Chapter 3

# Representations of finite groups

Let $G$ be a group and $F$ be a field. An $F$-representation of $G$ is a group homomorphism $\rho : G \to \mathrm{GL}(V_F)$ where $V$ a finite dimensional $F$-vector space. Denote by $\mathrm{Rep}_F(G)$ the category of all $F$-representations. The goal of this chapter is to develop the general theory of complex representations ($F = \mathbb{C}$) of finite groups $G$. Some of the results hold for more general $F$ or $G$. We choose to present those general versions whenever they do not require too much additional efforts.

For general $F$, the abstract theory of modules and rings developed in the previous two chapters will be helpful (e.g. the Wedderburn–Artin theorem and the adjoint properties of $\otimes$ and hom for non-commutative rings).

For $F = \mathbb{C}$ and $|G| < \infty$, the essential tool to study representations is the theory of characters $\chi_\rho := \operatorname{tr} \rho : G \to F$ which can be regarded as an analogue of the Fourier transform in the discrete non-abelian case. In fact two representations $\rho$, $\rho'$ are equivalent if and only if $\chi_\rho = \chi_{\rho'}$. Being (class) functions on $G$, characters are much easier to handle than the actual representations. Hence

*Be More Concerned with Your Character than Your Representation!*

UCLA basketball coach—John Wooden

Based on the character theory, two celebrated results discussed in this chapter are (1) Burnside's theorem that any finite group with order $p^a q^b$, $p$ and $q$ are primes, is solvable; (2) Brauer's theorem that any character of $G$ is "integrally determined" by linear characters (i.e. $\dim_F V = 1$) of certain "elementary subgroups" $H \subset G$. This result is important in number theory.

## 1. The basics

Group representations are generalizations of group actions on finite sets. If $G$ acts on $S$, let $V := \bigoplus_{s \in S} Fs$ with base $S$, then $\rho : G \to \mathrm{GL}(V)$

defined by $\rho(g)s := gs$ and extending linearly over $F$:

$$\rho(g) \sum_{s\in S} a_s\, s = \sum_{s\in S} a_s\, gs = \sum_{s\in S} a_{g^{-1}s}\, s,$$

is called the permutation representation.

If $S = G$, with the action being the group multiplication (on the left), we get the regular representation $\rho_{\text{reg}}$ on $V_{\text{reg}} = F^{|G|}$. It is clear that $F^{|G|}$ is the underlying vector space of the group algebra $F[G]$, a fact we will explore in details shortly.

Here are some basic operations on representations. We denote $\rho(g) \sim A \in M_m(F)$ if $A$ is the matrix of $\rho(g)$ under a chosen basis of $V$. The dimension $m = \dim_F V =: \deg \rho$ is also called the degree of $\rho$.

(1) Direct sum: given $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1, 2$, we define $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}(V_1 \oplus V_2)$ by $(\rho_1 \oplus \rho_2)(g) = \rho_1(g) \oplus \rho_2(g)$. If $\rho_1(g) \sim A$, $\rho_2(g) \sim B$, then

$$\rho_1(g) \oplus \rho_2(g) \sim \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}.$$

(2) Tensor product: similarly we define $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V_1 \otimes_F V_2)$ by $(\rho_1 \otimes \rho_2)(g) = \rho_1(g) \otimes \rho_2(g) : v_1 \otimes v_2 \mapsto \rho_1(g)v_1 \otimes \rho_2(g)v_2$. Here all the tensor products are taken over the field $F$. If $V_1 = \bigoplus_i Fv_i$, $V_2 = \bigoplus_j Fw_j$, then $V_1 \otimes_F V_2 = \bigoplus Fv_i \otimes w_j$. Under the lexicographic order of the basis, namely $v_i \otimes w_j < v_{i'} \otimes w_{j'}$ if $i < i'$ or if $i = i'$ and $j < j'$, then

$$\rho_1(g) \otimes \rho_2(g) \sim A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in M_{mn}(F),$$

where $A \in M_m(F)$, $B \in M_n(F)$.

(3) Contragredient (dual): given $\rho : G \to \mathrm{GL}(V)$, $G$ acts on $\phi \in V^* = \hom_F(V, F)$ by $(g\phi)(v) := \phi(g^{-1}v)$. The inverse is inserted to ensure that $(gh)\phi = g(h\phi)$. This defines the dual representation $\rho^*$.

More precisely, if $V = \bigoplus Fv_i$, $\rho(g) \sim A$, then $V^* = \bigoplus Fv_j^*$ where $v_j^*$ is the dual basis such that $v_j^*(v_i) = \delta_{ji}$. The usual induced linear transformation on $V^*$ has matrix ${}^tA$. Hence $\rho^*(g) \sim {}^t(A^{-1}) = ({}^tA)^{-1}$.

(4) Equivalent representations: we say $\rho_1 \cong \rho_2$ if there is a vector space isomorphism $\eta : V_1 \cong V_2$ such that $\rho_2(g) = \eta\rho_1(g)\eta^{-1}$ for all $g \in G$.

It is clear that the group homomorphism $G \to \mathrm{GL}(V)$ extends linearly to an $F$-algebra homomorphism $F[G] \to \mathrm{End}_F V$. That is, a left $F[G]$-module structure on $V$. Conversely, a left $F[G]$-module $V$ leads to a representation of $G$. Thus the notion of sub/quotient/irreducible/completely reducible modules corresponds to the analogous notion of representations. Whenever there is only one $\rho$ involved, we simply write $gv := \rho(g)v$.

However, the notion of $\otimes$ and dual defined above for $F$-representations of $G$ do not correspond directly to the ones for $F[G]$-modules. Their relations will become transparent in later sections.

Here are two basic theorems: Maschke's theorem on complete reducibility and Clifford's theorem on restrictions to normal subgroups.

**Theorem 3.1** (Maschke)**.** *If* char $F \nmid |G| < \infty$, *then every* $\rho : G \to \mathrm{GL}(V)$ *is completely reducible.*

PROOF. If there is a $G$-invariant subspace $U \subset V$, we will show that there exists a $G$-invariant complemented subspace $U'$, and then he theorem follows by induction. We give two proofs of it. The first only works for $F = \mathbb{R}$ or $\mathbb{C}$. But it gives insights to motivate the second proof.

For $F = \mathbb{R}$ or $\mathbb{C}$, there exists a $G$-invariant inner product on $V$. Indeed for any inner product $(,)_0$ on $V$, the "balanced" inner product

$$(v, w) := \sum_{g \in G} (gv, gw)_0$$

is clearly $G$-invariant: $(hv, hw) = (v, w)$ for all $h \in G$. If $U \subset V$ is $G$-invariant then $U^\perp \subset V$ is also $G$-invariant: for $v \in U^\perp$, we have $(gv, u) = (v, g^{-1}u) = 0$ for all $u \in U$, hence $v \in U^\perp$.

For $F$ with char $F \nmid |G| < \infty$, we start with an arbitrary projection map $p_0$ (idempotent) onto $U$ instead. To adjust $p_0$ to a $G$-linear map $p$, i.e. $hp = ph$ for all $h \in G$, we simply take

$$p := \frac{1}{|G|} \sum_{g \in G} g^{-1} p_0 g,$$

and then $h^{-1}ph = p$. Moreover, $p$ is still a projection map onto $U$. For if $u \in U$, since $g(u) \in U$ we get $p_0 g(u) = g(u)$ and then $g^{-1} p_0 g(u) = u$ for all $g \in G$, so $p(u) = u$. Also for any $x \in V$ we have $p(x) \in U$ since $p_0 g(x) \in U$. Thus we have the decomposition $V = U \oplus U'$ corresponding to $1 = p + (1 - p)$ where $U' := \mathrm{im}(1 - p)$ is also $G$-invariant since $1 - p$ is an idempotent commuting with the $G$-action. $\square$

Consequently, there is a unique decomposition up to isomorphisms $\rho = \sum m_i \rho_i$, $V = \bigoplus V_i^{\oplus m_i}$ where $\rho_i : G \to \mathrm{GL}(V_i)$ are irreducible sub representations and $\rho_i \not\cong \rho_j$ for $i \neq j$. Thus the study of $F$-representations with char $F \nmid |G| < \infty$ is reduced to the study on irreducible ones.

*Definition* 3.2 (Restrictions and Conjugates).
(1) Let $\rho : G \to \mathrm{GL}(V)$, for any subgroup $H \subset G$ we define the restriction representation of $H$ on $V$ by

$$\rho_H \equiv \mathrm{Res}^G_H \rho \equiv \mathrm{Res}^G_H V := \rho|_H : H \to \mathrm{GL}(V).$$

(2) For $H \lhd G$, $\sigma : H \to \mathrm{GL}(U)$ and $g \in G$, we define the $g$-conjugate representation of $\sigma$ by

$$^g\sigma : H \to \mathrm{GL}(U), \qquad ^g\sigma(h) := \sigma(ghg^{-1}).$$

It preserves the lattice of $F[H]$-submodules. Also $\sigma_1 \cong \sigma_2 \Rightarrow {}^g\sigma_1 \cong {}^g\sigma_2$.

The next basic result works for any fields $F$ and any group $G$.

**Theorem 3.3** (Clifford). *Let $\rho : G \to \mathrm{GL}(V)$ be irreducible. Then $H \lhd G$ implies that $\rho_H$ is completely reducible and all irreducible components are conjugated with each other with the same multiplicity.*

PROOF. Let $U \subset V$ be an irreducible $F[H]$-submodule, say $U = F[H]v$ for some $v \in V \setminus \{0\}$. Then $V = \sum_{g\in G} gU$ since the sum is $G$-invariant. Also each $gU$ is $H$-invariant: for any $y \in U$, $h \in H$, $g^{-1}hg \in H$ and hence

$$hgy = g(g^{-1}hg)y \in gU.$$

Moreover, let $\sigma = \rho|_H$ acting on $U$, $\sigma' = \rho|_H$ acting on $gU$. Then the above formula means $\sigma' \cong {}^{g^{-1}}\sigma$ and so $gU$ is $F[H]$-irreducible for all $g \in G$.

This implies that $\rho_H$ on $V$ is completely reducible. It is also clear that if $U_1 \cong U_2$ for two irreducible components, the $gU_1 \cong gU_2$ too (all as $F[H]$-modules). Hence $\rho(g)$ permutes homogeneous components. $\square$

From now on, let $A := F[G]$ and denote by $\rho : A \to \mathrm{End}_F V$ under the same notation $\rho$. We will apply results on semi-simple artinian rings in the current setting. As before let

$$A' := \mathrm{End}_A V = C_{\mathrm{End}_F V}(\rho(A)) \subset \mathrm{End}_F V \cong M_{\dim V}(F),$$

and $A'' := \mathrm{End}_{A'} V \supset \rho(A)$. (Recall that $A''' = A'$ tautologically.)

If $\rho$ is known to be completely reducible, since $\dim_F V < \infty$, the density theorem then implies the double centralizer property $A'' = \rho(A)$. This is the case if $\mathrm{char}\, F \nmid |G| < \infty$ by Theorem 3.1.

In general, if $|G| < \infty$ then $A = F[G]$ is clearly artinian. In particular there are only a finite number of irreducible representations up to isomorphisms. Much more will be said below!

