Representations of Finite Groups I
(Math 240A)

(Robert Boltje, UCSC, Winter 2019)
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  Representations and Characters</td>
<td>3</td>
</tr>
<tr>
<td>2  Orthogonality Relations</td>
<td>15</td>
</tr>
<tr>
<td>3  Algebraic Integers</td>
<td>28</td>
</tr>
<tr>
<td>4  Burnside’s $p^a q^b$-Theorem</td>
<td>35</td>
</tr>
<tr>
<td>5  The Group Algebra and its Modules</td>
<td>40</td>
</tr>
<tr>
<td>6  The Tensor Product</td>
<td>51</td>
</tr>
<tr>
<td>7  Induction</td>
<td>59</td>
</tr>
<tr>
<td>8  Frobenius Groups</td>
<td>71</td>
</tr>
<tr>
<td>9  Elementary Clifford Theory</td>
<td>76</td>
</tr>
<tr>
<td>10 Artin’s and Brauer’s Induction Theorems</td>
<td>83</td>
</tr>
</tbody>
</table>
1 Representations and Characters

Throughout this section, \( F \) denotes a field and \( G \) a finite group.

1.1 Definition A (matrix) representation of \( G \) over \( F \) of degree \( n \in \mathbb{N} \) is a group homomorphism \( \Delta: G \to \text{GL}_n(F) \). The representation \( \Delta \) is called faithful if \( \Delta \) is injective. Two representations \( \Delta: G \to \text{GL}_n(F) \) and \( \Gamma: G \to \text{GL}_m(F) \) are called equivalent if \( n = m \) and if there exists an invertible matrix \( S \in \text{GL}_n(F) \) such that \( \Gamma(g) = S\Delta(g)S^{-1} \) for all \( g \in G \). In this case we often write \( \Gamma = S\Delta S^{-1} \) for short.

1.2 Remark In the literature, sometimes a representation of \( G \) over \( F \) is defined as a pair \((V, \rho)\) where \( V \) is a finite-dimensional \( F \)-vector space and \( \rho: G \to \text{Aut}_F(V)(= \text{GL}(V)) \) is a group homomorphism into the group of \( F \)-linear automorphisms of \( V \). These two concepts can be translated into each other. Choosing an \( F \)-basis of \( V \) we obtain a group isomorphism \( \text{Aut}_F(V) \sim \to \text{GL}_n(F) \) (where \( n = \dim_F V \)) and composing \( \rho \) with this isomorphism we obtain a representation \( \Delta: G \to \text{Aut}_F(V) \sim \to \text{GL}_n(F) \). If we choose another basis then we obtain equivalent representations. Conversely, if \( \Delta: G \to \text{GL}_n(F) \) is a representation, we choose any \( n \)-dimensional \( F \)-vector space \( V \) and a basis of \( V \) (for instance \( V = F^n \) with the canonical basis) and obtain a homomorphism \( \rho: G \to \text{GL}_n(F) \sim \to \text{Aut}_F(V) \). Representations \((V, \rho)\) and \((W, \sigma)\) are called equivalent if there exists an \( F \)-linear isomorphism \( \varphi: V \to W \) such that \( \sigma(g) = \varphi \circ \rho(g) \circ \varphi^{-1} \) for all \( g \in G \). The above constructions induce mutually inverse bijections between the set of equivalence classes of representations \((V, \rho)\) and the set of equivalence classes of matrix representations \( \Delta \) of \( G \) over \( F \).

If one takes \( V := F^n \), the space of column vectors together with the standard basis \((e_1, \ldots, e_n)\) then the matrix representation \( \Delta \) corresponds to \((F^n, \rho)\) with \( \rho(g)v = \Delta(g)v \).

1.3 Examples

(a) The trivial representation is the homomorphism \( \Delta: G \to \text{GL}_1(F) \), \( g \mapsto 1 \).

(b) For \( n \geq 2 \) let \( D_{2n} = \langle \sigma, \tau \mid \sigma^n = 1, \tau^2 = 1, \tau \sigma \tau = \sigma^{-1} \rangle \) be the dihedral group of order \( 2n \). We define a faithful representation \( \Delta \) of \( D_{2n} \) over \( \mathbb{R} \) by

\[
\Delta(\sigma) := \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix} \quad \text{and} \quad \Delta(\tau) := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},
\]

where \( \phi \) is a suitable angle. This representation is faithful because \( \Delta \) is injective.
where $\phi = 2\pi/n$. Note that $\Delta(\sigma)$ is the counterclockwise rotation about $2\pi/n$ and $\tau$ is the reflection about the vertical axis in $\mathbb{R}^2$.

