi(1) - \sum_{\sigma \text{ gen}} \psi(\sigma) \\ &= \varphi(a) - \sum_{\sigma \text{ gen}} \psi(\sigma) \\ &= \sum_{\sigma \text{ gen}} (1 - \psi(\sigma)). \end{aligned}$$

The sum $\sum \psi(\sigma)$ taken over generators of A is an algebraic integer, and is in fact a rational number (for any number of elementary reasons), hence a rational integer. Furthermore, if ψ is non-trivial, all real parts of

$$1 - \psi(\sigma)$$

are > 0 if $\sigma \neq \text{id}$ and are 0 if $\sigma = \text{id}$. From the last two inequalities, we conclude that the sums must be equal to a positive integer. If ψ is the trivial character, then the sum is clearly 0. Our proposition is proved.

Remark. Theorem 8.4 and Proposition 8.6 arose in the context of zeta functions and L-functions, in Aramata's proof that the zeta function of a number field divides the zeta function of a finite extension [Ar 31], [Ar 33]. See also Brauer [Br 47a], [Br 47b]. These results were also used by Brauer in showing an asymptotic behavior in algebraic number theory, namely

$$\log(hR) \sim \log \mathbf{D}^{1/2} \text{ for } [k : \mathbf{Q}]/\log \mathbf{D} \to 0,$$

where h is the number of ideal classes in a number field k, R is the regulator, and $\mathbf{D}$ is the absolute value of the discriminant. For an exposition of this application, see [La 70], Chapter XVI.

Bibliography

[Ar 31] H. Aramata, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **7** (1931), pp. 334–336

[Ar 33] H. Aramata, Über die Teilbarkeit der Dedekindschen Zetafunktionen, *Proc. Imp. Acad. Tokyo* **9** (1933), pp. 31–34

[Br 47a] R. Brauer, On the zeta functions of algebraic number fields, *Amer. J. Math.* **69** (1947), pp. 243–250

[Br 47b] R. Brauer, On Artin's L-series with general group characters, *Ann. Math.* **48** (1947), pp. 502–514

[La 70] S. Lang, *Algebraic Number Theory*, Springer Verlag (reprinted from Addison-Wesley, 1970)

§9. SUPERSOLVABLE GROUPS

Let G be a finite group. We shall say that G is **supersolvable** if there exists a sequence of subgroups

$$\{1\} \subset G_1 \subset G_2 \subset \cdots \subset G_m = G$$

such that each G_i is normal in G, and G_{i+1}/G_i is cyclic of prime order.

From the theory of p-groups, we know that every p-group is super-solvable, and so is the direct product of a p-group with an abelian group.

Proposition 9.1. *Every subgroup and every factor group of a super-solvable group is supersolvable.*

Proof. Obvious, using the standard homomorphism theorems.

Proposition 9.2. *Let G be a non-abelian supersolvable group. Then there exists a normal abelian subgroup which contains the center properly.*

Proof. Let C be the center of G, and let $\bar{G} = G/C$. Let $\bar{H}$ be a normal subgroup of prime order in $\bar{G}$ and let H be its inverse image in G under the canonical map $G \to G/C$. If σ is a generator of $\bar{H}$, then an inverse image σ of $\bar{\sigma}$, together with C, generate H. Hence H is abelian, normal, and contains the center properly.

Theorem 9.3. (Blichfeldt). *Let G be a supersolvable group, let k be algebraically closed. Let E be a simple (G, k)-space. If* $\dim_k E > 1$, *then there exists a proper subgroup H of G and a simple H-space F such that E is induced by F.*

Proof. Since a simple representation of an abelian group is 1-dimensional, our hypothesis implies that G is not abelian.

We shall first give the proof of our theorem under the additional hypothesis that E is faithful. (This means that $\sigma x = x$ for all $x \in E$ implies $\sigma = 1$.) It will be easy to remove this restriction at the end.

Lemma 9.4. *Let G be a finite group, and assume k algebraically closed. Let E be a simple, faithful G-space over k. Assume that there exists a normal abelian subgroup H of G containing the center of G properly. Then there exists a proper subgroup H_1 of G containing H, and a simple H_1-space F such that E is the induced module of F from H_1 to G.*

Proof. We view E as an H-space. It is a direct sum of simple H-spaces, and since H is abelian, such simple H-space is 1-dimensional.

Let $v \in E$ generate a 1-dimensional H-space. Let ψ be its character. If $w \in E$ also generates a 1-dimensional H-space, with the same character ψ, then for all $a, b \in k$ and $\tau \in H$ we have

$$\tau(av + bw) = \psi(\tau)(av + bw).$$

If we denote by F_ψ the subspace of E generated by all 1-dimensional H-subspaces having the character ψ, then we have an H-direct sum decomposition

$$E = \bigoplus_{\psi} F_\psi.$$

We contend that $E \neq F_\psi$. Otherwise, let $v \in E$, $v \neq 0$, and $\sigma \in G$. Then $\sigma^{-1}v$ is a 1-dimensional H-space by assumption, and has character ψ. Hence for $\tau \in H$,

$$\tau(\sigma^{-1}v) = \psi(\tau)\sigma^{-1}v$$

$$(\sigma\tau\sigma^{-1})v = \sigma\psi(\tau)\sigma^{-1}v = \psi(\tau)v.$$

This shows that $\sigma\tau\sigma^{-1}$ and τ have the same effect on the element v of E. Since H is not contained in the center of G, there exist $\tau \in H$ and $\sigma \in G$ such that $\sigma\tau\sigma^{-1} \neq \tau$, and we have contradicted the assumption that E is faithful.

We shall prove that G permutes the spaces F_ψ transitively.

Let $v \in F_\psi$. For any $\tau \in H$ and $\sigma \in G$, we have

$$\tau(\sigma v) = \sigma(\sigma^{-1}\tau\sigma)v = \sigma\psi(\sigma^{-1}\tau\sigma)v = \psi_\sigma(\tau)\sigma v,$$

where ψ_σ is the function on H given by $\psi_\sigma(\tau) = \psi(\sigma^{-1}\tau\sigma)$. This shows that σ maps F_ψ into F_{ψ_σ}. However, by symmetry, we see that σ^{-1} maps F_{ψ_σ} into F_ψ, and the two maps σ, σ^{-1} give inverse mappings between F_{ψ_σ} and F_ψ. Thus G permutes the spaces $\{F_\psi\}$.

Let $E' = GF_{\psi_0} = \sum \sigma F_{\psi_0}$ for some fixed ψ_0. Then E' is a G-subspace of E, and since E was assumed to be simple, it follows that $E' = E$. This proves that the spaces $\{F_\psi\}$ are permuted transitively.

Let $F = F_{\psi_1}$ for some fixed ψ_1. Then F is an H-subspace of E. Let H_1 be the subgroup of all elements $\tau \in G$ such that $\tau F = F$. Then $H_1 \neq G$ since $E \neq F_\psi$. *We contend that F is a simple H_1-subspace, and that E is the induced space of F from H_1 to G.*

To see this, let $G = \bigcup H_1\bar{c}$ be a decomposition of G in terms of right cosets of H_1. Then the elements $\{\bar{c}^{-1}\}$ form a system of left coset representatives of H_1. Since

$$E = \sum_{\sigma \in G} \sigma F$$

it follows that

$$E = \sum_{c} \bar{c}^{-1}F.$$

We contend that this last sum is direct, and that F is a simple H_1-space.

Since G permutes the spaces $\{F_\psi\}$, we see by definition that H_1 is the isotropy group of F for the operation of G on this set of spaces, and hence that the elements of the orbit are precisely $\{\bar{c}^{-1}F\}$, as c ranges over all the cosets. Thus the spaces $\{\bar{c}^{-1}F\}$ are distinct, and we have a direct sum decomposition

$$E = \bigoplus_c \bar{c}^{-1}F.$$

If W is a proper H_1-subspace of F, then $\bigoplus \bar{c}^{-1}W$ is a proper G-subspace of E, contradicting the hypothesis that E is simple. This proves our assertions.

We can now apply Theorem 7.3 to conclude that E is the induced module from F, thereby proving Theorem 9.3, in case E is assumed to be faithful.

Suppose now that E is not faithful. Let G_0 be the normal subgroup of G which is the kernel of the representation $G \to \mathrm{Aut}_k(E)$. Let $\bar{G} = G/G_0$. Then E gives a faithful representation of $\bar{G}$. As E is not 1-dimensional, then $\bar{G}$ is not abelian and there exists a proper normal subgroup $\bar{H}$ of $\bar{G}$ and a simple $\bar{H}$-space F such that

$$E = \mathrm{ind}_{\bar{H}}^{\bar{G}}(F).$$

Let H be the inverse image of $\bar{H}$ in the natural map $G \to \bar{G}$. Then $H \supset G_0$, and F is a simple H-space. In the operation of $\bar{G}$ as a permutation group of the k-subspaces $\{\sigma F\}_{\sigma \in G}$, we know that $\bar{H}$ is the isotropy group of one component. Hence H is the isotropy group in G of this same operation, and hence applying Theorem 7.3 again, we conclude that E is induced by F in G, i.e.

$$E = \mathrm{ind}_H^G(F),$$

thereby proving Theorem 9.3.