**Theorem 3.4.** *Let $|G| < \infty$, then $A = F[G]$ is semi-simple $\iff$ $\operatorname{char} F \nmid |G|$.*

Proof. If $\operatorname{char} F \nmid |G| < \infty$, then ${}_A A$ is completely reducible by Theorem 3.1. Hence $A$ is semi-simple by the Wedderburn–Artin–Jacobson structure theorem on artinian rings. Conversely, if $\operatorname{char} F \mid |G|$, then for $z := \sum_{g \in G} g$ we have $gz = z = zg$ for all $g \in G$, hence $Fz \subset A$ is an ideal. But $z^2 = (\sum g)z = |G|z = 0$ in $A$, hence $Fz$ is a nilpotent ideal and then $A$ is not semi-simple (again by the structure theorem). $\square$

Now we assume $\operatorname{char} F \nmid |G| < \infty$. By the structure theorems,

$$A = F[G] = A_1 \oplus \ldots \oplus A_s, \qquad A_s \cong M_{n_i}(\Delta_i),$$

where $\Delta_i$'s are division algebras over $F$. Let $I_i$ be a minimal left ideal of $A_i$, then it is also a minimal left ideal of $A$. Thus we obtain $s$ equivalence classes of irreducible $F$-representations $\rho_1, \ldots, \rho_s$ of $G$. Also

$$M_{n_i}(\Delta_i) = \bigoplus_{j=1}^{n_i} M_{n_i}(\Delta_i) e_{jj}$$

is the decomposition into $n_i$ copies of $I_i$ as the $j$-th column spaces. Let $d_i = \dim_F \Delta_i$ then $\dim_F I_i = n_i d_i$. This implies

**Corollary 3.5.** *For $\rho_{\text{reg}}$ which acts on the space ${}_A A$, we have*

$$\rho_{\text{reg}} = \bigoplus_{i=1}^{s} n_i \rho_i, \qquad |G| = \sum_{i=1}^{s} n_i^2 d_i.$$

Next we determine the center of $A$. Clearly

$$C(A) = C(A_1) \oplus \ldots \oplus C(A_s), \qquad C(A_i) = C(\Delta_i).$$

On the other hand, let $C_j$, $1 \le j \le r$ be the conjugacy classes of $G$. Then

**Proposition 3.6.** *$C(A) = \bigoplus_{j=1}^{r} F c_j$, where $c_j := \sum_{g \in C_j} g$.*

Proof. Let $a = \sum_{g \in G} a_g \, g \in A$, then

$$h^{-1} a h = \sum_{g \in G} a_g \, h^{-1} g h = \sum_{g \in G} a_{hgh^{-1}} \, g = a$$

for all $h \in G$ is equivalent to that all the coefficients in the same conjugacy class are the same. That is, $a$ is a linearly combination of $c_j$'s. Also $c_j$'s are clearly linearly independent, hence they form a basis of $C(A)$. $\square$

**Corollary 3.7.** *Let $r$ be the number of conjugacy classes of $G$ and $s$ be the number of irreducible $F$-representations of $G$, then*

(1) *$r = \dim_F C(A) = \sum_{i=1}^{s} \dim_F C(\Delta_i)$. In particular $r = s$ if and only if $\Delta_i$ is a central simple algebra over $F$ for all $i$.*

(2) *If* $F = \bar{F}$ *then* $\Delta_i = F$, $r = s$ *and* $|G| = \sum_{i=1}^{s} n_i^2$.

*Example* 3.8. (1) Cyclic groups: $G = C_n = \langle\, g \mid g^n = 1\,\rangle$, $F = \mathbb{Q}$. Then

$$A = \mathbb{Q}[G] \cong \mathbb{Q}[x]/(x^n - 1) \cong \bigoplus\nolimits_{d|n} \mathbb{Q}[x]/\ell_d(x) \cong \bigoplus\nolimits_{d|n} \mathbb{Q}(\zeta_d)$$

where $\ell_n(x) \in \mathbb{Z}[x]$ is the $d$-th cyclotomic polynomial which is irreducible over $\mathbb{Q}$, $\mathbb{Q}(\zeta_d)$ is the $d$-th cyclotomic field with $\zeta_d = e^{2\pi\sqrt{-1}/d}$.

In this case $A$ is abelian, hence all $n_i = 1$ and $\Delta_i = C(\Delta_i) = \mathbb{Q}(\zeta_{d_i})$ for some $d_i \mid n$. The irreducible representation $\rho_d$ corresponding to $d \mid n$ has degree $\psi(d)$.

If we start with $F = \mathbb{Q}(\zeta_n)$ instead, then

$$A \cong F[x]/\prod\nolimits_{i=0}^{n-1}(x - \zeta_n^i) \cong \bigoplus\nolimits_{i=0}^{n-1} F[x]/(x - \zeta_n^i) \cong \bigoplus\nolimits_{i=1}^{n} V_i$$

where $V_i \cong Fe_i$ is an one dimensional representation with $ge_i = \zeta_n^i e_i$. Hence there are $r = s = n$ inequivalent irreducible representations of $G$.

If we start with $\mathbb{Q}(\zeta_n) \supset F \supset \mathbb{Q}$, the structure of $F[G]$ varies dramatically!

(2) Dihedral groups: $G = D_n = \langle\, R, S \mid R^n = 1, S^2 = 1, SRS = R^{-1}\,\rangle$. We have $|D_n| = 2n$ and a set of representatives is given by $\{\, R^k, R^kS \mid 0 \le k \le n-1\,\} \supset C_n = \langle R\rangle$. The conjugacy classes are determined by

| $n$ | $r = \#$conj. classes | representatives |
|---|---|---|
| $2\nu + 1$ | $\nu + 2$ | $R^0, \ldots, R^\nu, S$ |
| $2\nu$ | $\nu + 3$ | $R^0, \ldots, R^\nu, R, RS$ |

Here are a few irreducible $\mathbb{C}$-representations: let $\rho_1 = \mathbf{1}$, $\rho_2 = \mathbf{sgn} : R \mapsto (1), S \mapsto (-1)$ be the obvious degree 1 representations on $F = \mathbb{C}$. Since $SRS = R^{n-1}$, those degree 1 representations of $C_n$ are generally not representations of $D_n$.

For $n = 2\nu + 1$, for each $k \in [1, \nu]$ we define a degree 2 representation

$$\sigma_k : \quad R \mapsto \begin{pmatrix} w^k & 0 \\ 0 & w^{-k} \end{pmatrix}, \quad S \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad V = \mathbb{C}e_1 \oplus \mathbb{C}e_2.$$

Here $w = \zeta_n$. They are clearly irreducible and inequivalent. We have constructed $2 + \nu = r$ irreducible $\mathbb{C}$-representations hence they are all of them. As a consistency check we compute $\sum_{i=1}^{r} n_i^2 = 2 \times 1^2 + \nu \times 2^2 = 2(2\nu + 1) = 2n = |D_n|$.

For $n = 2\nu$, $\nu \ge 2$, two more degree 1 representations are found: $\rho_3 : R \mapsto (-1), S \mapsto (1)$, $\rho_4 := \rho_2 \otimes \rho_3 : R \mapsto (-1), S \mapsto (-1)$. But now we take only $\sigma_k$, $k \in [1, \nu - 1]$ since $\sigma_\nu$ is reducible—it contains the invariant subspace $\mathbb{C}(e_1 + e_2)$. This gives all the $r = \nu + 3$ irreducible $\mathbb{C}$-representations. Also $\sum_{i=1}^{r} n_i^2 = 4 \times 1 + (\nu - 1) \times 2^2 = 4\nu = 2n = |D_n|$ as expected.

(3) Quaternion group: $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}^\times$. Notice that $Q_8 \ncong D_4$ since every subgroup of $Q_8$ is normal which is not the case for $D_4$.

Let $F = \mathbb{Q}$. There are at least two irreducible $\mathbb{Q}$-representations, the trivial one of degree 1 and the natural one of degree 4 acting on $\mathbb{H}(\mathbb{Q})$, the quaternion numbers with $\mathbb{Q}$ coordinates. The structure theorem then forces a decomposition

$$\mathbb{Q}[Q_8] = \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{H}(\mathbb{Q}).$$

This is consistent with the fact that there are 5 conjugacy classes of $Q_8$, namely $\{1\}$, $\{-1\}$, $\{i,-i\}$, $\{j,-j\}$, $\{k,-k\}$. If we consider $F = \mathbb{Q}(\sqrt{-1})$ instead, the decomposition becomes

$$F[Q_8] = F \oplus F \oplus F \oplus F \oplus M_2(F),$$

where $\mathbb{H}(\mathbb{Q}) \otimes_{\mathbb{Q}} F \cong M_2(F)$. This decomposes the degree 4 irreducible representation $\mathbb{H}(\mathbb{Q})$ into two copies of the degree 2 one $V = F^{\oplus 2}$.

Exercise 3.1. Write down the explicit formulas of the decompositions of $F[G]$ in Example 3.8, (2) and (3).

Example 3.8, (1) and (3) suggest the following

*Definition* 3.9 (Absolute irreducibility and splitting fields).

(1) Let $K/F$ be a field extension, then we define the $K$-representation $\rho_K := \rho \otimes_F K$ by composing $\rho$ with $\mathrm{GL}(V_F) \to \mathrm{GL}(V_F \otimes_F K)$.

(2) A representation $\rho$ is absolutely irreducible if $\rho_K$ is irreducible for all extension field $K/F$. This is equivalent to that $\rho_{\bar{F}}$ is irreducible.

(3) $K$ is a splitting field of $G$ if all irreducible $K$-representations of $G$ are absolutely irreducible. In particular, $\bar{F}$ is always a splitting field.

In Example 3.8-(1), $\mathbb{Q}(\zeta_n)$ is a splitting field of $C_n$. In Example 3.8-(3), $\mathbb{Q}(\sqrt{-1})$ is a splitting field of $Q_8$. These are finite extensions of $\mathbb{Q}$. According to the theory of CSA/$F$, a splitting field can be chosen to be a finite extension of $F$. More precise statement can be made.

**Theorem 3.10.** *Let* $\operatorname{char} F \nmid |G| < \infty$, $\rho : G \to \mathrm{GL}(V_F)$. *Then*

(1) *$\rho$ is irreducible* $\Longleftrightarrow$ $A' := \mathrm{End}_A V$ *is a division $F$-algebra.*

(2) *$\rho$ is absolutely irreducible* $\Longleftrightarrow$ $A' = F\,\mathrm{id}_V$.

PROOF. (1) "$\Rightarrow$" by Schur's lemma. For "$\Leftarrow$": if $\rho$ is reducible, Maschke's theorem implies $V = U \oplus U'$ for two sub representations. The projection $p$ onto $U$ then satisfies $p^2 = p$, that is $p(p-1) = 0$, but $p \neq 0, 1$.

(2) "$\Rightarrow$": if there is a $c \in A' \setminus F\,\mathrm{id}_V$, then the minimal polynomial $m_c(x) \in F[x]$ of $c$ is irreducible (since $A'$ is a division $F$-algebra by (1)). Consider the simple extension $K = F[x]/(m_c(x))$. It is a general fact that the minimal polynomial of a linear transformation is unchanged under field extensions. But $m_c(x)$ factors in $K[x]$, hence $0 = m_c(c) = f(c)g(c)$ and $A'_K$ is not a division $F$-algebra, this leads to a contradiction by (1). For "$\Leftarrow$": $A' = F\,\mathrm{id}_V$ implies $A'_K = K\,\mathrm{id}_V$. Hence $\rho_K$ is irreducible for all $K/F$. $\square$

Using this result together with knowledge in CSA$/F$, we may deduce

**Theorem 3.11.** *Let* char $F \nmid |G| < \infty$*. Then* $F$ *is a splitting field of* $G$ *if and only if* $F[G] \cong \bigoplus_i M_{n_i}(F)$*. That is,* $F$ *splits all the division algebras* $\Delta_i$ *appeared in the semi-simple decomposition.*

The proof is left to the readers.