(c) The map $\Delta: \text{Sym}(n) \to \text{GL}_n(F)$, which maps $\sigma \in \text{Sym}(n)$ to the permutation matrix of $\sigma$ is a faithful representation of $\text{Sym}(n)$ of degree $n$ over any field. It is called the natural representation of $\text{Sym}(n)$. (The permutation matrix of $\sigma$ has in its $i$-th column the canonical basis vector $e_{\sigma(i)}$, i.e., $\Delta(\sigma)$ maps $e_i$ to $e_{\sigma(i)}$.)

(d) If $\Delta: G \to \text{GL}_n(F)$ is a representation and $H \leq G$ then the restriction of $\Delta$ to $H$,

$$\text{Res}_H^G(\Delta): H \xrightarrow{i} G \xrightarrow{\Delta} \text{GL}_n(F)$$

is a representation of $H$ over $F$ of the same degree. Here, $i: H \to G$ denotes the inclusion map. More generally, if $f: H \to G$ is an arbitrary group homomorphism between two arbitrary finite groups then also

$$\text{Res}_f(\Delta): H \xrightarrow{f} G \xrightarrow{\Delta} \text{GL}_n(F)$$

is a representation of $H$ over $F$ of degree $n$.

(e) If $G = \{g_1, \ldots, g_n\}$ and if we define the homomorphism $f: G \to \text{Sym}(n)$ by $(f(g))(i) = j$, when $gg_i = g_j$, then

$$G \xrightarrow{f} \text{Sym}(n) \xrightarrow{\Delta} \text{GL}_n(F),$$

with $\Delta$ as in (c), is a representation, called the regular representation of $G$. If we rearrange the ordering of the elements $g_1, \ldots, g_n$ we obtain an equivalent representation.

(f) If $\Delta_1: G \to \text{GL}_{n_1}(F)$ and $\Delta_2: G \to \text{GL}_{n_2}(F)$ are representations of $G$ over $F$ then also their direct sum

$$\Delta_1 \oplus \Delta_2: G \to \text{GL}_{n_1+n_2}(F), \quad g \mapsto \begin{pmatrix} \Delta_1(g) & 0 \\ 0 & \Delta_2(g) \end{pmatrix}$$

is a representation of $G$ over $F$. Since

$$\begin{pmatrix} \Delta_2(g) & 0 \\ 0 & \Delta_1(g) \end{pmatrix} = \begin{pmatrix} 0 & I_{n_2} \\ I_{n_1} & 0 \end{pmatrix} \begin{pmatrix} \Delta_1(g) & 0 \\ 0 & \Delta_2(g) \end{pmatrix} \begin{pmatrix} 0 & I_{n_1} \\ I_{n_2} & 0 \end{pmatrix},$$

we see that $\Delta_1 \oplus \Delta_2$ and $\Delta_2 \oplus \Delta_1$ are equivalent.

(g) Let $E/F$ be a Galois extension of degree $n$ with Galois group $G$. Then $G \leq \text{Aut}_F(E)$ and we obtain a representation $(E, i)$ in the sense of Remark 1.2, with $i: G \to \text{Aut}_F(E)$ the inclusion.
1.4 Definition Let $\Delta: G \to \text{GL}_n(F)$ be a representation.

(a) We say that $\Delta$ is decomposable if it is equivalent to $\Delta_1 \oplus \Delta_2$ for some representations $\Delta_1$ and $\Delta_2$ of $G$ over $F$. Otherwise it is called indecomposable.

(b) We say that $\Delta$ is reducible if it is equivalent to a block upper triangular representation, i.e., to a representation of the form

\[
g \mapsto \begin{pmatrix} A(g) & B(g) \\ 0 & C(g) \end{pmatrix}
\]

where $A(g) \in \text{Mat}_{n_1}(F)$, $B(g) \in \text{Mat}_{n_1 \times n_2}(F)$, $C(g) \in \text{Mat}_{n_2}(F)$, and where $n_1, n_2 \in \mathbb{N}$ are independent of $g \in G$. Otherwise, it is called irreducible.

1.5 Remark Let $\Delta: G \to \text{GL}_n(F)$ be a representation.

(a) If $\Delta$ is decomposable then $\Delta$ is also reducible. Thus, if $\Delta$ is irreducible it is also indecomposable.