Corollary 9.5. *Let G be a product of a p-group and a cyclic group, and let k be algebraically closed. If E is a simple (G, k)-space and is not 1-dimensional, then E is induced by a 1-dimensional representation of some subgroup.*

Proof. We apply the theorem step by step using the transitivity of induced representations until we get a 1-dimensional representation of a subgroup.

§10. BRAUER'S THEOREM

We let $k = \mathbf{C}$ be the field of complex numbers. We let R be a subring of k. We shall deal with $X_R(G)$, i.e. the ring consisting of all linear combinations with coefficients in R of the simple characters of G over k. (It is a ring by Proposition 2.1.)

Let $H = \{H_\alpha\}$ be a fixed family of subgroups of G, indexed by indices $\{\alpha\}$. We let $V_R(G)$ be the additive subgroup of $X_R(G)$ generated by all the functions which are induced by functions in $X_R(H_\alpha)$ for some H_α in our family. In other words,

$$V_R(G) = \sum_\alpha \operatorname{ind}_{H_\alpha}^G(X_R(H_\alpha)).$$

We could also say that $V_R(G)$ is the subgroup generated over R by all the characters induced from all the H_α.

Lemma 10.1. *$V_R(G)$ is an ideal in $X_R(G)$.*

Proof. This is immediate from Theorem 6.1.

For many applications, the family of subgroups will consist of "elementary" subgroups: Let p be a prime number. By a **p-elementary group** we shall mean the product of a p-group and a cyclic group (whose order may be assumed prime to p, since we can absorb the p-part of a cyclic factor into the p-group). An element $\sigma \in G$ is said to be **p-regular** if its period is prime to p, and **p-singular** if its period is a power of p. Given $x \in G$, we can write in a unique way

$$x = \sigma\tau$$

where σ is p-singular, τ is p-regular, and σ, τ commute. Indeed, if $p^r m$ is the period of x, with m prime to p, then $1 = \nu p^r + \mu m$ whence $x = (x^m)^\mu (x^{p^r})^\nu$ and we get our factorization. It is clearly unique, since the factors have to lie in the cyclic subgroup generated by x. We call the two factors the **p-singular** and **p-regular factors** of x respectively.

The above decomposition also shows:

Proposition 10.2. *Every subgroup and every factor group of a p-elementary group is p-elementary. If S is a subgroup of the p-elementary group $P \times C$, where P is a p-group, and C is cyclic, of order prime to p, then*

$$S = (S \cap P) \times (S \cap C).$$

Proof. Clear.

Our purpose is to show, among other things, that if our family $\{H_\alpha\}$ is such that every p-elementary subgroup of G is contained in some H_α, then $V_R(G) = X_R(G)$ for every ring R. It would of course suffice to do it for $R = \mathbf{Z}$, but for our purposes, it is necessary to prove the result first using a bigger ring. The main result is contained in Theorems 10.11 and 10.13, due to Brauer. We shall give an exposition of Brauer-Tate (*Annals of Math.*, July 1955).

We let R be the ring $\mathbf{Z}[\zeta]$ where ζ is a primitive n-th root of unity. There exists a basis of R as a $\mathbf{Z}$-module, namely $1, \zeta, \dots, \zeta^{N-1}$ for some integer N. This is a trivial fact, and we can take N to be the degree of the irreducible polynomial of ζ over $\mathbf{Q}$. This irreducible polynomial has leading coefficient 1, and has integer coefficients, so the fact that

$$1, \zeta, \ldots, \zeta^{N-1}$$

form a basis of $\mathbf{Z}[\zeta]$ follows from the Euclidean algorithm. We don't need to know anything more about this degree N.

We shall prove our assertion first for the above ring R. The rest then follows by using the following lemma.

Lemma 10.3. *If $d \in \mathbf{Z}$ and the constant function $d.1_G$ belongs to V_R then $d.1_G$ belongs to $V_{\mathbf{Z}}$.*

Proof. We contend that $1, \zeta, \ldots, \zeta^{N-1}$ are linearly independent over $X_{\mathbf{Z}}(G)$. Indeed, a relation of linear dependence would yield

$$\sum_{\nu=1}^{s} \sum_{j=0}^{N-1} c_{\nu j} \chi_\nu \zeta^j = 0$$

with integers $c_{\nu j}$ not all 0. But the simple characters are linearly independent over k. The above relation is a relation between these simple characters with coefficients in R, and we get a contradiction. We conclude therefore that

$$V_R = V_{\mathbf{Z}} \oplus V_{\mathbf{Z}}\zeta \oplus \cdots \oplus V_{\mathbf{Z}}\zeta^{N-1}$$

is a direct sum (of abelian groups), and our lemma follows.

If we can succeed in proving that the constant function 1_G lies in $V_R(G)$, then by the lemma, we conclude that it lies in $V_{\mathbf{Z}}(G)$, and since $V_{\mathbf{Z}}(G)$ is an ideal, that $X_{\mathbf{Z}}(G) = V_{\mathbf{Z}}(G)$.

To prove our theorem, we need a sequence of lemmas.

Two elements x, x' of G are said to be **p-conjugate** if their p-regular factors are conjugate in the ordinary sense. It is clear that p-conjugacy is an equivalence relation, and an equivalence class will be called a **p-conjugacy class**, or simply a **p-class**.

Lemma 10.4. *Let $f \in X_R(G)$, and assume that $f(\sigma) \in \mathbf{Z}$ for all $\sigma \in G$. Then f is constant* mod p *on every p-class.*

Proof. Let $x = \sigma\tau$, where σ is p-singular, and τ is p-regular, and σ, τ commute. It will suffice to prove that

$$f(x) \equiv f(\tau) \pmod{p}.$$

Let H be the cyclic subgroup generated by x. Then the restriction of f to H can be written

$$f_H = \sum a_j \psi_j$$

with $a_j \in R$, and ψ_j being the simple characters of H, hence homomorphisms of H into k^*. For some power p^r we have $x^{p^r} = \tau^{p^r}$, whence $\psi_j(x)^{p^r} = \psi_j(\tau)^{p^r}$, and hence

$$f(x)^{p^r} \equiv f(\tau)^{p^r} \pmod{pR}.$$

We now use the following lemma.

Lemma 10.5. *Let $R = \mathbf{Z}[\zeta]$ be as before. If $a \in \mathbf{Z}$ and $a \in pR$ then $a \in p\mathbf{Z}$.*

Proof. This is immediate from the fact that R has a basis over $\mathbf{Z}$ such that 1 is a basis element.

Applying Lemma 10.5, we conclude that $f(x) \equiv f(\tau) \pmod{p}$, because $b^{p^r} \equiv b \pmod{p}$ for every integer b.

Lemma 10.6. *Let τ be p-regular in G, and let T be the cyclic subgroup generated by τ. Let C be the subgroup of G consisting of all elements commuting with τ. Let P be a p-Sylow subgroup of C. Then there exists an element $\psi \in X_R(T \times P)$ such that the induced function $f = \psi^G$ has the following properties:*

(i) $f(\sigma) \in \mathbf{Z}$ *for all* $\sigma \in G$.

(ii) $f(\sigma) = 0$ *if σ does not belong to the p-class of* τ.

(iii) $f(\tau) = (C : P) \not\equiv 0 \pmod{p}$.

Proof. We note that the subgroup of G generated by T and P is a direct product $T \times P$. Let $\psi_1, \ldots, \psi_r$ be the simple characters of the cyclic group T, and assume that these are extended to $T \times P$ by composition with the projection:

$$T \times P \to T \to k^*.$$

We denote the extensions again by $\psi_1, \ldots, \psi_r$. Then we let

$$\psi = \sum_{\nu=1}^{r} \overline{\psi_\nu(\tau)}\psi_\nu.$$

The orthogonality relations for the simple characters of T show that

$$\psi(\tau y) = \psi(\tau) = (T : 1) \quad \text{for} \quad y \in P$$

$$\psi(\sigma) = 0 \quad \text{if} \quad \sigma \in TP, \quad \text{and} \quad \sigma \notin \tau P.$$

We contend that ψ^G satisfies our requirements.

First, it is clear that ψ lies in $X_R(TP)$.

We have for $\sigma \in G$:

$$\psi^G(\sigma) = \frac{1}{(TP : 1)} \sum_{x \in G} \psi_{TP}(x\sigma x^{-1}) = \frac{1}{(P : 1)} \mu(\sigma)$$

where $\mu(\sigma)$ is the number of elements $x \in G$ such that $x\sigma x^{-1}$ lies in τP. The number $\mu(\sigma)$ is divisible by $(P : 1)$ because if an element x of G moves σ into τP by conjugation, so does every element of Px. Hence the values of ψ^G lie in $\mathbf{Z}$.