## 2. Complex characters

In this section we work with complex representations of finite groups $G$, namely $F = \mathbb{C}$ unless specified otherwise.

*Definition* 3.12. Let $\rho : G \to \mathrm{GL}(V)$ be a $F$-representation. The character of $\rho$ is the function $\chi_\rho : G \to F$ defined by $\chi_\rho(g) := \operatorname{tr} \rho(g)$.

At the first sight it seems that characters $\chi$ contain less information than the representation $\rho$. However, for a single matrix $A$ the complete information of $\operatorname{tr} A^k$ for all $k \in \mathbb{N}$ is equivalent to the characteristic polynomial $f_A(x)$. Hence the trace function over the group $\rho(G)$ indeed contain rich informations of $\rho$. In fact we will show that "$\chi$ characterizes $\rho$ for $F = \mathbb{C}$"!

We start with a few immediate consequences following the definition:

(1) $\chi_\rho$ is a class function:

$$\operatorname{tr} \rho(hgh^{-1}) = \operatorname{tr} \rho(h)\rho(g)\rho(h)^{-1} = \operatorname{tr} \rho(g).$$

Namely $\chi_\rho(g)$ depend only on the conjugacy class of $g$. We denote the subspace of class functions by

$$\mathscr{C}(G, F) \subset F^{|G|}.$$

(2) If $U \subset V$ is $\rho(G)$-invariant, then

$$\chi_\rho = \chi_{\rho|_U} + \chi_{\rho|_{V/U}}.$$

This follow from the observation that for a choice of basis respects $V = U \oplus U_0$ (vector space decomposition) we have

$$\rho(g) \sim \begin{pmatrix} \rho|_U(g) & * \\ 0 & \rho|_{V/U}(g) \end{pmatrix}.$$

(3) $\chi_{\rho_1 \otimes \rho_2} = \chi_{\rho_1}\chi_{\rho_2}$ since $\operatorname{tr} A \otimes B = \operatorname{tr} A \operatorname{tr} B$, which is clear from

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & a_{mm}B \end{pmatrix}, \qquad m := \deg \rho_1.$$

(1), (2), (3) work for any $F$. Now we use the assumption $F = \mathbb{C}$:

(4) If $g^d = 1$ then $\rho(g)^d = \mathrm{id}_V$. Thus $m_{\rho(g)}(x) \mid (x^d - 1)$ which implies that all roots $w_i$'s are distinct $d$-th roots of 1. Then $\rho(g)$ is diagonalizable

$$\rho(g) \sim \begin{pmatrix} w_1 & & \\ & \ddots & \\ & & w_m \end{pmatrix}, \qquad m := \deg \rho$$

In particular $\chi_\rho(g) = \sum_{i=1}^m w_i$, which leads to the simple observation:

**Corollary 3.13.** *$|\chi_\rho(g)| \le \deg \rho$, with equality holds if and only if $\rho(g) = w\, \mathrm{id}_V$ where $w^d = 1$ for $d = \exp G$.*

*Moreover, $\chi_\rho(g) = \deg \rho$ if and only if $\rho(g) = \mathrm{id}_V$, i.e. $g \in \ker \rho$.*

(5) $\chi_{\rho^*} = \overline{\chi_\rho}$ since ${}^t\mathrm{diag}(w_i)^{-1} = \mathrm{diag}(w_i)^{-1} = \mathrm{diag}(w_i^{-1}) = \mathrm{diag}(\overline{w_i})$.

*Example* 3.14. (1) For the trivial representation $\mathbf{1}$ on $F$, $\chi_{\mathbf{1}}(g) = 1_F$ for all $g \in G$.

(2) For the regular representation, $\chi_{\mathrm{reg}}(1) = |G|$ and $\chi_{\mathrm{reg}}(g) = 0$ for all $g \neq 1$.

(3) For $F = \mathbb{C}$, the number of equivalence classes of irreducible representations $s$ is the same as the number of conjugacy classes $r$ (Corollary 3.7-(2)). A character table is a $r \times r$ table to list all possible character values for a finite group $G$.

For $G = D_n$, using Example 3.8-(2) we may calculate its character table easily: for $n = 2\nu + 1$, it is

| | $1$ | $S$ | $R^j$ |
|---|---|---|---|
| $\mathbf{1}$ | $1$ | $1$ | $1$ |
| $\mathbf{sgn}$ | $1$ | $-1$ | $1$ |
| $\sigma_k$ | $2$ | $0$ | $w^{kj} + w^{-kj}$ |

where $k, j \in [1, \nu]$. Notice that $\chi$ characterizes $\rho$: $\chi_\rho \neq \chi_{\rho'}$ if $\rho \not\cong \rho'$.

The major reason to make the character theory powerful comes from Schur's orthogonality relations which we describe now. At the beginning we may work with any field $F$ and group $G$ with with $\mathrm{char}\, F \nmid |G| < \infty$.

For $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to \mathrm{GL}(V')$, we have a representation

$$\rho'' : G \to \hom_F(V, V') = V' \otimes_F V^*$$

defined by, for any $g \in G$, $e \in \hom_F(V, V')$,

$$\rho''(g)\, e := \rho'(g)\, e\, \rho(g)^{-1}.$$

(Indeed $\rho'' = \rho' \otimes \rho^*$ as defined before.) Now we "symmetrize it":

*Claim* 3.15. $\eta(e) := \sum_{g \in G} \rho'(g)\, e\, \rho(g)^{-1} \in \hom_{F[G]}(V, V')$.

PROOF.

$$\rho'(h)\eta(e) = \sum_g \rho'(hg)\, e\, \rho(g)^{-1} = \sum_g \rho'(g)\, e\, \rho(h^{-1}g)^{-1}$$
$$= \Big(\sum_g \rho'(g)\, e\, \rho(g)^{-1}\Big)\rho(h) = \eta(e)\rho(h).$$

This shows that $\eta(e)$ is a morphism of $F[G]$-modules. □

If both $\rho$ and $\rho'$ are irreducible, then Schur's lemma implies that $\eta(e) = 0$ whenever $\rho \not\cong \rho'$.

If $\rho' = \rho$, then $\eta(e) \in \operatorname{End}_{F[H]} V$ which is a division $F$-algebra. If we further assume that $F$ is a splitting field of $G$, say $F = \mathbb{C}$, or simply that $\rho$ is absolutely irreducible, then we have $\eta(e) \in F\,\mathrm{id}_V$ by Theorem 3.10.

For $F = \mathbb{C}$, a direct proof is easy: let $\lambda \in \mathbb{C}$ be an eigenvalue of $\eta(e)$, then $0 \neq \ker(\eta(e) - \lambda\mathrm{id}_V) \subset V$ is readily seen to be $\rho(G)$-invariant, hence it equals $V$ since $\rho$ is irreducible, and so $\eta(e) = \lambda\mathrm{id}_V$.

**Theorem 3.16** (Schur's orthogonality relations)**.** *Let $F$ be a splitting field of $G$ with $\operatorname{char} F \nmid |G| < \infty$. $\rho_1, \ldots, \rho_s$ be the set of irreducible representations with matrices $\rho_i(g) \sim (T^i_{rt})(g)$. Then $\operatorname{char} F \nmid n_i := \deg \rho_i$ for all $i$ and*

(i) $\sum_g T^j_{kl}(g) T^i_{rt}(g^{-1}) = 0$ *if $i \neq j$,*

(ii) $\sum_g T^i_{kl}(g) T^i_{rt}(g^{-1}) = \delta_{kt}\delta_{lr}\dfrac{|G|}{n_i}$.

PROOF. Let $e_{lr}$ be the elementary matrix, then the sum is simply $\eta(e_{lr})_{kt}$ and (i) follows directly.

For (ii), we have $\eta(e_{lr})_{kt} = \lambda_{lr}\delta_{kl}$ for some $\lambda_{lr} \in F$. Since

$$T^i_{rt}(g^{-1}) = (T^i(g))^{-1}_{rt},$$

by summing over $k = l \in [1, n_i]$ we get $0 \neq |G|\,\delta_{lr} = n_i\,\lambda_{lr}$ since $\operatorname{char} F \nmid |G|$. This implies $\operatorname{char} F \nmid n_i$ and (ii) follows accordingly. □

*Remark* 3.17. For $F = \mathbb{C}$, we will prove later that $n_i \mid |G|$. This fails for general $F$ even for cyclic groups, see Example 3.8-(1).

From now on we work only for $F = \mathbb{C}$. A major benefit from it is:

*Definition* 3.18. For $\phi, \psi \in \mathbb{C}^{|G|} = \{ f : G \to \mathbb{C} \}$, we define the (Hermitian) inner product

$$(\phi, \psi)_G := \frac{1}{|G|}\sum_{g\in G} \overline{\phi(g)}\psi(g).$$

**Corollary 3.19.** *Let $\chi_i = \chi_{\rho_i}$, $i \in [1, s]$ be the irreducible characters. Then*

$$(\chi_i, \chi_j) = \delta_{ij}.$$

PROOF. Since $\chi_i(g) = \sum_{k=1}^{n_i} T^i_{kk}(g)$ and

$$\chi_i(g^{-1}) = \operatorname{tr} \rho_i(g^{-1}) = \operatorname{tr} \rho_i(g)^{-1} = \overline{\operatorname{tr} \rho_i(g)} = \overline{\chi_i(g)},$$

Theorem 3.16-(i) then implies that $(\chi_i, \chi_j) = 0$ if $i \neq j$. For $i = j$, Theorem 3.16-(ii) implies that $(\chi_i, \chi_i) = \sum_{k,r=1}^{n_i} \delta_{kr}\delta_{kr}/n_i = 1$. □

Every complex representation $\rho$ of $G$ can be uniquely decomposed as

$$\rho = m_1 \rho_1 \oplus \ldots \oplus m_s \rho_s, \qquad m_i \in \mathbb{Z}_{\geq 0}.$$

Hence $\chi_\rho = m_1 \chi_1 + \ldots + m_s \chi_s$ and then $m_i = (\chi_\rho, \chi_i)$. This implies

**Corollary 3.20.** *For $\mathbb{C}$-representations, $\rho \cong \rho'$ if and only if $\chi_\rho = \chi_{\rho'}$.*

Also $(\chi_\rho, \chi_\rho) = \sum_{i=1}^{s} m_i^2$, which implies

**Corollary 3.21.** *A $\mathbb{C}$-representation $\rho$ is irreducible if and only if $(\chi_\rho, \chi_\rho) = 1$.*

Finally, since "$s = r$" for $F = \mathbb{C}$, we conclude

**Theorem 3.22.** *The irreducible characters $\chi_1, \ldots, \chi_s$ form an orthonormal basis of the space of class functions $\mathscr{C}(G)$.*

SECOND PROOF. The theorem is equivalent to $s = r$, which is proved via the Wedderburn–Artin structure theorem. Here we give a direct proof using only the character theory. We only need to show

*Claim* 3.23. If $f \in \mathscr{C}(G)$ has $(f, \chi_i) = 0$ for all $i \in [1, s]$ then $f = 0$.