(b) A subspace $U$ of $F^n$ is called invariant under $\Delta$ (or $\Delta$-stable) if $\Delta(g)u \in U$ for all $g \in G$ and $u \in U$. More generally, if $(V, \rho)$ is a representation corresponding to $\Delta$, a subspace $U$ of $V$ is called invariant under $\Delta$ (or $\Delta$-stable) if $(\rho(g))(u) \in U$ for all $g \in G$ and $u \in U$. Note that $\Delta$ is decomposable if and only if $V$ has a decomposition $V = U \oplus W$ into two non-zero $\Delta$-invariant subspaces $U$ and $V$. And $\Delta$ is reducible if $V$ has a $\Delta$-invariant subspace $U$ with $\{0\} \neq U \neq V$.

In the following remark we recall a few results from linear algebra.

1.6 Remark Let $V$ be a finite-dimensional $\mathbb{C}$-vector space.

(a) A map

\[
(-, -): V \times V \to \mathbb{C}
\]

is called a hermitian scalar product on $V$ if the following holds for all $x, x', y, y' \in V$ and $\lambda \in \mathbb{C}$:

\[
(x + x', y) = (x, y) + (x', y), \quad (x, y + y') = (x, y) + (x, y'),
\]

\[
(\lambda x, y) = \lambda (x, y), \quad (x, \lambda y) = \overline{\lambda} (x, y),
\]

\[
(y, x) = \overline{(x, y)}, \quad (x, x) \in \mathbb{R}_{\geq 0},
\]

\[
(x, x) = 0 \iff x = 0.
\]
(b) Let \((-,-)\) be a hermitian scalar product on \(V\). And let \(f : V \rightarrow V\) be an automorphism of \(V\). Recall that \(f\) is called \textit{unitary} with respect to \((-,-)\) if \((f(x), f(y)) = (x, y)\) for all \(x, y \in V\). The following results hold:

(i) The vector space \(V\) has an \textit{orthonormal basis} with respect to \((-,-)\), i.e., a basis \((v_1, \ldots, v_n)\) such that \((v_i, v_j) = \delta_{i,j}\) for \(i, j \in \{1, \ldots, n\}\).

(ii) An automorphism \(f\) of \(V\) is unitary if and only if the representing matrix \(A\) of \(f\) with respect to an orthonormal basis is unitary (i.e., \(AA^* = 1\), where \(A^* = A^t\)).

(c) The complex vector space \(\mathbb{C}^n\) has the \textit{standard hermitian scalar product} 
\[ (x, y) = x_1 \bar{y}_1 + x_2 \bar{y}_2 + \cdots + x_n \bar{y}_n. \]
The standard basis \((e_1, \ldots, e_n)\) is an orthonormal basis with respect to this product. An automorphism \(f : \mathbb{C}^n \rightarrow \mathbb{C}^n\) is unitary with respect to \((-,-)\) if and only if the unique matrix \(A \in \text{GL}_n(\mathbb{C})\) with the property \(f(x) = Ax\), for all \(x \in \mathbb{C}^n\), is a unitary matrix, since \(A\) is the representing matrix of \(f\) with respect to \((e_1, \ldots, e_n)\).

(d) The unitary \(n \times n\)-matrices form a subgroup \(U(n)\) of \(\text{GL}_n(\mathbb{C})\). Every unitary matrix is diagonalizable, i.e., conjugate to a diagonal matrix. Its eigenvalues are complex numbers of absolute value 1.

1.7 Proposition \textit{Every complex representation} \(\Delta : G \rightarrow \text{GL}_n(\mathbb{C})\) \textit{is equivalent to a unitary representation}, i.e., \textit{to a representation} \(\Gamma : G \rightarrow \text{GL}_n(\mathbb{C})\) \textit{with} \(\Gamma(g) \in U(n)\) \textit{for all} \(g \in G\).

\textbf{Proof} \textit{For} \(x, y \in \mathbb{C}^n\) \textit{define}
\[ \langle x, y \rangle := \sum_{g \in G} (\Delta(g)x, \Delta(g)y), \]
where \((-,-)\) is the standard hermitian scalar product on \(\mathbb{C}^n\). It is easy to check that \(\langle -, - \rangle\) is again a hermitian scalar product on \(\mathbb{C}^n\) and we have
\[ \langle \Delta(g)x, \Delta(g)y \rangle = \sum_{h \in G} (\Delta(h)\Delta(g)x, \Delta(h)\Delta(g)y) = \sum_{k \in G} (\Delta(k)x, \Delta(k)y) = \langle x, y \rangle, \]
for all \(x, y \in \mathbb{C}^n\) and \(g \in G\). Thus, \(\Delta(g)\) is unitary with respect to \((-,-)\), for every \(g \in G\). Let \(S \in \text{GL}_n(\mathbb{C})\) be a matrix such that its columns \((v_1, \ldots, v_n)\) form an orthonormal basis of \(\mathbb{C}^n\) with respect to \((-,-)\). Then the representing matrix \(S^{-1}\Delta(g)S\) of \(\Delta(g)\) with respect to \((v_1, \ldots, v_n)\) is unitary. Thus, the representation \(\Gamma = S^{-1}\Delta S\) is unitary. \(\square\)