Furthermore, $\mu(\sigma) \neq 0$ only if σ is p-conjugate to τ, whence our condition (ii) follows.

Finally, we can have $x\tau x^{-1} = \tau y$ with $y \in P$ only if $y = 1$ (because the period of τ is prime to p). Hence $\mu(\tau) = (C : 1)$, and our condition (iii) follows.

Lemma 10.7. *Assume that the family of subgroups $\{H_\alpha\}$ covers G (i.e. every element of G lies in some H_α). If f is a class function on G taking its values in $\mathbf{Z}$, and such that all the values are divisible by $n = (G : 1)$, then f belongs to $V_R(G)$.*

Proof. Let γ be a conjugacy class, and let p be prime to n. Every element of G is p-regular, and all p-subgroups of G are trivial. Furthermore, p-conjugacy is the same as conjugacy. Applying Lemma 10.6, we find that there exists in $V_R(G)$ a function taking the value 0 on elements $\sigma \notin \gamma$, and taking an integral value dividing n on elements of γ. Multiplying this function by some integer, we find that there exists a function in $V_R(G)$ taking the value n for all elements of γ, and the value 0 otherwise. The lemma then follows immediately.

Theorem 10.8. (Artin). *Every character of G is a linear combination with rational coefficients of induced characters from cyclic subgroups.*

Proof. In Lemma 10.7, let $\{H_\alpha\}$ be the family of cyclic subgroups of G. The constant function $n.1_G$ belongs to $V_R(G)$. By Lemma 10.3, this function belongs to $V_{\mathbf{Z}}(G)$, and hence $nX_{\mathbf{Z}}(G) \subset V_{\mathbf{Z}}(G)$. Hence

$$X_{\mathbf{Z}}(G) \subset \frac{1}{n} V_{\mathbf{Z}}(G),$$

thereby proving the theorem.

Lemma 10.9. *Let p be a prime number, and assume that every p-elementary subgroup of G is contained in some H_α. Then there exists a function $f \in V_R(G)$ whose values are in $\mathbf{Z}$, and $\equiv 1 \pmod{p^r}$.*

Proof. We apply Lemma 10.6 again. For each p-class γ, we can find a function f_γ in $V_R(G)$, whose values are 0 on elements outside γ, and $\not\equiv 0 \bmod p$ for elements of γ. Let $f = \sum f_\gamma$, the sum being taken over all p-classes. Then $f(\sigma) \not\equiv 0 \pmod{p}$ for all $\sigma \in G$. Taking $f^{(p-1)p^{r-1}}$ gives what we want.

Lemma 10.10. *Let p be a prime number and assume that every p-elementary subgroup of G is contained in some H_α. Let $n = n_0 p^r$ where n_0 is prime to p. Then the constant function $n_0.1_G$ belongs to $V_{\mathbf{Z}}(G)$.*

Proof. By Lemma 10.3, it suffices to prove that $n_0.1_G$ belongs to $V_R(G)$. Let f be as in Lemma 10.9. Then

$$n_0.1_G = n_0(1_G - f) + n_0 f.$$

Since $n_0(1_G - f)$ has values divisible by $n_0 p^r = n$, it lies in $V_R(G)$ by Lemma 10.7. On the other hand, $n_0 f \in V_R(G)$ because $f \in V_R(G)$. This proves our lemma.

Theorem 10.11. (Brauer). *Assume that for every prime number p, every p-elementary subgroup of G is contained in some H_α. Then $X(G) = V_{\mathbf{Z}}(G)$. Every character of G is a linear combination, with integer coefficients, of characters induced from subgroups H_α.*

Proof. Immediate from Lemma 10.10, since we can find functions $n_0.1_G$ in $V_{\mathbf{Z}}(G)$ with n_0 relatively prime to any given prime number.

Corollary 10.12. *A class function f on G belongs to $X(G)$ if and only if its restriction to H_α belongs to $X(H_\alpha)$ for each α.*

Proof. Assume that the restriction of f to H_α is a character on H_α for each α. By the theorem, we can write

$$1_G = \sum_\alpha c_\alpha \operatorname{ind}_{H_\alpha}^G(\psi_\alpha)$$

where $c_\alpha \in \mathbf{Z}$, and $\psi_\alpha \in X(H_\alpha)$. Hence

$$f = \sum_\alpha c_\alpha \operatorname{ind}_{H_\alpha}^G(\psi_\alpha f_{H_\alpha}),$$

using Theorem 6.1. If $f_{H_\alpha} \in X(H_\alpha)$, we conclude that f belongs to $X(G)$. The converse is of course trivial.

Theorem 10.13. (Brauer). *Every character of G is a linear combination with integer coefficients of characters induced by 1-dimensional characters of subgroups.*

Proof. By Theorem 10.11, and the transitivity of induction, it suffices to prove that every character of a p-elementary group has the property stated in the theorem. But we have proved this in the preceding section, Corollary 9.5.

§11. FIELD OF DEFINITION OF A REPRESENTATION

We go back to the general case of k having characteristic prime to $\#G$. Let E be a k-space and assume we have a representation of G on E. Let k' be an extension field of k. Then G operates on $k' \otimes_k E$ by the rule

$$\sigma(a \otimes x) = a \otimes \sigma x$$

for $a \in k'$ and $x \in E$. This is obtained from the bilinear map on the product $k' \times E$ given by

$$(a, x) \mapsto a \otimes \sigma x.$$

We view $E' = k' \otimes_k E$ as the extension of E by k', and we obtain a representation of G on E'.

Proposition 11.1. *Let the notation be as above. Then the characters of the representations of G on E and on E' are equal.*

Proof. Let $\{v_1, \dots, v_m\}$ be a basis of E over k. Then

$$\{1 \otimes v_1, \dots, 1 \otimes v_m\}$$

is a basis of E' over k'. Thus the matrices representing an element σ of G with respect to the two bases are equal, and consequently the traces are equal.

Conversely, let k' be a field and k a subfield. A representation of G on a k'-space E' is said to be **definable over** k if there exists a k-space E and a representation of G on E such that E' is G-isomorphic to $k' \otimes_k E$.

Proposition 11.2. *Let E, F be simple representation spaces for the finite group G over k. Let k' be an extension of k. Assume that E, F are not G-isomorphic. Then no k'-simple component of $E_{k'}$ appears in the direct sum decomposition of $F_{k'}$ into k'-simple subspaces.*

Proof. Consider the direct product decomposition

$$k[G] = \prod_{\mu=1}^{s(k)} R_\mu(k)$$

over k, into a direct product of simple rings. Without loss of generality, we may assume that E, F are simle left ideals of $k[G]$, and they will belong to distinct factors of this product by assumption. We now take the tensor product with k', getting nothing else but $k'[G]$. Then we obtain a direct product decomposition over k'. Since $R_\nu(k)R_\mu(k) = 0$ if $\nu \neq \mu$, this will actually be given by a direct product decomposition of each factor $R_\mu(k)$:

$$k'[G] = \prod_{\mu=1}^{s(k)} \prod_{i=1}^{m(\mu)} R_{\mu i}(k').$$

Say $E = L_\nu$ and $F = L_\mu$ with $\nu \neq \mu$. Then $R_\mu E = 0$. Hence $R_{\mu i} E_{k'} = 0$ for each $i = 1, \ldots, m(\mu)$. This implies that no simple component of $E_{k'}$ can be G-isomorphic to any one of the simple left ideals of $R_{\mu i}$, and proves what we wanted.

Corollary 11.3. *The simple characters $\chi_1, \ldots, \chi_{s(k)}$ of G over k are linearly independent over any extension k' of k.*

Proof. This follows at once from the proposition, together with the linear independence of the k'-simple characters over k'.

Propositions 11.1 and 11.2 are essentially general statements of an abstract nature. The next theorem uses Brauer's theorem in its proof.

Theorem 11.4. (Brauer). *Let G be a finite group of exponent m. Every representation of G over the complex numbers (or an algebraically closed field of characteristic 0) is definable over the field $\mathbf{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity.*

Proof. Let χ be the character of a representation of G over $\mathbf{C}$, i.e. an effective character. By Theorem 10.13, we can write

$$\chi = \sum_j c_j \operatorname{ind}_{S_j}^G(\psi_j), \qquad c_j \in \mathbf{Z},$$

the sum being taken over a finite number of subgroups S_j, and ψ_j being a 1-dimensional character of S_j. It is clear that each ψ_j is definable over $\mathbf{Q}(\zeta_m)$. Thus the induced character ψ_j^G is definable over $\mathbf{Q}(\zeta_m)$. Each ψ_j^G can be written

$$\psi_j^G = \sum_\mu d_{j\mu}\chi_\mu, \qquad d_{j\mu} \in \mathbf{Z}$$

where $\{\chi_\mu\}$ are the simple characters of G over $\mathbf{Q}(\zeta_m)$. Hence

$$\chi = \sum_\mu \left(\sum_j c_j d_{j\mu} \right) \chi_\mu.$$

The expression of χ as a linear combination of the simple characters over k is unique, and hence the coefficient

$$\sum_j c_j d_{j\mu}$$

is $\geqq 0$. This proves what we wanted.