For each $i \in [1, s]$, we define

$$T_i := \sum_{g \in G} \overline{f(g)} \rho_i(g) \in \operatorname{End}_{\mathbb{C}} V_i.$$

In fact $T_i$ is $\rho_i(G)$-linear: for any $h \in G$ we compute

$$\begin{aligned} \rho_i(h) T_i &= \sum_{g \in G} \overline{f(g)} \rho_i(hg) = \Big( \sum_{g \in G} \overline{f(g)} \rho_i(hgh^{-1}) \Big) \rho_i(h) \\ &= \Big( \sum_{g \in G} \overline{f(h^{-1}gh)} \rho_i(g) \Big) \rho_i(h) = T_i \, \rho_i(h) \end{aligned}$$

since $f$ is a class function. Schur's lemma implies that $T_i = \lambda I_{V_i}$. But $\operatorname{tr} T_i = (f, \chi_i) = 0$ hence $T_i = 0$. In particular this implies

$$\sum_{g \in G} \overline{f(g)} \, \rho_{\mathrm{reg}}(g) = 0.$$

Apply it to the vector 1 we get $\sum_{g \in G} \overline{f(g)} \, g = 0$. So $f(g) = 0$ for all $g$. □

*Example* 3.24. (1) We had seen that $\rho_{\text{reg}} = \sum_{i=1}^{s} n_i \, \rho_i$ using the structure theorem for $F[G]$ (cf. Corollary 3.5). For $F = \mathbb{C}$ this follows from the character theory immediately since the multiplicity $m_i$ of $\rho_i$ in $\rho_{\text{reg}}$ is

$$m_i = (\chi_{\text{reg}}, \chi_i) = \frac{1}{|G|} \sum_g \chi_{\text{reg}}(g) \chi_i(g) = \chi_i(1) = \deg \rho_i = n_i.$$

(2) Character table for $S_4$ is given by

| | $(1)_1$ | $(12)_6$ | $(123)_8$ | $(1234)_6$ | $(12)(34)_3$ |
|---|---|---|---|---|---|
| $\mathbf{1}$ | 1 | 1 | 1 | 1 | 1 |
| **sgn** | 1 | $-1$ | 1 | $-1$ | 1 |
| $\rho_{\text{st}}$ | 3 | 1 | 0 | $-1$ | $-1$ |
| $\rho_{\text{st}} \otimes$ **sgn** | 3 | $-1$ | 0 | 1 | $-1$ |
| $W$ | 2 | 0 | $-1$ | 0 | 2 |

To see it, there are 5 conjugacy classes $C_j$ shown in the top row where the subscript is $|C_j|$. As a check, we see that $\sum_{j=1}^{5} |C_j| = 24 = |S_4|$.

There are 5 irreducible $\mathbb{C}$-representations of $S_4$ where the first two degree 1 representations $\rho_1, \rho_2$ are obviously there. From $1 + 1 + n_3^2 + n_4^2 + n_5^2 = 24$ we see that the remaining 3 must be of degree 3, 3, 2.

To get 3-dimensional representations, the standard way is to make $S_4$ acts on $\mathbb{C}^4 = \bigoplus_{i=1}^{4} \mathbb{C} \, e_i$ as a permutation representation on the basis. Since $v := \sum_{i=1}^{4} e_i$ spans a $S_4$-invariant line, we get a $S_4$ representation on $V := \mathbb{C}^4 / \mathbb{C} \, v \cong (\mathbb{C} \, v)^{\perp}$. We call it $\rho_3 = \rho_{\text{st}}$ and it character (written as a vector in the above order) is

$$\chi_{\text{st}} = \chi_{\mathbb{C}^4} - \chi_{\mathbb{C} \, v} = (4, 2, 1, 0, 0) - (1, 1, 1, 1, 1) = (3, 1, 0, -1, -1).$$

$\rho_{\text{st}}$ is indeed irreducible since $(\chi_{\text{st}}, \chi_{\text{st}}) = (3^2 + 6 + 0 + 6 + 3)/24 = 1$.

To get another degree 3 representation $\rho_4$. we tensor $\rho_3$ with non-trivial degree 1 representations. It must be irreducible since $(\chi\chi', \chi\chi') = (\chi, \chi)$ if $\deg \chi' = 1$.

We call the remaining $\rho_5$ of degree 2 by $W$. $\chi_W$ is easily determined by the others since $0 = \chi_{\text{reg}}(g) = \sum n_i \chi_i(g)$ for $g \neq 1$. The result is $\chi_W = (2, 0, -1, 0, 2)$.

We have determined $W$ abstractly. To see it concretely, the idea is to make use of subgroups or quotient groups of $S_4$. For example, we have an exact sequence

$$1 \to K_4 \to S_4 \xrightarrow{\pi} S_3 \to 1$$

where $K_4 = \{ 1, (12)(34), (13)(24), (14)(23) \} \lhd S_4$ is the Klein 4-group. Then any irreducible representation $\sigma$ of $S_3$ is also irreducible for $S_4$ via $\sigma \circ \pi$. Since $S_3 \cong D_3$, we may simply take $\sigma_1$ in Example 3.8-(2) to get $W = \sigma_1 \circ \pi$. It is readily seen that $\chi_{\sigma_1} \circ \pi$ (cf. Example 3.14-(3)) coincides with $\chi_W$ as computed above.

(3) Product groups: if $G$ (resp. $G'$) has irreducible $\mathbb{C}$-representations $\rho_i$ (resp. $\rho_j'$), then the irreducible $\mathbb{C}$-representations of $G \times G'$ are given precisely by the "outer tensor product" $\rho_i \, \# \, \rho_j'$'s where

$$(\rho \, \# \, \rho')(g, g') := \rho(g) \otimes \rho'(g') \in \mathrm{GL}\,(V \otimes V').$$

Indeed,

$$
\begin{aligned}
(\chi_{\rho\#\rho'}, \chi_{\rho\#\rho'}) &= \frac{1}{|G \times G'|} \sum_{g,g'} |\chi_{\rho\#\rho'}(g,g')|^2 \\
&= \frac{1}{|G|} \sum_{g} |\chi_\rho(g)|^2 \frac{1}{|G'|} \sum_{g'} |\chi_{\rho'}(g')|^2 = (\chi_\rho, \chi_\rho)(\chi_{\rho'}, \chi_{\rho'}).
\end{aligned}
$$

Hence $(\chi_{\rho\#\rho'}, \chi_{\rho\#\rho'}) = 1$ if and only if $(\chi_\rho, \chi_\rho) = 1 = (\chi_{\rho'}, \chi_{\rho'})$. This shows that $\{\, \rho_{ij} := \rho_i \# \rho'_j \mid i \in [1,s], j \in [1,s'] \,\}$ gives $ss'$ inequivalent irreducible representations of $G \times G'$. To see that they are all of them, we simply notice that

$$\textstyle\sum_{i,j} (\deg \rho_{ij})^2 = \sum_{i,j} (\deg \rho_i)^2 (\deg \rho'_j)^2 = |G||G'| = |G \times G'|.$$

Example 3.24-(3) shows that representation theory for product groups is completely reduced to the study of its factors. In fact, representation theory of normal subgroups are sub-theory of the group as shown in Example 3.24-(2). In general there are plenty of subgroup while few of then are normal. Hence it is more practical to study relations of representation theories with subgroups. This will be carried out in later sections.

There is a situation where all good things happen, namely the case of (finite) abelian groups or abelian subgroups.

**Proposition 3.25.** *Let $G$ be a finite group, then $G$ is abelian if and only of all its complex irreducible representations are one-dimensional.*

PROOF. This follows from the structure theorem directly: $G$ is abelian $\Leftrightarrow$ $G$ has $|G| = r = s$ conjugacy classes $\Leftrightarrow$ all $n_i = 1$ in $|G| = \sum_{i=1}^{s} n_i^2$. $\square$

A direct proof for the "only if" part is also easy: let $\rho : G \to \mathrm{GL}(V)$ be irreducible. Let $g \in G$ and $0 \neq \ker(\rho(g) - \lambda(g) I_V) =: V_0$ for some eigenvalue $\lambda(g) \in \mathbb{C}$. Since $G$ is abelian, $V_0$ is $\rho(G)$-invariant and hence $V = V_0$. This implies that $\rho(g) = \lambda(g) I_V$ for all $g \in G$. But then any $\mathbb{C}\, v \subset V$ is $\rho(G)$-invariant hence in fact $V$ is one-dimensional.

**Corollary 3.26.** *Let $G$ be a finite abelian group, then the set of all irreducible $\mathbb{C}$-representations of $G$ forms a group $\hat{G} := \hom(G, \mathbb{C}^\times)$, the dual group of $G$, which is isomorphic to $G$ (non-canonically).*

PROOF. Degree 1 representations are necessarily irreducible and equivalent to their characters $\rho = \chi_\rho : G \to \mathbb{C}^\times$. They form a group under tensor product, which coincides with multiplication of characters. For $G$ finite abelian, we get the character group $\hat{G}$ as defined.

The fundamental theorem of (finitely generated) abelian groups implies that $G = \bigoplus G_i$, $G_i = \langle g_i \rangle \cong \mathbb{Z}/(e_i)$. Then

$$\hat{G} = \hom(\bigoplus G_i, \mathbb{C}^\times) \cong \prod \hom(G_i, \mathbb{C}^\times) \cong \prod \mu_{e_i} \cong G,$$

where $\hat{G}_i \cong \mu_{e_i}$ (the group of $e_i$-th roots of 1) since each $\rho \in \hom(G_i, \mathbb{C}^\times)$ is determined by $\rho(g) \in \mu_{e_i}$. $\square$

Exercise 3.2. Let $A \subset G$ be an abelian subgroup and $\rho$ be an irreducible complex representation of $G$ with degree $n_\rho$. (1) Show that $n_\rho \leq [G : A]$. (2) For $A = C(G)$, show that $n_\rho^2 \leq [G : A]$.

*Remark* 3.27. The orthogonality of characters for abelian groups is essentially trivial. The same reasoning as in Corollary 3.26 reduces the problem to the one for cyclic groups, which is a simple exercise in geometric series.

To conclude this section, we emphasize that it is essential, in finite group representations, to construct/analyze invariant subspaces. This is mostly achieved by (i) averaging/symmetrizing a linear transformation or (ii) to work with eigenspaces of an operator lying in the center.

## 3. Arithmetic properties of characters

Recall that $a \in \mathbb{C}$ is an algebraic number, i.e. $a$ is algebraic over $\mathbb{Q}$, if there is a monic polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(a) = 0$. Also $a$ is an algebraic integer, i.e. $a$ is integral over $\mathbb{Z}$, if the monic polynomial $f(x) \in \mathbb{Z}[x]$. We may always take $f(x)$ to be the minimal polynomial.

It is elementary to see that (1) $a$ is algebraic over $\mathbb{Q} \Rightarrow ma$ is integral over $\mathbb{Z}$ for some $m \in \mathbb{Z}$. (2) If $a \in \mathbb{Q}$ and integral over $\mathbb{Z}$ then $a \in \mathbb{Z}$.

**Lemma 3.28.** *Let $a \in \mathbb{C}$, then $a$ is integral over $\mathbb{Z} \iff$ there is a finitely generated $\mathbb{Z}$-module $M \subset \mathbb{C}$ such that $aM \subset M$.*

Proof. If $f(a) = 0$ for $f(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0 \in \mathbb{Z}[x]$, then $M := \bigoplus_{i=0}^{n-1} \mathbb{Z}\, a^i$ satisfies $aM \subset M$.