6
1.8 Corollary Let $\Delta : G \to \text{GL}_n(\mathbb{C})$ be a representation and let $g \in G$ be an element of order $k$. Furthermore, set $\zeta := e^{2\pi i/k} \in \mathbb{C}$, a primitive $k$-th root of unity. Then there exists $S \in \text{GL}_n(\mathbb{C})$ (which can depend on $g$) such that

$$S\Delta(g)S^{-1} = \text{diag}(\zeta^{i_1}, \ldots, \zeta^{i_n}) = \begin{pmatrix} \zeta^{i_1} & & \\ & \ddots & \\ & & \zeta^{i_n} \end{pmatrix},$$

the diagonal matrix with diagonal entries $\zeta^{i_1}, \ldots, \zeta^{i_n}$, where the exponents $i_1, \ldots, i_n$ are elements in $\{0, 1, \ldots, k-1\}$.

Proof By Proposition 1.7, the matrix $\Delta(g)$ is conjugate to a unitary matrix. Moreover, by Remark 1.6(d), every unitary matrix is conjugate to a diagonal matrix. Thus, there exists $S \in \text{GL}_n(\mathbb{C})$ such that $S\Delta(g)S^{-1}$ is a diagonal matrix, say with diagonal entries $d_1, \ldots, d_n$. Finally, since $g^k = 1$, we have $(S\Delta(g)S^{-1})^k = S\Delta(g)^kS^{-1} = S\Delta(g^k)S^{-1} = I_n$. This implies that the entries $d_i$ must satisfy $d_i^k = 1$ for $i = 1, \ldots, n$. Now the statement of the corollary follows immediately. 

Note that the previous corollary only says that each matrix $\Delta(g), g \in G$, is individually diagonalizable. This does not mean that $\Delta$ as a representation is diagonalizable, i.e., $\Delta$ is equivalent to a representation with diagonal matrices as values. Clearly, $\Delta$ as a representation is diagonalizable if and only if it is equivalent to a direct sum of representations of degree 1.

1.9 Theorem Assume that $|G| = |G| \cdot 1_F$ is invertible in $F$. Let $\Delta : G \to \text{GL}_n(F)$ be a representation and let $U \subseteq F^n$ be an $F$-subspace that is $\Delta$-invariant. Then there exists a $\Delta$-invariant $F$-subspace $V \subseteq F^n$ such that $F^n = U \oplus V$.

Proof Let $u_1, \ldots, u_r$ be an $F$-basis of $U$ and extend it to an $F$-basis $u_1, \ldots, u_n$ of $F^n$. Let $A \in \text{Mat}_n(F)$ be defined by $Au_i = u_i$ for $i = 1, \ldots, r$ and $Au_i = 0$ for $i = r + 1, \ldots, n$. We set

$$A' := \frac{1}{|G|} \sum_{g \in G} \Delta(g^{-1})A\Delta(g).$$

Then we have

(i) $A'u = u$ for all $u \in U$. 

7
(ii) $A'x \in U$ for all $x \in F^n$.

(iii) $A'A'x = A'x$ for all $x \in F^n$.

(iv) $A'\Delta(h) = \Delta(h)A'$ for all $h \in G$.

In fact, to see (i), note that

$$A'u = \frac{1}{|G|} \sum_{g \in G} \Delta(g^{-1})A\Delta(g)u = \frac{1}{|G|} \sum_{g \in G} \Delta(g^{-1})\Delta(g)u = \frac{1}{|G|} \sum_{g \in G} u = u,$$

since $\Delta(g)u \in U$ for all $g \in G$ and $u \in U$. To see (ii), note that $A\Delta(g)x \in U$ for all $x \in F^n$. Now (iii) follows immediately from (i) and (ii). And (iv) follows from the computation

$$A'\Delta(h) = \frac{1}{|G|} \sum_{g \in G} \Delta(g^{-1})A\Delta(gh) = \frac{1}{|G|} \sum_{\tilde{g} \in G} \Delta(h\tilde{g}^{-1})A\Delta(\tilde{g}) = \Delta(h)A',$$

where we made the substitution $\tilde{g} = gh$.