§12. EXAMPLE: GL_2 OVER A FINITE FIELD

Let F be a field. We view $GL_2(F)$ as operating on the 2-dimensional vector space $V = F^2$. We let F^a be the algebraic closure as usual, and we let $V^a = F^a \times F^a = F^a \otimes V$ (tensor product over F). By **semisimple**, we always mean absolutely semisimple, i.e. semisimple over the algebraic closure F^a. An element $\alpha \in GL_2(F)$ is called **semisimple** if V^a is semisimple over $F^a[\alpha]$. A subgroup is called **semisimple** if all its elements are semisimple.

Let K be a separable quadratic extension of F. Let $\{\omega_1, \omega_2\}$ be a basis of K. Then we have the regular representation of K with respect to this basis, namely multiplication representing K^* as a subgroup of $GL_2(F)$. The elements of norm 1 correspond precisely to the elements of $SL_2(F)$ in the image of K^*. A different choice of basis of K corresponds to conjugation of this image in $GL_2(F)$. Let C_K denote one of these images. Then C_K is called a **non-split Cartan subgroup**. The subalgebra

$$F[C_K] \subset \mathrm{Mat}_2(F)$$

is isomorphic to K itself, and the units of the algebra are therefore the elements of $C_K \approx K^*$.

Lemma 12.1. *The subgroup C_K is a maximal commutative semisimple subgroup.*

Proof. If $\alpha \in GL_2(F)$ commutes with all elements of C_K then α must lie in $F[C_K]$, for otherwise $\{1, \alpha\}$ would be linearly independent over $F[C_K]$, whence $\mathrm{Mat}_2(F)$ would be commutative, which is not the case. Since α is invertible, α is a unit in $F[C_K]$, so $\alpha \in C_K$, as was to be shown.

By the **split Cartan subgroup** we mean the group of diagonal matrices

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \text{ with } a, d \in F^*.$$

We denote the split Cartan by A, or $A(F)$ if the reference to F is needed.

By a **Cartan subgroup** we mean a subgroup conjugate to the split Cartan or to one of the subgroups C_K as above.

Lemma 12.2. *Every maximal commutative semisimple subgroup of $GL_2(F)$ is a Cartan subgroup, and conversely.*

Proof. It is clear that the split Cartan subgroup is maximal commutative semisimple. Suppose that H is a maximal commutative semisimple subgroup of $GL_2(F)$. If H is diagonalizable over F, then H is contained in a conjugate of the split Cartan. On the other hand, suppose H is not diagonalizable over F. It is diagonalizable over the separable closure of F, and the two eigenspaces of dimension 1 give rise to two characters

$$\psi,\ \psi' : H \to F^{s*}$$

of H in the multiplicative group of the separable closure. For each element $\alpha \in H$ the values $\psi(\alpha)$ and $\psi'(\alpha)$ are the eigenvalues of α, and for some element $\alpha \in H$ these eigenvalues are distinct, otherwise H is diagonalizable over F. Hence the pair of elements $\psi(\alpha)$, $\psi'(\alpha)$ are conjugate over F. The image $\psi(H)$ is cyclic, and if $\psi(\alpha)$ generates this image, then we see that $\psi(\alpha)$ generates a quadratic extension K of F. The map

$$\alpha \mapsto \psi(\alpha) \text{ with } \alpha \in H$$

extends to an F-linear mapping, also denoted by ψ, of the algebra $F[H]$ into K. Since $F[H]$ is semisimple, it follows that $\psi : F[H] \to K$ is an isomorphism. Hence ψ maps H into K^*, and in fact maps H onto K^* because H was taken to be maximal. This proves the lemma.

In the above proof, the two characters ψ, ψ' are called the **(eigen)characters of the Cartan subgroup**. In the split case, if α has diagonal elements, a, d then we get the two characters such that $\psi(\alpha) = a$ and $\psi'(\alpha) = d$. In the split case, the values of the characters are in F. In the non-split case, these values are conjugate quadratic over F, and lie in K.

Proposition 12.3. *Let H be a Cartan subgroup of $GL_2(F)$ (split or not). Then H is of index 2 in its normalizer $N(H)$.*

Proof. We may view $GL_2(F)$ as operating on the 2-dimensional vector space $V^a = F^a \oplus F^a$, over the algebraic closure F^a. Whether H is split or not, the eigencharacters are distinct (because of the separability assumption in the non-split case), and an element of the normalizer must either fix or interchange the eigenspaces. If it fixes them, then it lies in H by the maximality of H in Lemma 12.2. If it interchanges them, then it does not lie in H, and generates a unique coset of N/H, so that H is of index 2 in N.

In the split case, a representative of N/A which interchanges the eigenspaces is given by

$$w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In the non-split case, let σ: $K \to K$ be the non-trivial automorphism. Let $\{\alpha, \sigma\alpha\}$ be a normal basis. With respect to this basis, the matrix of σ is precisely the matrix

$$w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Therefore again in this case we see that there exists a non-trivial element in the normalizer of A. Note that it is immediate to verify the relation

$$M(\sigma)M(x)M(\sigma^{-1}) = M(\sigma x),$$

if $M(x)$ is the matrix associated with an element $x \in K$.

Since the order of an element in the multiplicative group of a field is prime to the characteristic, we conclude:

If F has characteristic p, then an element of finite order in $GL_2(F)$ is semisimple if and only if its order is prime to p.

Conjugacy classes

We shall determine the conjugacy classes explicitly. We specialize the situation, and from now on we let:

F = finite field with q elements;
$G = GL_2(F)$;
Z = center of G;
A = diagonal subgroup of G;
$C \approx K^*$ = a non-split Cartan subgroup of G.

Up to conjugacy there is only one non-split Cartan because over a finite field there is only one quadratic extension (in a given algebraic closure F^{a}) (*cf.* Corollary 2.7 of Chapter XIV). Recall that

$$\#(G) = (q^2 - 1)(q^2 - q) = q(q + 1)(q - 1)^2.$$

This should have been worked out as an exercise before. Indeed, $F \times F$ has q^2 elements, and $\#(G)$ is equal to the number of bases of $F \times F$. There are $q^2 - 1$ choices for a first basis element, and then $q^2 - q$ choices for a second (omitting $(0, 0)$ the first time, and all chosen elements the second time). This gives the value for $\#(G)$.

There are two cases for the conjugacy classes of an element α.

Case 1. The characteristic polynomial is reducible, so the eigenvalues lie in F. In this case, by the Jordan canonical form, such an element is conjugate to one of the matrices

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad \text{with } d \neq a.$$

These are called **central**, **unipotent**, or **rational not central** respectively.

Case 2. The characteristic polynomial is irreducible. Then α is such that $F[\alpha] \approx E$, where E is the quadratic extension of F of degree 2. Then $\{1, \alpha\}$ is a basis of $F[\alpha]$ over F, and the matrix associated with α under the representation by multiplication on $F[\alpha]$ is

$$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix},$$

where a, b are the coefficients of the characteristic polynomial $X^2 + ax + b$.

We then have the following table.

Table 12.4

class	# of classes	# of elements in the class
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$q - 1$	1
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$q - 1$	$q^2 - 1$
$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ with $a \neq d$	$\frac{1}{2}(q - 1)(q - 2)$	$q^2 + q$
$\alpha \in C - F^*$	$\frac{1}{2}(q - 1)q$	$q^2 - q$

In each case one computes the number of elements in a given class as the index of the normalizer of the element (or centralizer of the element). Case 1 is trivial. Case 2 can be done by direct computation, since the centralizer is then seen to consist of the matrices

$$\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}, \ x \in F,$$

with $x \neq 0$. The third and fourth cases can be done by using Proposition 12.3.

As for the number of classes of each type, the first and second cases correspond to distinct choices of $a \in F^*$ so the number of classes is $q - 1$ in each case. In the third case, the conjugacy class is determined by the eigenvalues. There are $q - 1$ possible choices for a, and then $q - 2$ possible choices for d. But the non-ordered pair of eigenvalues determines the conjugacy class, so one must divide $(q-1)(q-2)$ by 2 to get the number of classes. Finally, in the case of an element in a non-split Cartan, we have already seen that if σ generates $\mathrm{Gal}(K/F)$, then $M(\sigma x)$ is conjugate to $M(x)$ in $GL_2(F)$. But on the other hand, suppose $x, x' \in K^*$ and $M(x)$, $M(x')$ are conjugate in $GL_2(F)$ under a given regular representation of K^* on K with respect to a given basis. Then this conjugation induces an F-algebra isomorphism on $F[C_K]$, whence an automorphism of K, which is the identity, or the non-trivial automorphism σ. Consequently the number of conjugacy classes for elements of the fourth type is equal to

$$\frac{\#(K) - \#(F)}{2} = \frac{q^2 - q}{2},$$

which gives the value in the table.

Borel subgroup and induced representations

We let:

U = group of unipotent elements $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$;

B = Borel subgroup $= UA = AU$.