Conversely, given $M = \sum_{j=1}^n \mathbb{Z} m_j \subset \mathbb{C}$ such that $aM \subset M$, then $am_i = \sum a_{ij} m_j$ for some $a_{ij} \in \mathbb{Z}$. That is,

$$\textstyle\sum_{i=1}^n (a\delta_{ij} - a_{ij}) m_j = 0, \qquad i \in [1, n].$$

Hence $f(a) = 0$ for $f(x) := \det(x\delta_{ij} - a_{ij}) \in \mathbb{Z}[x]$, which is monic. $\square$

**Corollary 3.29.** *The set $R$ of all algebraic integers is a ring and the set $\overline{\mathbb{Q}}$ of all algebraic numbers is a field. The quotient field of $R$ equals $\overline{\mathbb{Q}}$.*

PROOF. For $a, b \in R$, we need show that $a + b \in R$ and $ab \in R$.

Let $f(x), g(x) \in \mathbb{Z}[x]$ be monic polynomials with $f(a) = 0$, $g(b) = 0$. If $\deg f(x) = m$, $\deg g(x) = n$, we set

$$M = \sum_{i \in [0,m-1], j \in [0,n-1]} \mathbb{Z}\, a^i b^j.$$

Then it is clear that

$$(a + b)M \subset M, \qquad abM \subset M$$

since all terms with $a$ degree higher than $m - 1$ or $b$ degree higher than $n - 1$ can be reduced using $f(a) = 0 = g(b)$.

The proof that $\overline{\mathbb{Q}}$ is a field is entirely the same. We simply replace $\mathbb{Z}$-modules by $\mathbb{Q}$-vector spaces in Lemma 3.28 to get criterion for $a$ being algebraic. Then the same proof as above gives the result.

Since $R \subset \overline{\mathbb{Q}}$, its quotient field $Q(R) \subset \overline{\mathbb{Q}}$. For the reverse inclusion, $a \in \overline{\mathbb{Q}} \Rightarrow b = ma \in R$ for some $m \in \mathbb{Z}$, hence $a = b/m \in Q(R)$. □

Now we investigate these integral properties for irreducible complex representations $\rho_i$ and their characters $\chi_i$ of a finite group $G$.

**Corollary 3.30.** *All character values $\chi(g)$'s are algebraic integers.*

PROOF. Roots of unity are algebraic integers. Hence any finite integral combination of them, e.g. $\chi(g)$, is too by Corollary 3.29. □

Much better/precise results hold through investigation on the "interactions" between irreducible representations and conjugacy classes:

**Theorem 3.31.** *Let $\chi_1, \ldots, \chi_s$ be the irreducible characters of $G$, $n_i = \deg \chi_i$, $C_1, \ldots, C_s$ the conjugacy classes, and $c_j = \sum_{g \in C_j} g$. Then*
(1) *On $V_i$, $\rho_i(c_j) = \lambda_{ij} I_{V_i}$ is a scalar multiplication with*

$$\lambda_{ij} = \frac{\chi_i(c_j)}{n_i} = |C_j| \frac{\chi_i(g_j)}{n_i}, \qquad g_j \in C_j, \quad i, j \in [1, s].$$

(2) *All these eigenvalues $\lambda_{ij}$ are algebraic integers.*

PROOF. Recall that $c_j = \sum_{g \in C_j} g$, $j \in [1, s]$, is a base of $Z = C(F[G])$ for any field $F$ (Proposition 3.6). Since $c_j c_k \in Z$, the proof actually implies that

$$c_j c_k = \sum\nolimits_\ell m_{jk}^\ell \, c_\ell$$

for some $m_{jk}^\ell \in \mathbb{Z}_{\geq 0}$. Let $F = \mathbb{C}$ and apply $\rho_i$ to the above formula.

In doing so we notice that $\rho_i(c_j) = \lambda \, I_{V_i}$ for an eigenvalue $\lambda \in \mathbb{C}$. This follows from the fact that $c_j \in Z$ and then $\ker(\rho_i(c_j) - \lambda \, I_{V_i}) \subseteq V_i$ is a non-trivial $\rho_i(G)$-invariant subspace, hence equals $V_i$. Taking trace we get $n_i \lambda = \chi_i(c_j) = |C_j| \chi_i(g_j)$ for any $g_j \in C_j$, hence the formula for $\lambda_{ij}$.

Now for each $i$, $\rho_i(c_j)\rho_i(c_k) = \sum m_{jk}^\ell \, \rho_i(c_\ell)$ gives

$$\lambda_{ij} \lambda_{ik} = \sum\nolimits_\ell m_{ij}^\ell \lambda_{i\ell}.$$

For $M = \sum_{m=1}^s \mathbb{Z} \, \lambda_{im}$ we get $\lambda_{ij} M \subset M$, hence $\lambda_{ij} \in R$ as expected. $\square$

**Corollary 3.32.** *$n_i \mid |G|$ for all $i$.*

PROOF. From the orthogonal relation $(\chi_i, \chi_j) = \delta_{ij}$, we compute

$$\delta_{ij} = \frac{1}{|G|} \sum\nolimits_{k=1}^s \sum\nolimits_{g \in C_k} \overline{\chi_i(g)} \chi_j(g).$$

For $i = j$ and for any choice of $g_k \in C_k$, we get

$$\mathbb{Q} \ni \frac{|G|}{n_i} = \sum_{k=1}^s \overline{\chi_i(g_k)} \left( |C_k| \frac{\chi_i(g_k)}{n_i} \right) \in R.$$

Thus $|G|/n_i \in \mathbb{Z}$. $\square$

*Remark* 3.33. In Schur's orthogonal relation (Theorem 3.16-(ii)), we might have already concluded $|G|/n_i \in \mathbb{Z}$ if we know that $\rho_i(g)$ can be represented by matrices $T_i(g)$ over $R$. Since all the traces are $R$-valued, this seems to be plausible. It turns out to be a deep question which remains largely open in representation theory of finite groups.

The divisibility in Corollary 3.32 is nice but not optimal, since for abelian groups we indeed have $n_i = 1$ for all $i$. The following improvement due to Tate takes into account the abelian phenomenon.

**Proposition 3.34.** *Let $Z$ be the center of $G$, then $n_i \mid [G : Z]$ for all $i$.*

PROOF. Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible complex representation. Consider the $m$-th outer tensor product $\rho^m : G^m \to \mathrm{GL}(V^{\otimes m})$ which is still irreducible (cf. Example 3.24-(3)).

Since $\rho(g)$ acts as scalar multiplications on $V$ for $g \in Z$, we see that $\ker \rho^m$ contains the subgroup $D := \{ (g_i) \in Z^m \mid \prod g_i = 1 \}$ which has order $|Z|^{m-1}$. Hence we get an irreducible representation

$$\bar{\rho}^m : G^m/D \to \mathrm{GL}(V^{\otimes m}).$$

Corollary 3.32 implies that $(\deg \rho)^m \mid |G|^m/|Z|^{m-1} = [G:Z]^m |Z|^{-1}$. Since this holds for all $m \in \mathbb{N}$, we then conclude that $\deg \rho \mid [G:Z]$. $\square$

One of the most remarkable early applications of character theory is

**Theorem 3.35** (Burnside 1904)**.** *Any finite group $G$ with $|G| = p^a q^b$ is solvable, where $p$ and $q$ are primes and $a, b \in \mathbb{Z}_{\geq 0}$..*

The proof requires some preparations. First we need to improve the "interactions" between irreducible representations and conjugacy classes.

**Lemma 3.36.** *Let $\rho : G \to \mathrm{GL}(V)$ be an irreducible $\mathbb{C}$-representation of a finite group $G$, and $C$ be a conjugacy class such that $(|C|, \deg \rho) = 1$.*

*Then for every $g \in C$, either $\chi_\rho(g) = 0$ or $\rho(g) \in \mathbb{C}\, 1_V$.*

PROOF. Denote $\chi = \chi_\rho$ and $\deg \rho = d$. Then $1 = \ell|C| + md$ for some $\ell, m \in \mathbb{Z}$. By Theorem 3.31-(2), we get

$$a := \frac{\chi(g)}{d} = \ell\,|C|\frac{\chi(g)}{d} + m\chi(g) \in R.$$

Let $N = \exp G$ and $H = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Then $\chi(g)$ is a sum of $N$-th roots of 1. Since any $s \in H$ sends $N$-th roots of 1 to themselves, we have $|\chi(g)| \leq d \Rightarrow |s\chi(g)| \leq d$. So $|sa| \leq 1$ for all $s \in H$. Then

$$|N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(a)| = |\textstyle\prod_{s \in H} sa| \leq 1.$$

Since $N_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}(a) \in \mathbb{Q} \cap R = \mathbb{Z}$, it must be 0 or $\pm 1$.

The former case occurs if and only if $a = 0$, i.e. $\chi(g) = 0$. In the latter case we have $|\chi(g)| = d$. This implies $\rho(g) = w\, I_V$ for some $w = \zeta_N^k$. $\square$

**Theorem 3.37.** *Let $G$ be a finite non-abelian simple group. Then every conjugacy class $C$ of $G$ has $|C| \neq p^m$ for any prime $p$ and $m \in \mathbb{N}$.*

PROOF. Suppose that $|C| = p^m$, $m \geq 1$.

Let $\rho_1 = \mathbf{1}, \rho_2, \ldots, \rho_s$ be the irreducible representations of $G$, $\chi_i := \chi_{\rho_i}$ and $n_i := \deg \rho_i$. $G$ is simple implies that for $i \geq 2$, $\ker \rho_i = \{1\}$. Define

$$G_i := \{ g \in G \mid \rho_i(g) \in \mathbb{C}\, I_V \} \lhd G.$$

Let $i \geq 2$. If $p \nmid n_i$ and $\chi_i(g) \neq 0$ for $g \in C_i$, then Lemma 3.36 implies that $G_i \neq \{1\}$. Since $G$ is simple, we get $G_i = G$. However, this implies that

$$G \cong \rho_i(G) = \rho_i(G_i) \subset \mathbb{C}^\times$$

is abelian, which is excluded by our assumption. Hence if $p \nmid n_i$, $i \geq 2$, then $\chi_i(g) = 0$ for $g \in C$.

Now for $g \neq 1$ we have

$$0 = \chi_{\text{reg}}(g) = 1 + \textstyle\sum_{i=2}^{s} n_i \chi_i(g).$$

In particular for $g \in C$ we get $0 = 1 + p\,a$ where $a \in R$. But this implies that $-1/p \in R$ which is a contradiction. This proves the theorem. □

Proof of Burnside's theorem. Let $|G| = p^a q^b$ with $a \geq 1$. (If $a = 0$ then $G$ is solvable since $|G| = q^b$.)

Let $P \in \operatorname{Syl}_p(G)$ and $Z = C(P) \neq \{1\}$. Pick $1 \neq z \in Z$, then

$$C(z) \equiv C_G(z) \supset P$$

implies that $[G : C(z)] = q^c$ for $c \leq b$. Recall that $[G : C(z)] = |C|$, where $C$ is the conjugacy class of $z$. Thus if $[G : C(z)] \neq 1$ the above theorem implies that either $G$ is abelian, hence solvable, or $G$ is not simple.

In the latter case there is a normal subgroup $1 \neq H \triangleleft G$. By induction on $|G|$, both $H$ and $G/H$ are solvable. Hence $G$ is solvable. □

A näive extension of Burnside's theorem is not possible since $A_5$ is a simple group with $|A_5| = 60 = 2^2 \times 3 \times 5$. In fact $A_5$ is the unique simple non-abelian group with order $\leq 60$. Nevertheless, without the prime 2, Feit and Thompson had achieved the following "ground-breaking" result:

**Theorem 3.38** (Feit–Thompson 1963)**.** *A finite group of odd order is solvable.*

The proof consists of 255 pages which also relies on character theory heavily. Unfortunately it is outside the scope of this basic course.

## 4. Inductions and restrictions

*Definition* 3.39 (Induced representation). Let $H \subset G$ be a subgroup of finite index $r = [G : H] < \infty$ and $\sigma : H \to \mathrm{GL}(U)$ be an $F$-representation of $H$. The induced $F[G]$-module

$$\operatorname{Ind}_H^G \sigma \equiv \operatorname{Ind}_H^G U := F[G] \otimes_{F[H]} U$$

defines a representation $\sigma^G : G \to \mathrm{GL}(U^G)$ with $U^G := \bigoplus^r U$, called the induced representation of $\sigma$ from $H$ to $G$.

To get an explicit formula of the action, let $s_i \in G$, $i \in [1, r]$ be representatives of cosets $G/H = \{ H_i = s_i H \mid i \in [1, r] \}$. Then $G$ acts on $G/H$ as permutations $\pi : G \to S_r$ and we get $\mu_i(g) \in H$, $i \in [1, r]$, such that

$$gH_i = H_{\pi(g)i},$$
$$gs_i = s_{\pi(g)i}\, \mu_i(g).$$

Set $A = F[G]$ and $B = F[H]$ and then $B \hookrightarrow A$ is an $F$-subalgebra. Viewing $A = A_B$ and using the fact that any $g \in G$ has a unique representation $g = s_i h$ with $h \in H$, we see that $A$ is a free right $B$-module with base $s_i$'s.

Thus, if $\{e_j\}$ is a $F$-base of $U$ then $\{s_i \otimes_B e_j\}$ is a $F$-base of

$$A \otimes_B U = \bigoplus\nolimits_{i=1}^{r} s_i \otimes_B U.$$

An element $u = (u_i)_{i=1}^r \in U^G \cong A \otimes_B U$ corresponds to (for $u_i = \sum a_{ij}\, e_j$)

$$u = \sum\nolimits_{i=1}^{n} s_i \otimes_B u_i = \sum\nolimits_{i,j} a_{ij}\, s_i \otimes_B e_j.$$

**Proposition 3.40** (Induced character)**.** *For $(u_i)_{i=1}^r \in U^G$, we have*

$$\sigma^G(g)\left((u_i)_{i=1}^r\right) = \left(\sigma(\mu_{\pi(g)^{-1}i}(g))\, u_{\pi(g)^{-1}i}\right)_{i=1}^r.$$

*If $G$ is a finite group then*

$$\chi_{\sigma^G}(g) = \sum_{i=1}^{r} \tilde{\chi}_\sigma(s_i^{-1} g s_i) = \frac{1}{|H|} \sum_{s \in G} \tilde{\chi}_\sigma(s^{-1} g s),$$

*where $\tilde{\chi}_\sigma(g) := \chi(g)$ for $g \in H$ and $\tilde{\chi}(g) := 0$ if $g \notin H$.*

PROOF. We compute, for $k \in [1, r]$,

$$\begin{aligned}\sigma^G(g)(s_k \otimes_B u_k) &= g s_k \otimes_B u_k = s_{\pi(g)k}\, \mu_k(g) \otimes_B u_k \\ &= s_{\pi(g)k} \otimes_B \sigma(\mu_k(g))\, u_k.\end{aligned}$$

Thus if $\pi(g)k = i$ then $k = \pi(g)^{-1} i$ as stated.

The character $\chi_{\sigma^G}(g)$ is defined. It receives non-trivial contributions on the block $s_i U := s_i \otimes_B U$ only if $\pi(g)i = i$. That is, $g s_i H = s_i H$, or equivalently $s_i^{-1} g s_i \in H$. In that case we have $\mu_i(g) = s_i^{-1} g s_i$ and the above explicit computation shows that the trace of $\sigma^G(g)$ on $s_i U$ equals $\chi_\sigma(s_i^{-1} g s_i)$ as stated. When $G$ is finite, $H$ is then finite and for all $s = s_i h$ with $h \in H$ we have the same character value

$$\chi_\sigma(s^{-1} g s) = \chi_\sigma(h^{-1} s_i^{-1} g s_i h) = \chi_\sigma(s_i^{-1} g s_i).$$

Hence the last formula follows. □

There is also a simple criterion to characterize induced modules:

**Proposition 3.41.** *Let $H \subset G$ with $r = [G : H] < \infty$ and $\rho : G \to \mathrm{GL}(V)$ be an $F$-representation. Then $\rho = \sigma^G$ for $\sigma : H \to \mathrm{GL}(U) \iff$* (i) *$U \subset V$ as $F[H]$-modules and* (ii) *$V = \bigoplus_{i=1}^{r} s_i U$ where $\{s_i\}$ represents $G/H$.*

PROOF. Denote $A = F[G]$ and $B = F[H]$.

$\Rightarrow$: since $U^G = A \otimes_B U = \bigoplus_{i=1}^{r} s_i \otimes_B U$, we simply pick $s_1 = 1$ and identify $s_i U = s_i \otimes_B U \subset U^G$.

$\Leftarrow$: the assumptions show that $V = AU$. Also $s_i \in G$ implies that $s_i$ is invertible in $A$, hence $s_i : U \to s_i U$, $x \mapsto s_i x$ is bijective. Then

$$[s_i U : F] = [U : F] \implies [V : F] = [G : H][U : F].$$

Now the map $A \times U \to V$, $(a, x) \mapsto ax$ is $B$-balanced, hence we get a left $A$-module homomorphism $A \otimes_B U \to V$. It is bijective as shown above, hence it is an isomorphism. $\square$

*Example* 3.42. (1) Dihedral group: following notations in Example 3.8-(2),

$$G = D_n = \{\, R^k, SR^k \,\}_{k=0}^{n-1} \supset H = C_n = \langle R \rangle.$$

$G/H = \{H, SH\} \Rightarrow s_1 = 1, s_2 = S$. Now we determine $\pi(g) \in S_2$ and $\mu_i(g) \in H$:

$$R(H) = (H), \quad R(SH) = SR^{-1}H = (SH) \quad \implies \quad \pi(R) = (1),$$
$$S(H) = (SH), \quad S(SH) = (H) \quad \implies \quad \pi(S) = (12).$$

Hence $Rs_1 = s_1 R$, $Rs_2 = RS = SR^{-1} = s_2 R^{-1}$ determines $\mu_i(R)$, $Ss_1 = s_2 \cdot 1$, $Ss_2 = s_1 \cdot 1$ determines $\mu_i(S)$. Now let $\sigma : H \to \mathbb{C}^\times$ be the degree 1 representation with $\sigma(R) = w$ where $w^n = 1$. Then we get from Proposition 3.40:

$$\sigma^G(R) \sim \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}, \qquad \sigma^G(S) \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

This recovers the expression given in Example 3.8-(2).

(2) Let $G \supset H$. Consider the trivial case $\sigma = \mathbf{1}_H$ on one-dimensional $U = Fe$. Then $s_i \otimes_B e$, $i \in [1, r]$ is a base of $U^G$. Since $\sigma^G(g)(s_i \otimes e) = s_{\pi(g)i} \otimes e$, we get

$$\chi_{\mathbf{1}_H^G}(g) = \#\,\mathrm{Fix}(\pi(g)) = \#\,\{\, aH \mid gaH = aH \,\}.$$

If $\sigma : H \to F^\times$ is one-dimensional but not necessarily trivial, we call $\sigma^G$ a "monomial representation". It has the property that the matrix for $\sigma^G(g)$ has exactly one non-trivial entry in each column and in each row.

(3) Induction from normal subgroups. The formula for induced characters in Proposition 3.40 shows that $\chi_{\sigma^G}$ vanishes outside the subgroup in $G$ generated by all the conjugates $\bigcup_{g \in G} gHg^{-1}$.

In particular when $H \triangleleft G$, $\chi_{\sigma^G}(g)$ is non-trivial only for $g \in H$. Nevertheless it consists of sum of characters of its various conjugates ${}^s\sigma$ and it is unclear what is $\sigma^G$—$G$ acts non-trivially on the quotient group $G/H$ and the induced action of $G/H$ on $G/H$ is the regular action. For example take $H = \{1\}$ then we get $\rho_{\rm reg}$ and $\chi_{\rm reg}$ on $G$.

More detailed study on Example 3.42-(2) and (3) will be given shortly. Here are some basic properties of the induced modules/representations:

**Theorem 3.43.** *Let $G \supset K$ and $K \supset H$, both being of finite index, and $\sigma : H \to \mathrm{GL}(U)$, $\rho : G \to \mathrm{GL}(V)$ be $F$-representations. Then*

(1) $(\sigma^K)^G \cong \sigma^G$.
(2) *If $W \subset U$ is $\sigma(H)$-invariant then $W^G \subset U^G$ is $\sigma^G(G)$-invariant. If $\sigma = \sigma_1 \oplus \sigma_2$ then $\sigma^G = \sigma_1^G \oplus \sigma_2^G$.*
(3) *(Projection formula) $\sigma^G \otimes \rho \cong (\sigma \otimes \rho_H)^G$.*
(4) $(\sigma^G)^* \cong (\sigma^*)^G$.

PROOF. Let $A = F[G]$, $B = F[K]$ and $C = F[H]$. Then (1) follows from

$$A \otimes_B (B \otimes_C U) \cong (A \otimes_B B) \otimes_C U \cong A \otimes_C U.$$

For (2), recall that $A$ is a free $C$-module, hence

$$0 \to W \to U \quad \Longrightarrow \quad 0 \to A \otimes_C W \to A \otimes_C U.$$

Similarly if $U = \bigoplus W_i$ then $A \otimes_C U = \bigoplus A \otimes_C W_i$.

For (3), again we have a näive $F$-vector space isomorphism

$$f : (A \otimes_C U) \otimes_F V \xrightarrow{\sim} A \otimes_C (U \otimes_F V)$$

defined by $f((a \otimes_C x) \otimes_F y) = a \otimes_C (x \otimes_F y)$. However the $G$-actions are not compatible with $f$. Namely

$$g((a \otimes_C x) \otimes_F y) = (ga \otimes_C x) \otimes_F gy \neq g(a \otimes_C (x \otimes_F y)) = ga \otimes_C (x \otimes_F y).$$

To remedy it, we consider the modified $F$-vector space isomorphism

$$\tilde{f}((a \otimes_C x) \otimes_F y) := (a \otimes_C x) \otimes_F ay.$$

Then it is readily seen that the $G$-actions are compatible with $\tilde{f}$.

The proof of (4) is left to the readers as exercises. □

Now we prove the first main result of induced modules:

**Theorem 3.44** (Frobenius reciprocity)**.** *Let $H \subset G$ with $[G : H] < \infty$. Let $F = \bar{F}$ and $\rho$ (resp. $\sigma$) be irreducible $F$-representations of $G$ (resp. $H$). Assume further that $\sigma^G$ and $\rho_H$ are both completely reducible, e.g.* char $F \nmid |G| < \infty$, *then*

$$\text{multiplicity of } \rho \text{ in } \sigma^G = \text{multiplicity of } \sigma \text{ in } \rho_H.$$

THE PROOF FOR $F = \mathbb{C}$, $|G| < \infty$ USING CHARACTERS.

$$\begin{aligned}(\chi_{\sigma^G}, \chi_\rho)_G &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a,g\in G}\overline{\tilde{\chi}_\sigma(a^{-1}ga)}\chi_\rho(g)\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a,g\in G}\overline{\tilde{\chi}_\sigma(g)}\chi_\rho(aga^{-1})\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a\in G,\, h\in H}\overline{\chi_\sigma(h)}\chi_\rho(aha^{-1})\\ &= \frac{1}{|H|}\sum_{a\in G,\, h\in H}\overline{\chi_\sigma(h)}\chi_\rho(h) = (\chi_\sigma, \chi_{\rho_H})_H.\end{aligned}$$

Notice that $\chi_\rho(aha^{-1}) = \chi_\rho(h)$ is used. □

The general case requires some preparation.