Then $\#(B) = q(q-1)^2 = (q-1)(q^2-q)$. We shall construct representations of G by inducing characters from B, and eventually we shall construct all irreducible representations of G by combining the induced representations in a suitable way. We shall deal with four types of characters. Except in the first type, which is 1-dimensional and therefore obviously simple, we shall prove that the other types are simple by computing induced characters. In one case we need to subtract a one-dimensional character. In the other cases, the induced character will turn out to be simple. The procedure will be systematic. We shall give a table of values for each type. We verify in each case that for the character χ which we want to prove simple we have

$$\sum_{\beta \in G} |\chi(\beta)|^2 = \#(G),$$

and then apply Theorem 5.17(a) to get the simplicity. Once we have done this for all four types, from the tables of values we see that they are distinct. Finally, the total number of distinct characters which we have exhibited will be equal to the number of conjugacy classes, whence we conclude that we have exhibited all simple characters.

We now carry out this program. I myself learned the simple characters of $GL_2(F)$ from a one-page handout by Tate in a course at Harvard, giving the subsequent tables and the values of the characters on conjugacy classes. I filled out the proofs in the following pages.

First type

$\mu : F^* \to C^*$ denotes a homomorphism. Then we obtain the character

$\mu \circ \det : G \to \mathbf{C}^*$,

which is 1-dimensional. Its values on representatives of the conjugacy classes are given in the following table.

Table 12.5(I)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
$\mu \circ \det$	$\mu(a)^2$	$\mu(a)^2$	$\mu(ad)$	$\mu \circ \det(\alpha)$

The stated values are by definition. The last value can also be written

$$\mu(\det \alpha) = \mu(N_{K/F}(\alpha)),$$

viewing α as an element of K^*, because the reader should know from field theory that the determinant gives the norm.

A character of G will be said to be of **first type** if it is equal to $\mu \circ \det$ for some μ. There are $q - 1$ characters of first type, because $\#(F^*) = q - 1$.

Second type

Observe that we have $B/U = A$. A character of A can therefore be viewed as a character on B via B/U. We let:

$\psi_\mu = \mathrm{res}_A(\mu \circ \det)$, and view ψ_μ therefore as a character on B. Thus

$$\psi_\mu\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \mu(ad).$$

We obtain the induced character

$$\psi_\mu^G = \mathrm{ind}_B^G(\psi_\mu).$$

Then ψ_μ^G is not simple. It contains $\mu \circ \det$, as one sees by Frobenius reciprocity:

$$\langle \mathrm{ind}_B^G \psi_\mu, \mu \circ \det \rangle_G = \langle \psi_\mu, \mu \circ \det \rangle_B = \frac{1}{\#(B)} \sum_{\beta \in B} |\mu \circ \det(\beta)|^2 = 1.$$

Characters $\chi = \psi_\mu^G - \mu \circ \det$ will be called of **second type**.

The values on the representatives of conjugacy classes are as follows.

Table 12.5(II)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} d \neq a$	$\alpha \in C - F^*$
$\psi_\mu^G - \mu \circ \det$	$q\mu(a)^2$	0	$\mu(ad)$	$-\mu \circ \det(\alpha)$

Actually, one computes the values of ψ_μ^G, and one then subtracts the value of $\theta \circ \det$. For this case and the next two cases, we use the formula for the induced function:

$$\mathrm{ind}_H^G(\varphi)(\alpha) = \frac{1}{\#(H)} \sum_{\beta \in G} \varphi_H(\beta\alpha\beta^{-1})$$

where φ_H is the function equal to φ on H and 0 outside H. An element of the center commutes with all $\beta \in G$, so for $\varphi = \psi_\mu$ the value of the induced character on such an element is

$$\frac{\#(G)}{\#(B)}\mu(a)^2 = (q + 1)\mu(a)^2,$$

which gives the stated value.

For an element $u = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$, the only elements $\beta \in G$ such that $\beta u \beta^{-1}$ lies in B are the elements of B (by direct verification). It is then immediate that

$$\operatorname{ind}_B^G(\psi_\mu)\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} = \mu(a)^2,$$

which yields the stated value for the character χ. Using Table 12.4, one finds at once that $\sum |\chi(\beta)|^2 = \#(G)$, and hence;

A character χ of second type is simple.

The table of values also shows that there are $q - 1$ characters of second type. The next two types deal especially with the Cartan subgroups.

Third type

$\psi : A \rightarrow \mathbf{C}^*$ denotes a homomorphism.

As mentioned following Proposition 12.3, the representative $w = w_A = w^{-1}$ for $N(A)/A$ is such that

$$w\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}w = \begin{pmatrix} d & 0 \\ 0 & a \end{pmatrix} = \alpha^w \quad \text{if } \alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}.$$

Thus conjugation by w is an automorphism of order 2 on A. Let $[w]\psi$ be the conjugate character; that is, $([w]\psi)(\alpha) = \psi(w\alpha w) = \psi(\alpha^w)$ for $\alpha \in A$. Then $[w](\mu \circ \det) = \mu \circ \det$. The characters $\mu \circ \det$ on A are precisely those which are invariant under $[w]$. The others can be written in the form

$$\psi\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \psi_1(a)\psi_2(d),$$

with distinct characters ψ_1, ψ_2: $F^* \rightarrow \mathbf{C}^*$. In light of the isomorphism $B/U \approx A$, we view ψ has a character on B. Then we form the induced character

$$\psi^G = \operatorname{ind}_B^G(\psi) = \operatorname{ind}_B^G([w]\psi).$$

With ψ such that $[w]\psi \neq \psi$, the characters $\chi = \psi^G$ will be said to be of the **third type**. Here is their table of values.

Table 12.5(III)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\alpha = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}_{d \neq a}$	$\alpha \in C - F^*$
ψ^G $\psi \neq [w]\psi$	$(q+1)\psi(a)$	$\psi(a)$	$\psi(\alpha) + \psi(\alpha^w)$	0

The first entry on central elements is immediate. For the second, we have already seen that if $\beta \in G$ is such that conjugating

$$\beta\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}\beta^{-1} \in B,$$

then $\beta \in B$, and so the formula

$$\psi^G(\alpha) = \frac{1}{\#(B)} \sum_{\beta \in G} \psi_B(\beta\alpha\beta^{-1})$$

immediately gives the value of ψ^G on unipotent elements. For an element of A with $a \neq d$, there is the additional possibility of the normalizer of A with the elements w, and the value in the table then drops out from the formula. For elements of the non-split Cartan group, there is no element of G which conjugates them to elements of B, so the value in the last column is 0.

We claim that a character $\chi = \psi^G$ of third type is simple.

The proof again uses the test for simplicity, i.e. that $\sum |\chi(\beta)|^2 = \#(G)$. Observe that two elements α, $\alpha' \in A$ are in the same conjugacy class in G if and only if $\alpha' = \alpha$ or $\alpha' = [w]\alpha$. This is verified by brute force. Therefore, writing the sum $\sum |\psi^G(\beta)|^2$ for β in the various conjugacy classes, and using Table 12.4, we find:

$$\sum_{\beta \in G} |\psi^G(\beta)|^2 = (q+1)^2(q-1)$$
$$+ (q-1)(q^2-1) + (q^2+q) \sum_{\alpha \in (A - F^*)/w} |\psi(\alpha) + \psi(\alpha^w)|^2.$$

The third term can be written

$$\frac{1}{2}(q^2+q) \sum_{\alpha \in A\text{-}F^*} (\psi(\alpha) + \psi(\alpha^w))(\psi(\alpha^{-1}) + \psi(\alpha^{-w}))$$
$$= \frac{1}{2}(q^2+q) \sum_{\alpha \in A - F^*} (1 + 1 + \psi(\alpha^{1-w}) + \psi(\alpha^{w-1})).$$

We write the sum over $\alpha \in A - F^*$ as a sum for $\alpha \in A$ minus the sum for

$\alpha \in F^*$. If $\alpha \in F^*$ then $\alpha^{1-w} = \alpha^{w-1} = 1$. By assumption on ψ, the character

$$\alpha \mapsto \psi(\alpha^{1-w}) \text{ for } \alpha \in A$$

is non-trivial, and therefore the sum over $\alpha \in A$ is equal to 0. Therefore, putting these remarks together, we find that the third term is equal to

$$\frac{1}{2}(q^2 + q)[2(q-1)^2 - 2(q-1) - 2(q-1)] = q(q^2-1)(q-3).$$

Hence finally

$$\begin{aligned}\sum_{\beta \in G} |\psi^G(\beta)|^2 &= (q+1)(q^2-1) + (q-1)(q^2-1) + q(q^2-1)(q-3)\\ &= q(q-1)(q^2-1) = \#(G),\end{aligned}$$

thus proving that ψ^G is simple.

Finally we observe that there are $\frac{1}{2}(q-1)(q-2)$ characters of third type. This is the number of characters ψ such that $[w]\psi \neq \psi$, divided by 2 because each pair ψ and $[w]\psi$ yields the same induced character ψ^G. The table of values shows that up to this coincidence, the induced characters are distinct.