*Definition* 3.45. For $F$-representations $\tau : G \to \mathrm{GL}(W)$ and $\tau' : G \to \mathrm{GL}(W')$ we define the "intertwining number"

$$\iota(\tau, \tau') := \dim_F \hom_A(W, W').$$

For $F = \bar{F}$ Schur's lemma implies that if $\tau$ and $\tau'$ are both irreducible then $\iota(\tau, \tau') = 1$ or $0$ depending on whether $\tau \cong \tau'$ or not. In any case we have the symmetric property $\iota(\tau, \tau') = \iota(\tau', \tau)$. Thus for completely reducible $\tau = \bigoplus \tau_i$ and $\tau' = \bigoplus \tau'_j$ the pairing is symmetric:

$$\iota(\tau, \tau') = \textstyle\sum_{i,j} \iota(\tau_i, \tau'_j) = \sum_{i,j} \iota(\tau'_j, \tau_i) = \iota(\tau', \tau).$$

If $\tau$ is irreducible then $\iota(\tau, \tau')$ is exactly the multiplicity of $\tau'$ in $\tau$.

THE PROOF FOR THE GENERAL CASE. Denote $A = F[G]$, $B = F[H]$, $\rho : G \to \mathrm{GL}(V)$, $\sigma : H \to \mathrm{GL}(U)$. The adjoint property for $\otimes$ and hom implies the following $F$-vector space isomorphism (by viewing $A = {}_A A_B$):

$$\hom_A(A \otimes_B U, V) \xrightarrow{\sim} \hom_B(U, \hom_A(A, V)).$$

Notice that the left $B$-module structure of $\hom_A(A, V)$ is precisely $\rho_H$. The equality on $\dim_F$ then proves the theorem. □

Exercise 3.3. (1) Prove the Frobenius reciprocity formula: for completely reducible $\rho$ for $G$, $\sigma$ for $H$: $\iota(\sigma, \rho_H)_H = \iota(\sigma^G, \rho)_G$. (2) For $H \subset G$, $G$ finite, define Ind and Res for class functions $\phi \in \mathscr{C}(G)$, $\psi \in \mathscr{C}(H)$ and prove

$$(\psi, \operatorname{Res} \phi)_H = (\operatorname{Ind} \psi, \phi)_G.$$

(3) Prove a generalization for any finite group homomorphism $f : H \to G$.

The second main result is a criterion for the irreducibility of an induced representation due to Mackey. We start with the natural question: let $H \subset G$ with $[G : H] < \infty$ and let $\sigma : H \to \mathrm{GL}(U)$ be a given $F$-representation.

$$\text{What is } (\sigma^G)_K \text{ for any } K \subset G?$$

For $g \in G$, we observe that $gU := g \otimes U \subset U^G$ is stabilized by ${}^gH := gHg^{-1}$: indeed $ghg^{-1}(g \otimes x) = a \otimes hx \in gU$. Since $[G : {}^gH] = [G : H] < \infty$, we obtain a ${}^gH$-submodule and hence a $K \cap {}^gH$-submodule for any $K \subset G$:

$$gU \hookrightarrow (U^G)_{{}^gH}, \qquad gU \hookrightarrow (U^G)_{K\cap {}^gH}.$$

**Lemma 3.46.** *$\{k_i g\}$ represents $KgH/H$ if and only $\{k_i\}$ represents $K/K \cap {}^gH$.*

PROOF. $k_1gH = k_2gH \iff k_1g = k_2gh$ for some $h \in H \iff k_2^{-1}k_1 = ghg^{-1}$ $(\in K \cap {}^gH) \iff k_1(K \cap {}^gH) = k_2(K \cap {}^gH)$. □

**Theorem 3.47** (Mackey decomposition)**.** *Let $\Delta = K\backslash G/H$ be the set of all double cosets $D = KgH$ in $G$. Then*

$$(U^G)_K = \bigoplus\nolimits_{D\in\Delta} DU,$$

*where $DU := \sum_{g\in D} gU \cong (gU)_{K\cap {}^gH}{}^K$ for amy $g \in D$.*

PROOF. Let $U^G = \bigoplus_{i=1}^r s_iU$ where $\{s_i\}_{i=1}^r$ represents $G/H$. Then for $m = [KgH : H] = [K : K \cap {}^gH]$,

$$\begin{aligned} g \in G \Longrightarrow D &:= KgH = s_{i_1}H \sqcup \ldots \sqcup s_{i_m}H \quad (s_{i_1} := g) \\ &\Longrightarrow DU = kgHU = s_{i_1}U \oplus \ldots \oplus s_{i_m}U, \end{aligned}$$

where $DU$ is $F[K]$-invariant. This implies $(U^G)_K = \bigoplus_{D\in\Delta} DU$.

Moreover, $gU = s_{i_1}U \subset DU$ as $F[K \cap {}^gH]$-submodule. Lemma 3.46 implies that we may choose $\{s_{i_j} = k_jg\}_{j=1}^m$ with $k_1 = 1$. Proposition 3.41 then implies $DU \cong (gU)_{K\cap {}^gH}{}^K$. The theorem is proved. □

**Theorem 3.48** (Mackey's irreducibility criterion)**.** *Let $F = \bar{F}$,* char $F \nmid |G| < \infty$*, $\sigma : H \to \mathrm{GL}(U)$ for $H \subset G$. Then $\sigma^G$ is irreducible if and only if*

(1) *$\sigma$ is irreducible,*
(2) *for all $g \notin H$, $U$ and $gU$ are disjoint as $F[H \cap {}^gH]$-modules.*

PROOF. By Theorem 3.44 and 3.47, $\sigma^G$ is irreducible if and only if

$$\begin{aligned} 1 = \iota(\sigma^G, \sigma^G) &= \iota(\sigma, {\sigma^G}_H) \\ &= \sum_{D \in H\backslash G/H} \iota(\sigma, {(gU)_{H\cap {}^gH}}^H) \\ &= \sum_{D \in H\backslash G/H} \iota(U_{H\cap {}^gH}, (gU)_{H\cap {}^gH}). \end{aligned}$$

This is equivalent to $\iota(U_H, U_H) \equiv \iota(\sigma, \sigma) = 1$ for $g = 1$, i.e. $\sigma$ is irreducible, and $\iota(U_{H\cap {}^gH}, (gU)_{H\cap {}^gH}) = 0$ for all $g \notin H$. □

We conclude this section by a few important corollaries, notably (4).

**Corollary 3.49.** *Following the notations in Theorem 3.48, then*

(1) *If $\deg \sigma = 1$, then $\sigma^G$ is irreducible if and only if for all $g \notin H$, $\sigma(h) \neq \sigma(ghg^{-1})$ for some $h \in H \cap {}^gH$.*
(2) *Let $H \triangleleft G$. Then $\sigma^G$ is irreducible if and only if $\sigma$ is irreducible and ${}^g\sigma \ncong \sigma$ for all $g \notin H$.*
(3) *Let $H \triangleleft G$ and $T(\sigma) := \{ g \in G \mid {}^g\sigma \cong \sigma \} \supset H$. If $\tau$ is an irreducible representation of $T(\sigma)$ such that $\tau_H$ contains $\sigma$ then $\tau^G$ is irreducible.*
(4) *Let $H \triangleleft G$. If $\rho$ is an irreducible representation of $G$ such that $\sigma$ is an irreducible component of $\rho_H$, then $\rho = \tau^G$ for some irreducible representation $\tau$ of $T(\sigma)$.*

The group $T(\sigma)$ is called the inertia group of $\sigma$.

PROOF. (1) is obvious.

(2) follows from the facts that ${}^gH = H$ and the $H$-action on $gU$ is ${}^g\sigma$.

(3): let $\tau : T := T(\sigma) \to \mathrm{GL}(V)$. Since $H \triangleleft T$, Clifford's theorem (Theorem 3.3) says that all irreducible components of $\tau_H$, i.e. $V$, are conjugated to $\sigma$. Hence they are all isomorphic to $\sigma$ by the definition of $T$.

To show that $V^G$ is irreducible, let $g \notin T$ and consider $V$ and $gV$ as $F[T \cap {}^gT]$-modules. By the above result for $V$, $gV$ is then isomorphic to a sum of copies of $gU$ as $F[H]$-modules. The $H$-action on $gU$ is given ${}^g\sigma$ which is not isomorphic to $\sigma$ since $g \notin T$. Thus $V$ and $gV$ are disjoint as $F[H]$-modules. Since $T \cap {}^gT \supset H$, they are also disjoint as $F[T \cap {}^gT]$-modules. Thus the result follows from Theorem 3.48.

(4) Take an irreducible component $\tau$ of $\rho_T$ such that $\tau_H \supset \sigma$. By (3), $\tau^G$ is irreducible. Hence $\rho = \tau^G$ by Theorem 3.44 (Frobenius reciprocity). □

## 5. Brauer's theorem on induced characters

Throughout this section we assume $F \subset \mathbb{C}$ and $|G| < \infty$.

*Definition* 3.50. (1) A group $G$ is $p$-elementary if $G = Z \times P$ with $Z$ cyclic, $P$ a $p$-group and $p \nmid |Z|$. $G$ is elementary if it is $p$-elementary for some $p$.

(2) $G$ is $p$-quasi-elementary if there is a cyclic $Z \triangleleft G$, with $G/Z$ a $p$-group and $p \nmid |Z|$. Clearly $p$-elementary $\Rightarrow$ $p$-quasi-elementary.

It is clear tat the subgroup $Z$ specified in Definition 3.50 is unique. Also any subgroup of a $p$(-quasi)-elementary group is $p$(-quasi)-elementary.

**Lemma 3.51.** (i) *$G$ is $p$-quasi-elementary $\iff$ $G = AP$ with $A \triangleleft G$ being cyclic and $P$ is a $p$-group.* (ii) *A $p$-quasi-elementary group is $p$-elementary $\iff$ $Z \subset C(G) \iff P \triangleleft G$ where $P$ is given in* (i).

Proof. (i) "$\Rightarrow$": let $P \in \mathrm{Syl}_p(G)$, then $P \cap Z = \{1\} \Rightarrow G = ZP = PZ$.

(i) "$\Leftarrow$": there is a unique decomposition $A = Z \times W$ with $p \nmid |Z|$ and $W$ a $p$-group. Then $Z \triangleleft G$ and $G/Z = WP$ is a $p$-group. $\square$

The main goal of this section is to prove

**Theorem 3.52** (Brauer). *Any complex character of $G$ is an integral combination of monomial characters induced from elementary subgroups of $G$.*

The proof consists of two main steps. To state them we need

*Definition* 3.53. The group of generalized characters is defined as

$$\mathrm{ch}(G) := \bigoplus \mathbb{Z}\chi_i.$$

Also for $\mathscr{F}$ being a family of subgroups of $G$, we define

$$\mathrm{ch}_{\mathscr{F}}(G) := \{\mathbb{Z}\text{-combinations of } \psi^G \text{ where } \psi \in \mathrm{ch}(H), H \in \mathscr{F}\}.$$

Since $\psi^G\chi = (\psi\chi_H)^G$, we see that $\mathrm{ch}_{\mathscr{F}}(G)$ is an ideal of $\mathrm{ch}(G)$.