Fourth type

$\theta : K^* \to \mathbf{C}^*$ denotes a homomorphism, which is viewed as a character on $C = C_K$.

By Proposition 12.3, there is an element $w \in N(C)$ but $w \notin C$, $w = w^{-1}$. Then

$$\alpha \mapsto w\alpha w = [w]\alpha$$

is an automorphism of C, but $x \mapsto wxw$ is also a field automorphism of $F[C] \approx K$ over F. Since $[K : F] = 2$, it follows that conjugation by w is the automorphism $\alpha \mapsto \alpha^q$. As a result we obtain the conjugate character $[w]\theta$ such that

$$([w]\theta)(\alpha) = \theta([w]\alpha) = \theta(\alpha^w),$$

and we get the induced character

$$\theta^G = \operatorname{ind}_C^G(\theta) = \operatorname{ind}_C^G([w]\theta).$$

Let $\mu : F^* \to \mathbf{C}^*$ denote a homomorphism as in the first type. Let:

$\lambda : F^+ \to \mathbf{C}^*$ be a *non-trivial* homomorphism.

$(\mu, \lambda) =$ the character on ZU such that

$$(\mu, \lambda)\left(\begin{pmatrix} a & ax \\ 0 & a \end{pmatrix}\right) = \mu(a)\lambda(x).$$

$(\mu, \lambda)^G = \operatorname{ind}_{ZU}^G(\mu, \lambda)$.

A routine computation of the same nature that we have had previously gives the following values for the induced characters θ^G and $(\mu, \lambda)^G$.

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}_{d \neq a}$	$\alpha \in C - F^*$
θ^G	$(q^2 - q)\theta(a)$	0	0	$\theta(\alpha) + \theta(\alpha^w)$
$(\mu, \lambda)^G$	$(q^2 - 1)\mu(a)$	$-\mu(a)$	0	0

These are intermediate steps. Note that a direct computation using Frobenius reciprocity shows that θ^G occurs in the character $(\text{res}\,\theta, \lambda)^G$, where the restriction $\text{res}\,\theta$ is to the group F^*, so $\text{res}\,\theta$ is one of our characters μ. Thus we define:

$$\theta' = (\text{res}\,\theta, \lambda)^G - \theta^G = ([w]\theta)',$$

which is an effective character. A character θ' is said to be of **fourth type** if θ is such that $\theta \neq [w]\theta$. These are the characters we are looking for. Using the intermediate table of values, one then finds the table of values for those characters of fourth type.

Table 12.5(IV)

χ	$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}_{d \neq a}$	$\alpha \in C - F^*$
θ' $\theta \neq [w]\theta$	$(q - 1)\theta(a)$	$-\theta(a)$	0	$-\theta(\alpha) - \theta(\alpha^w)$

We claim that the characters θ' of fourth type are simple.

To prove this, we evaluate

$$\sum_{\beta \in G} |\theta'(\beta)|^2 = (q - 1)^2(q - 1) + (q - 1)(q^2 - 1)$$

$$+ \frac{1}{2}(q^2 - q) \sum_{\alpha \in K^* - F^*} |\theta(\alpha) + \theta(\alpha^w)|^2.$$

We use the same type of expansion as for characters of third type, and the final value does turn out to be $\#(G)$, thus proving that θ' is simple.

The table also shows that there are $\frac{1}{2}\#(C - F^*) = \frac{1}{2}(q^2 - q)$ distinct characters of fourth type. We thus come to the end result of our computations.

Theorem 12.6. *The irreducible characters of $G = GL_2(F)$ are as follows.*

type		number of that type	dimension
I	$\mu \circ \det$	$q - 1$	1
II	$\psi_\mu^G - \mu \circ \det$	$q - 1$	q
III	ψ^G from pairs $\psi \neq [w]\psi$	$\frac{1}{2}(q - 1)(q - 2)$	$q + 1$
IV	θ' from pairs $\theta \neq [w]\theta$	$\frac{1}{2}(q - 1)q$	$q - 1$

Proof. We have exhibited characters of four types. In each case it is immediate from our construction that we get the stated number of distinct characters of the given type. The dimensions as stated are immediately computed from the dimensions of induced characters as the index of the subgroup from which we induce, and on two occasions we have to subtract something which was needed to make the character of given type simple. The end result is the one given in the above table. The total number of listed characters is precisely equal to the number of classes in Table 12.4, and therefore we have found all the simple characters, thus proving the theorem.

EXERCISES

1. **The group S_3.** Let S_3 be the symmetric group on 3 elements,
   (a) Show that there are three conjugacy classes.
   (b) There are two characters of dimension 1, on S_3/A_3.
   (c) Let d_i ($i = 1, 2, 3$) be the dimensions of the irreducible characters. Since $\sum d_i^2 = 6$, the third irreducible character has dimension 2. Show that the third representation can be realized by considering a cubic equation $X^3 + aX + b = 0$, whose Galois group is S_3 over a field k. Let V be the k-vector space generated by the roots. Show that this space is 2-dimensional and gives the desired representation, which remains irreducible after tensoring with k^{a}.
   (d) Let $G = S_3$. Write down an idempotent for each one of the simple components of $\mathbf{C}[G]$. What is the multiplicity of each irreducible representation of G in the regular representation on $\mathbf{C}[G]$?

2. **The groups S_4 and A_4.** Let S_4 be the symmetric group on 4 elements.
   (a) Show that there are 5 conjugacy classes.
   (b) Show that A_4 has a unique subgroup of order 4, which is not cyclic, and which is normal in S_4. Show that the factor group is isomorphic to S_3, so the representations of Exercise 1 give rise to representations of S_4.
   (c) Using the relation $\sum d_i^2 = \#(S_4) = 24$, conclude that there are only two other irreducible characters of S_4, each of dimension 3.
   (d) Let $X^4 + a_2X^2 + a_1X + a_0$ be an irreducible polynomial over a field k, with Galois group S_4. Show that the roots generate a 3-dimensional vector space V over k, and that the representation of S_4 on this space is irreducible, so we obtain one of the two missing representations.
   (e) Let ρ be the representation of (d). Define ρ' by

$$\rho'(\sigma) = \rho(\sigma) \text{ if } \sigma \text{ is even;}$$
$$\rho'(\sigma) = -\rho(\sigma) \text{ if } \sigma \text{ is odd.}$$

   Show that ρ' is also irreducible, remains irreducible after tensoring with k^{a}, and is non-isomorphic to ρ. This concludes the description of all irreducible representations of S_4.
   (f) Show that the 3-dimensional irreducible representations of S_4 provide an irreducible representation of A_4.
   (g) Show that all irreducible representations of A_4 are given by the representations in (f) and three others which are one-dimensional.

3. **The quaternion group.** Let $Q = \{\pm 1, \pm x, \pm y, \pm z\}$ be the quaternion group, with $x^2 = y^2 = z^2 = -1$ and $xy = -yx$, $xz = -zx$, $yz = -zy$.
   (a) Show that Q has 5 conjugacy classes.
   Let $A = \{\pm 1\}$. Then Q/A is of type (2, 2), and hence has 4 simple characters, which can be viewed as simple characters of Q.
   (b) Show that there is only one more simple character of Q, of dimension 2. Show that the corresponding representation can be given by a matrix representation such that

$$\rho(x) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \rho(y) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \rho(z) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

   (c) Let $\mathbf{H}$ be the quaternion field, i.e. the algebra over $\mathbf{R}$ having dimension 4, with basis $\{1, x, y, z\}$ as in Exercise 3, and the corresponding relations as above. Show that $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{H} \approx \mathrm{Mat}_2(\mathbf{C})$ (2×2 complex matrices). Relate this to (b).

4. Let S be a normal subgroup of G. Let ψ be a simple character of S over $\mathbf{C}$. Show that $\mathrm{ind}_S^G(\psi)$ is simple if and only if $\psi = [\sigma]\psi$ for all $\sigma \in S$.

5. Let G be a finite group and S a normal subgroup. Let ρ be an irreducible representation of G over $\mathbf{C}$. Prove that either the restriction of ρ to S has all its irreducible components S-isomorphic to each other, or there exists a proper subgroup H of G containing S and an irreducible representation θ of H such that $\rho \approx \mathrm{ind}_H^G(\theta)$.

6. **Dihedral group D_{2n}.** There is a group of order $2n$ (n even integer $\geqq 2$) generated by two elements σ, τ such that

$$\sigma^n = 1,\ \tau^2 = 1, \quad \text{and} \quad \tau\sigma\tau = \sigma^{-1}.$$

It is called the **dihedral group**.

(a) Show that there are four representations of dimension 1, obtained by the four possible values ±1 for σ and τ.

(b) Let C_n be the cyclic subgroup of D_{2n} generated by σ. For each integer $r = 0, \ldots, n-1$ let ψ_r be the character of C_n such that

$$\psi_r(\sigma) = \zeta^r \quad (\zeta = \text{prim. } n\text{-th root of unity})$$

Let χ_r be the induced character. Show that $\chi_r = \chi_{n-r}$.

(c) Show that for $0 < r < n/2$ the induced character χ_r is simple, of dimension 2, and that one gets thereby $\left(\frac{n}{2} - 1\right)$ distinct characters of dimension 2.

(d) Prove that the simple characters of (a) and (c) give all simple characters of D_{2n}.

7. Let G be a finite group, semidirect product of A, H where A is commutative and normal. Let $A^\wedge = \text{Hom}(A, \mathbf{C}^*)$ be the dual group. Let G operate by conjugation on characters, so that for $\sigma \in G$, $a \in A$, we have

$$[\sigma]\psi(a) = \psi(\sigma^{-1}a\sigma).$$

Let $\psi_1, \ldots, \psi_r$ be representatives of the orbits of H in $A^\wedge$, and let $H_i (i = 1, \ldots, r)$ be the isotropy group of ψ_i. Let $G_i = AH_i$.

(a) For $a \in A$ and $h \in H_i$, define $\psi_i(ah) = \psi_i(a)$. Show that ψ_i is thus extended to a character on G_i.

Let θ be a simple representation of H_i (on a vector space over $\mathbf{C}$). From $H_i = G_i/A$, view θ as a simple representation of G_i. Let

$$\rho_{i,\theta} = \text{ind}_{G_i}^{G}(\psi_i \otimes \theta).$$

(b) Show that $\rho_{i,\theta}$ is simple.

(c) Show that $\rho_{i,\theta} \approx \rho_{i',\theta'}$ implies $i = i'$ and $\theta \approx \theta'$.

(d) Show that every irreducible representation of G is isomorphic to some $\rho_{i,\theta}$

8. Let G be a finite group operating on a finite set S. Let $\mathbf{C}[S]$ be the vector space generated by S over $\mathbf{C}$. Let ψ be the character of the corresponding representation of G on $\mathbf{C}[S]$.

(a) Let $\sigma \in G$. Show that $\psi(\sigma)$ = number of fixed points of σ in S.

(b) Show that $\langle \psi, 1_G \rangle_G$ is the number of G-orbits in S.

9. Let A be a commutative subgroup of a finite group G. Show that every irreducible representation of G over $\mathbf{C}$ has dimension $\leqq (G : A)$.

10. Let $\mathbf{F}$ be a finite field and let $G = SL_2(\mathbf{F})$. Let B be the subgroup of G consisting of all matrices

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in SL_2(\mathbf{F}), \text{ so } d = a^{-1}.$$

Let $\mu : \mathbf{F}^* \to \mathbf{C}^*$ be a homomorphism and let $\psi_\mu : B \to \mathbf{C}^*$ be the homomorphism such that $\psi_\mu(\alpha) = \mu(a)$. Show that the induced character $\text{ind}_B^G(\psi_\mu)$ is simple if $\mu^2 \neq 1$.

11. Determine all simple characters of $SL_2(\mathbf{F})$, giving a table for the number of such characters, representatives for the conjugacy classes, as was done in the text for GL_2, over the complex numbers.

12. Observe that $A_5 \approx SL_2(\mathbf{F}_4) \approx PSL_2(\mathbf{F}_5)$. As a result, verify that there are 5 conjugacy classes, whose elements have orders 1, 2, 3, 5, 5 respectively, and write down explicitly the character table for A_5 as was done in the text for GL_2.

13. Let G be a p-group and let $G \to \mathrm{Aut}(V)$ be a representation on a finite dimensional vector space over a field of characteristic p. Assume that the representation is irreducible. Show that the representation is trivial, i.e. G acts as the identity on V.

14. Let G be a finite group and let C be a conjugacy class. Prove that the following two conditions are equivalent. They define what it means for the class to be **rational**.

    RAT 1. For all characters χ of G, $\chi(\sigma) \in \mathbf{Q}$ for $\sigma \in C$.

    RAT 2. For all $\sigma \in C$, and j prime to the order of σ, we have $\sigma^j \in C$.

15. Let G be a group and let H_1, H_2 be subgroups of finite index. Let ρ_1, ρ_2 be representations of H_1, H_2 on R-modules F_1, F_2 respectively. Let $M_G(F_1, F_2)$ be the R-module of functions $f: G \to \mathrm{Hom}_R(F_1, F_2)$ such that

$$f(h_1\sigma h_2) = \rho_2(h_2)f(\sigma)\rho_1(h_1)$$

for all $\sigma \in G$, $h_i \in H_i$ $(i = 1, 2)$. Establish an R-module isomorphism

$$\mathrm{Hom}_R(F_1^G, F_2^G) \xrightarrow{\approx} M_G(F_1, F_2).$$

By F_i^G we have abbreviated $\mathrm{ind}_{H_i}^G(F_i)$.

16. (a) Let G_1, G_2 be two finite groups with representations on $\mathbf{C}$-spaces E_1, E_2. Let $E_1 \otimes E_2$ be the usual tensor product over $\mathbf{C}$, but now prove that there is an action of $G_1 \times G_2$ on this tensor product such that

$$(\sigma_1, \sigma_2)(x \otimes y) = \sigma_1 x \otimes \sigma_2 y \text{ for } \sigma_1 \in G_1,\ \sigma_2 \in G_2.$$

This action is called the **tensor product** of the other two. If ρ_1, ρ_2 are the representations of G_1, G_2 on E_1, E_2 respectively, then their tensor product is denoted by $\rho_1 \otimes \rho_2$. Prove: If ρ_1, ρ_2 are irreducible then $\rho_2 \otimes \rho_2$ is also irreducible. [*Hint*: Use Theorem 5.17.]

(b) Let χ_1, χ_2 be the characters of ρ_1, ρ_2 respectively. Show that $\chi_1 \otimes \chi_2$ is the character of the tensor product. By definition,

$$\chi_1 \otimes \chi_2(\sigma_1, \sigma_2) = \chi_1(\sigma_1)\, \chi_2(\sigma_2).$$

17. With the same notation as in Exercise 16, show that every irreducible representation of $G_1 \times G_2$ over $\mathbf{C}$ is isomorphic to a tensor product representation as in Exercise 16. [*Hint*: Prove that if a character is orthogonal to all the products $\chi_1 \otimes \chi_2$ of Exercise 16(b) then the character is 0.]

Tensor product representations

18. Let P be the non-commutative polynomial algebra over a field k, in n variables. Let $x_1, \ldots, x_r$ be distinct elements of P_1 (i.e. linear expressions in the variables $t_1, \ldots, t_n$)

and let $a_1, \dots, a_r \in k$. If

$$a_1 x_1^\nu + \cdots + a_r x_r^\nu = 0$$

for all integers $\nu = 1, \dots, r$ show that $a_i = 0$ for $i = 1, \dots, r$. [*Hint*: Take the homomorphism on the commutative polynomial algebra and argue there.]

19. Let G be a finite set of endomorphisms of a finite-dimensional vector space E over the field k. For each $\sigma \in G$, let c_σ be an element of k. Show that if

$$\sum_{\sigma \in G} c_\sigma T^r(\sigma) = 0$$

for all integers $r \geqq 1$, then $c_\sigma = 0$ for all $\sigma \in G$. [*Hint*: Use the preceding exercise, and Proposition 7.2 of Chapter XVI.]

20. **(Steinberg)**. Let G be a finite monoid, and $k[G]$ the monoid algebra over a field k. Let $G \to \operatorname{End}_k(E)$ be a faithful representation (i.e. injective), so that we identify G with a multiplicative subset of $\operatorname{End}_k(E)$. Show that T^r induces a representation of G on $T^r(E)$, whence a representation of $k[G]$ on $T^r(E)$ by linearity. If $\alpha \in k[G]$ and if $T^r(\alpha) = 0$ for all integers $r \geqq 1$, show that $\alpha = 0$. [*Hint*: Apply the preceding exercise.]

21. **(Burnside)**. Deduce from Exercise 20 the following theorem of Burnside: Let G be a finite group, k a field of characteristic prime to the order of G, and E a finite dimensional (G, k)-space such that the representation of G is faithful. Then every irreducible representation of G appears with multiplicity $\geqq 1$ in some tensor power $T^r(E)$.

22. Let $X(G)$ be the character ring of a finite group G, generated over $\mathbf{Z}$ by the simple characters over $\mathbf{C}$. Show that an element $f \in X(G)$ is an effective irreducible character if and only if $\langle f, f \rangle_G = 1$ and $f(1) \geqq 0$.