The first step is reduce to quasi-elementary subgroups:

**Theorem 3.54.** *Let $\mathscr{Q}$ be the family of all quasi-elementary subgroups of $G$, then*

$$\mathrm{ch}(G) = \mathrm{ch}_{\mathscr{Q}}(G).$$

**Lemma 3.55.** *Let $S \neq \emptyset$ be a finite set, $R \subset \mathbb{Z}^S$ be a "subrng".*

*If $R$ is not a subring, i.e. $1_S \notin R$, then there exists $x \in S$ and a prime $p$ such that $p \mid f(x)$ for all $f \in R$.*

PROOF. For $x \in S$, consider $I_x := \{f(x) \mid f \in R\} \subset \mathbb{Z}$ as a subgroup. If for all $x \in S$ we have $I_x = \mathbb{Z}$, say $f_x(x) = 1$, then

$$\prod_{x \in S}(f_x - 1_S) = 0.$$

Since $R$ is a rng, expanding this out we get $1_S \in R$. $\square$

**Lemma 3.56.** *For every $g \in G$ and a prime $p$, there is a $p$-quasi-elementary subgroup $H \subset G$ such that $p \nmid \chi_{\mathbf{1}_H{}^G}(g)$.*

PROOF. Write $\langle g \rangle = Z \times W$, $p \nmid |Z|$, $|W| = p^k$, $k \geq 0$. Let $N = N_G(Z)$, $\overline{H} \in \mathrm{Syl}_p(N/Z)$ which contains $\langle g \rangle / Z$. That is, $\langle g \rangle \subset H \subset N$ and $\overline{H} = H/Z$. This implies that $H$ is a $p$-quasi-elementary subgroup.

From Example 3.42-(2), we have

$$\chi_{\mathbf{1}_H{}^G}(g) = \#\,\mathrm{Fix}(\pi(g)), \qquad \mathrm{Fix}(\pi(g)) = \{aH \mid gaH = aH\}.$$

All these fixed cosets lies in $N$: indeed $a^{-1}ga \in H \Rightarrow a^{-1}Za \subset H$. However, since $H$ is $p$-quasi-elementary, $Z \subset H$ is the only subgroup with order $|Z|$. Hence $a^{-1}Za = Z$ and then $a \in N$.

Consider the action of $\langle g \rangle$ on $N/H$ by left multiplications. Since $Z \triangleleft N$, we get the induced action of $W = \langle g \rangle / Z$ on $N/H$. As $|W| = p^k$, every non-trivial orbit of it has order $p^e$ for some $e \geq 1$. (If $k = 0$ then there are no non-trivial orbits.) This implies

$$\chi_{\mathbf{1}_H{}^G}(g) \equiv [N \colon H] \pmod{p}.$$

By our construction, $H$ contains a Sylow $p$ subgroup of $N$, hnece $p \nmid [N \colon P]$. This implies that $p \nmid \chi_{\mathbf{1}_H{}^G}(g)$. $\square$

PROOF OF THEOREM 3.54. It is enough to show that $\chi_{\mathbf{1}_G} \in \mathrm{ch}_{\mathscr{Q}}(G)$. Let $R \subset \mathrm{ch}_{\mathscr{Q}}(G)$ be the subrng generated by all $\chi_{\mathbf{1}_H{}^G}$ with $H \in \mathscr{Q}$.

Now comes the key point: $R \subset \mathbb{Z}^{|G|}$, instead of just $\mathbb{C}^{|G|}$. If $\chi_{\mathbf{1}_G} \notin \mathrm{ch}_{\mathscr{Q}}(G)$ then $\chi_{\mathbf{1}_G} \notin R$. Lemma3.55 then implies there exists $g \in G$ and a prime $p$ such that $p \mid \chi(g)$ for all $\chi \in R$. But this contradicts to Lemma 3.56 for some $\chi_{\mathbf{1}_H{}^G}$ with $H \in \mathscr{Q}$. The theorem is proved. $\square$

The second step is to reduce to elementary subgroups. We shall need:

**Theorem 3.57** (Blichfeldt–Brauer)**.** *Let $\chi$ be an irreducible character of $p$-quasi-elementary group $G$, then*

(1) $\deg \chi = p^n$ *is a $p$-power.*
(2) $\chi = \lambda^G$ *for a linear character $\lambda$, i.e.* $\deg \lambda = 1$, *of some $H \subseteq G$.*

PROOF. Let $\chi = \chi_\rho$, $G = ZP$, $Z \lhd G$ being cyclic and $p \nmid |Z|$.

(1) Let $\sigma$ be an irreducible component of $\rho_Z$ and let $T = T(\sigma)$ be its inertia group. Corollary 3.49-(4) implies that $\rho = \tau^G$ for an irreducible representation $\tau$ of $T$. Since $[G\colon T] = p^s$ and $T$ is also $p$-quasi-elementary, if $T \neq G$ then (1) follows by induction on $|G|$.

If $T = G$, notice that $Z$ is cyclic (abelian) implies that $\deg\sigma = 1$.Then Clifford's theorem implies that $a \in Z$ acts as scalar multiplication on $V = V_\rho$. Thus $\rho$ is irreducible implies $\rho_P$ is irreducible. Hence $\deg\rho \mid |P|$ which is is a $p$-power.

(2) Let $\deg\chi = p^n$. We prove the result by induction on $n$. The case $n = 0$ is trivial, so let $n \geq 1$.

For any linear character $\lambda$ of $G$, $\chi\lambda = \chi \iff$

$$1 = (\chi, \chi\lambda) = \frac{1}{|G|}\sum\nolimits_{g\in G}\overline{\chi(g)}\chi(g)\lambda(g) = (\chi\overline{\chi}, \lambda).$$

That is, the multiplicity of $\lambda$ in $\rho\otimes\rho^*$ is 1.

Let $\Lambda := \{\,\lambda \mid \deg\lambda = 1,\ \chi\lambda = \chi\,\}$. $\Lambda$ is a group under multiplications. Now we consider the decomposition into irreducible characters:

$$\chi\overline{\chi} = \sum\nolimits_{\lambda\in\Lambda}\lambda + \sum\nolimits_{\deg\chi'\geq 2,\,\text{irred.}}\chi'.$$

By evaluating at $g = 1$, (1) implies that $p \mid |\Lambda|$. Hence there exists $\lambda_1 \in \Lambda \setminus \{\chi_1\}$ with $\lambda_1^p = \chi_1$, i.e. $\lambda_1 : G \to \mathbb{C}^\times$ has its image in $\langle\zeta_p\rangle$. So $G/K \cong \langle\zeta_p\rangle$ for $K := \ker\lambda$. By restricting to $K$ we get

$$\chi_K\overline{\chi}_K = \sum\nolimits_{\lambda\in\Lambda}\lambda_K + \sum\nolimits_{\deg\chi'\geq 2,\,\text{irred.}}\chi'_K$$

while $\lambda_{1K} = \chi_{\mathbf{1}_K}$. So $(\chi_K, \chi_K) = (\chi_K\overline{\chi}_K, \chi_{\mathbf{1}_K}) \geq 2$ and then $\rho_K$ is reducible.

Let $\tau$ be an irreducible component of $\rho_K$. Then $\rho$ is an irreducible component of $\tau^G$ by Frobenius reciprocity. Also $\deg\chi_\tau < \deg\chi$ and both are $p$-powers. Hence $p\deg\chi_\tau \leq \deg\chi$. But we have seen that $[G\colon K] = p$, so $\deg\chi_{\tau^G} = p\deg\chi_\tau$. This implies $\chi = \chi_{\tau^G}$.

Now (2) follows by induction (on $n$) and transitivity of induction (on representations). $\square$

**Lemma 3.58.** *Let $G = ZP$ be a $p$-quasi-elementary decomposition and let $W = C_G(P)\cap Z$. Then $H := WP = W\times P \subset G$ is an elementary subgroup.*

*If $\lambda : G \to \mathbb{C}^\times$ has $\lambda|_H = 1$ then $\lambda = \chi_1$.*

PROOF. It is clear that $P$ is a normal Sylow-$p$ subgroup of $H = WP$, hence $H = W\times P$ is $p$-elementary.

For the second statement, we need only to show that $\lambda|_Z = 1$.

Let $K = Z \cap \ker \lambda$. Since $\lambda$ is a homomorphism, we have $\lambda(b^{-1}dbKd^{-1}) = 1$. That is, $d(bK)d^{-1} = bK$. Take $b \in Z$, $d \in P$, this implies that $P$ acts on $bK$ by conjugation. Since $p \nmid |Z|$, we also have $p \nmid |K| = |bK|$. As $P$ is a $p$-group, this implies that the action of $P$ on $bK$ has a fixed point $bk$. Namely, $bK \cap C_G(P) \neq \emptyset$. Since

$$bK \cap C_G(P) \subset Z \cap C_G(P) = W \subset H,$$

we have $1 = \lambda(bk) = \lambda(b)$. This applies to every $b \in Z$, hence $\lambda|_Z = 1$. $\square$

Now we can complete the second step, and hence Brauer's theorem.

**Theorem 3.59.** *Any character $\chi$ of a p-quasi-elementary group $G$ is a $\mathbb{Z}$-combination of characters induced from linear characters of elementary subgroups of $G$.*

PROOF. We may assume that $\chi$ is irreducible. The proof is by induction on $|G|$. By Theorem 3.57 the proof is reduced to the case that $\deg \chi = 1$ (since subgroups of a quasi-elementary group are quasi-elementary).

Now let $H = WP \subset G$ as in Lemma 3.58. Let $\eta := \chi_H$, which is linear on the elementary subgroup $H$. Then

$$(\chi, \eta^G) = (\chi_H, \eta) = (\eta, \eta) = 1$$

by Frobenius reciprocity (degree 1 is irreducible). We claim that

$$\eta^G = \chi + \theta$$

where $\theta$ is a sum of characters of degree $\geq 2$: let $\chi'$ be any linear component in $\eta^G$, then $(\eta, \chi'_H) = (\eta^G, \chi') \geq 1$. Hence $\chi'_H = \eta$ (both are of degree 1). This applies to $\chi$ too. So for $\chi'' := \chi'\chi^{-1}$, we have $\chi''|_H = 1$. Lemma 3.58 then implies $\chi' = \chi$.

Now by Theorem 3.57 and induction on $|G|$, the theorem holds for $\theta$. Then the theorem also holds for $\chi = \eta^G - \theta$ since $\eta$ is linear on $H$. $\square$

Use reciprocity to prove the following more elementary version:

Exercise 3.4. [Artin's theorem] Let $\mathscr{F}$ be a family of subgroups of $G$. Then $G$ is the union of conjugates of $H \in \mathscr{F} \iff \bigoplus_{H \in \mathscr{F}} \mathrm{ch}(H) \to \mathrm{ch}(G)$ has finite cokernel. What does this say if $\mathscr{F}$ is the family of cyclic subgroups?

A simple consequence of Brauer's theorem is:

Exercise 3.5. Let $m = \exp G$. Show that $\mathbb{Q}(\zeta_m)$ is a splitting field of $G$.