23. In this exercise, we assume the next chapter on alternating products. Let ρ be an irreducible representation of G on a vector space E over $\mathbf{C}$. Then by functoriality we have the corresponding representations $S^r(\rho)$ and $\bigwedge^r(\rho)$ on the r-th symmetric power and r-th alternating power of E over $\mathbf{C}$. If χ is the character of ρ, we let $S^r(\chi)$ and $\bigwedge^r(\chi)$ be the characters of $S^r(\rho)$ and $\bigwedge^r(\rho)$ respectively, on $S^r(E)$ and $\bigwedge^r(E)$. Let t be a variable and let

$$\sigma_t(\chi) = \sum_{r=0}^{\infty} S^r(\chi)t^r, \quad \lambda_t(\chi) = \sum_{r=0}^{\infty} \textstyle\bigwedge^r(\chi)t^r.$$

(a) Comparing with Exercise 24 of Chapter XIV, prove that for $x \in G$ we have

$$\sigma_t(\chi)(x) = \det(I - \rho(x)t)^{-1} \quad \text{and} \quad \lambda_t(\chi)(x) = \det(I + \rho(x)t).$$

(b) For a function f on G define $\Psi^n(f)$ by $\Psi^n(f)(x) = f(x^n)$. Show that

$$-\frac{d}{dt}\log \sigma_t(\chi) = \sum_{n=1}^{\infty} \Psi^n(\chi)t^n \quad \text{and} \quad -\frac{d}{dt}\log \lambda_{-t}(\chi) = \sum_{n=1}^{\infty} \Psi^n(\chi)t^n.$$

(c) Show that

$$nS^n(\chi) = \sum_{r=1}^{n} \Psi^r(\chi)S^{n-r}(\chi) \quad \text{and} \quad n\textstyle\bigwedge^n(\chi) = \displaystyle\sum_{r=1}^{\infty} (-1)^{r-1}\Psi^r(\chi)\textstyle\bigwedge^{n-r}(\chi).$$

24. Let χ be a simple character of G. Prove that $\Psi^n(\chi)$ is also simple. (The characters are over $\mathbf{C}$.)

25. We now assume that you know §3 of Chapter XX.
    (a) Prove that the Grothendieck ring defined there for $\mathrm{Mod}_{\mathbf{C}}(G)$ is naturally isomorphic to the character ring $X(G)$.
    (b) Relate the above formulas with Theorem 3.12 of Chapter XX.
    (c) Read Fulton-Lang's *Riemann-Roch Algebra*, Chapter I, especially §6, and show that $X(G)$ is a λ-ring, with Ψ^n as the Adams operations.

Note. For further connections with homology and the cohomology of groups, see Chapter XX, §3, and the references given at the end of Chapter XX, §3.

26. The following formalism is the analogue of Artin's formalism of L-series in number theory. Cf. Artin's "Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren", Collected papers, and also S. Lang, "L-series of a covering", *Proc. Nat. Acad. Sc. USA* (1956). For the Artin formalism in a context of analysis, see J. Jorgenson and S. Lang, "Artin formalism and heat kernels", *J. reine angew. Math.* **447** (1994) pp. 165–200.

We consider a category with objects $\{U\}$. As usual, we say that a finite group G operates on U if we are given a homomorphism $\rho : G \to \mathrm{Aut}(U)$. We then say that U is a G-object, and also that ρ is a representation of G in U. We say that G operates trivially if $\rho(G) = \mathrm{id}$. For simplicity, we omit the ρ from the notation. By a G-morphism $f : U \to V$ between G-objects, one means a morphism such that $f \circ \sigma = \sigma \circ f$ for all $\sigma \in G$.

We shall assume that for each G-object U there exists an object U/G on which G operates trivially, and a G-morphism $\pi_{U,G} : U \to U/G$ having the following universal property: If $f : U \to U'$ is a G-morphism, then there exists a unique morphism

$$f/G : U/G \to U'/G$$

making the following diagram commutative:

$$\begin{tikzcd}
U \arrow[r, "f"] \arrow[d] & U' \arrow[d] \\
U/G \arrow[r, "f/G"'] & U'/G
\end{tikzcd}$$

In particular, if H is a normal subgroup of G, show that G/H operates in a natural way on U/H.

Let k be an algebraically closed field of characteristic 0. We assume given a functor E from our category to the category of finite dimensional k-spaces. If U is an object in our category, and $f : U \to U'$ is a morphism, then we get a homomorphism

$$E(f) = f_* : E(U) \to E(U').$$

(The reader may keep in mind the special case when we deal with the category of reasonable topological spaces, and E is the homology functor in a given dimension.)

If G operates on U, then we get an operation of G on $E(U)$ by functoriality.

Let U be a G-object, and $F : U \to U$ a G-morphism. If $P_F(t) = \prod (t - \alpha_i)$ is the characteristic polynomial of the linear map $F_* : E(U) \to E(U)$, we define

$$Z_F(t) = \prod (1 - \alpha_i t),$$

and call this the zeta function of F. If F is the identity, then $Z_F(t) = (1 - t)^{B(U)}$ where we define $B(U)$ to be $\dim_k E(U)$.

Let χ be a simple character of G. Let d_χ be the dimension of the simple representation of G belonging to χ, and $n = \operatorname{ord}(G)$. We define a linear map on $E(U)$ by letting

$$e_\chi = \frac{d_\chi}{n} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma_*.$$

Show that $e_\chi^2 = e_\chi$, and that for any positive integer μ we have $(e_\chi \circ F_*)^\mu = e_\chi \circ F_*^\mu$. If $P_\chi(t) = \prod (t - \beta_j(\chi))$ is the characteristic polynomial of $e_\chi \circ F_*$, define

$$L_F(t, \chi, U/G) = \prod (1 - \beta_j(\chi)t).$$

Show that the logarithmic derivative of this function is equal to

$$-\frac{1}{N} \sum_{\mu=1}^{\infty} \operatorname{tr}(e_\chi \circ F_*^\mu)t^{\mu-1}.$$

Define $L_F(t, \chi, U/G)$ for any character χ by linearity. If we write $V = U/G$ by abuse of notation, then we also write $L_F(t, \chi, U/V)$. Then for any χ, χ' we have by definition,

$$L_F(t, \chi + \chi', U/V) = L_F(t, \chi, U/V)L_F(t, \chi', U/V).$$

We make one additional assumption on the situation:
Assume that the characteristic polynomial of

$$\frac{1}{n} \sum_{\sigma \in G} \sigma_* \circ F_*$$

is equal to the characteristic polynomial of F/G on $E(U/G)$. Prove the following statement:

(a) If $G = \{1\}$ then

$$L_F(t, 1, U/U) = Z_F(t).$$

(b) Let $V = U/G$. Then

$$L_F(t, 1, U/V) = Z_F(t).$$

(c) Let H be a subgroup of G and let ψ be a character of H. Let $W = U/H$, and let ψ^G be the induced character from H to G. Then

$$L_F(t, \psi, U/W) = L_F(t, \psi^G, U/V).$$

(d) Let H be normal in G. Then G/H operates on $U/H = W$. Let ψ be a character of G/H, and let χ be the character of G obtained by composing ψ with the canonical map $G \to G/H$. Let $\varphi = F/H$ be the morphism induced on

$$U/H = W.$$

Then

$$L_\varphi(t, \psi, W/V) = L_F(t, \chi, U/V).$$

(e) If $V = U/G$ and $B(V) = \dim_k E(V)$, show that $(1 - t)^{B(V)}$ divides $(1 - t)^{B(U)}$. Use the regular character to determine a factorization of $(1 - t)^{B(U)}$.

27. Do this exercise after you have read some of Chapter VII. The point is that for fields of characteristic not dividing the order of the group, the representations can be obtained by "reducing modulo a prime". Let G be a finite group and let p be a prime not dividing the order of G. Let F be a finite extension of the rationals with ring of algebraic integers $\mathfrak{o}_F$. Suppose that F is sufficiently large so that all F-irreducible representations of G remain irreducible when tensored with $\mathbf{Q}^a = F^a$. Let $\mathfrak{p}$ be a prime of $\mathfrak{o}_F$ lying above p, and let $\mathfrak{o}_\mathfrak{p}$ be the corresponding local ring.
   (a) Show that an irreducible (G, F)-space V can be obtained from a $(G, \mathfrak{o}_\mathfrak{p})$-module E free over $\mathfrak{o}_\mathfrak{p}$, by extending the base from $\mathfrak{o}_\mathfrak{p}$ to F, i.e. by tensoring so that $V = E \otimes F$ (tensor product over $\mathfrak{o}_\mathfrak{p}$).
   (b) Show that the reduction mod $\mathfrak{p}$ of E is an irreducible representation of G in characteristic p. In other words, let $k = \mathfrak{o}/\mathfrak{p} = \mathfrak{o}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ where $\mathfrak{m}_\mathfrak{p}$ is the maximal ideal of $\mathfrak{o}_\mathfrak{p}$. Let $E(\mathfrak{p}) = E \otimes k$ (tensor product over $\mathfrak{o}_\mathfrak{p}$). Show that G operates on $E(\mathfrak{p})$ in a natural way, and that this representation is irreducible. In fact, if χ is the character of G on V, show that χ is also the character on E, and that $\chi \bmod \mathfrak{m}_\mathfrak{p}$ is the character on $E(\mathfrak{p})$.
   (c) Show that all irreducible characters of G in characteristic p are obtained as in (b).