Now set $V := \ker A'$. We first show that $V$ is $\Delta$-invariant. For $v \in V$ and $g \in G$ we obtain from (iv) that $A'\Delta(g)v = \Delta(g)A'v = 0$, which means that $\Delta(g)v \in \ker A' = V$. Next we show that $F^n = U + V$. In fact, let $x \in F^n$. Then using (ii) and (iii) we obtain $x = A'x + (x - A'x) \in U + V$. Finally, we show that $U \cap V = \{0\}$. So let $x \in U \cap V$. Then $0 = A'x = x$ by (i). This completes the proof.

### 1.10 Corollary

Assume that $|G|$ is invertible in $F$ and let $\Delta : G \to \text{GL}_n(F)$ be a representation. Then one has:

(a) The representation $\Delta$ is equivalent to a direct sum of irreducible representations.

(b) The representation $\Delta$ is indecomposable if and only if it is irreducible.

**Proof** (a) We prove this by induction on $n$. If $n = 1$, the statement holds, since every representation of degree 1 is irreducible by definition. Assume now that $n > 1$. If $\Delta$ is irreducible then we are done. So assume that $\Delta$ is not irreducible. Then there exists a $\Delta$-invariant $F$-subspace $\{0\} \neq U \neq F^n$. By Theorem 1.9, there exists a $\Delta$-invariant $F$-subspace $V$ of $F^n$ such that $F^n = U \oplus V$. Therefore, $\Delta$ is equivalent to $\Delta_1 \oplus \Delta_2$ for representations of degree $n_1, n_2 < n$. By induction the claim follows.

(b) If $\Delta$ is irreducible then it is also indecomposable for trivial reasons. Now assume that $\Delta$ is not irreducible. Then there exists a $\Delta$-invariant subspace $\{0\} \neq U \neq F^n$. By Theorem 1.9, $U$ has a $\Delta$-stable complement $V$ in $F^n$. This implies that $\Delta$ is not indecomposable. \qed
We recall the following theorem from Linear Algebra without proof.

1.11 Theorem Let $A_1, \ldots, A_k \in \text{Mat}_n(F)$. Then the following are equivalent:

(i) The matrices $A_1, \ldots, A_k$ are simultaneously diagonalizable over $F$, i.e., there exists $S \in \text{GL}_n(F)$ such $SA_iS^{-1}$ is a diagonal matrix, for all $i = 1, \ldots, k$.

(ii) The matrices $A_1, \ldots, A_k$ are individually diagonalizable over $F$ and they commute, i.e., $A_iA_j = A_jA_i$ for all $i, j \in \{1, \ldots, k\}$.

1.12 Corollary (a) Let $\Delta: G \to \text{GL}_n(\mathbb{C})$ be a representation satisfying $\Delta(g)\Delta(h) = \Delta(h)\Delta(g)$ for all $g, h \in G$. Then $\Delta$ is equivalent to a direct sum of representations of degree 1.

(b) Assume that $G$ is abelian. Then every representation $\Delta: G \to \text{GL}_n(\mathbb{C})$ is equivalent to a direct sum of representations of degree 1. In particular, every irreducible representation of $G$ has degree 1. In other words, the irreducible representations of $G$ are just the homomorphisms from $G$ to the multiplicative group $\mathbb{C}^\times$ of $\mathbb{C}$.

1.13 Definition Let $\Delta: G \to \text{GL}_n(F)$ be a representation. The character of $\Delta$ is defined as the function

$$
\chi := \chi_\Delta: G \xrightarrow{\Delta} \text{GL}_n(F) \xrightarrow{\text{tr}} F.
$$

The characters of representations of $G$ over $F$ are called the $F$-characters of $G$. If $F = \mathbb{C}$, we just call them characters, or sometimes complex characters of $G$. If $F = \mathbb{C}$ and $\Delta$ is irreducible then $\chi$ is called a (complex) irreducible character.

In the following remark we derive a few first properties of characters.

1.14 Remark Assume that $\Delta: G \to \text{GL}_n(F)$ is a representation and let $\chi = \chi_\Delta: G \to F$ denote its character.

(a) Recall that for two matrices $A, B \in \text{Mat}_n(F)$ one has $\text{tr}(AB) = \text{tr}(BA)$. In particular, if $S \in \text{GL}_n(F)$ one obtains $\text{tr}(SAS^{-1}) = \text{tr}(AS^{-1}S) = \text{tr}(A)$. This implies that if $\Delta$ and $\Gamma$ are equivalent representations then $\chi_\Delta = \chi_\Gamma$. Moreover, by the same property of the trace map we obtain, for any elements $g, x \in G$, that

$$
\chi(xgx^{-1}) = \text{tr}(\Delta(xgx^{-1}) = \text{tr}(\Delta(x)\Delta(g)\Delta(x)^{-1}) = \text{tr}(\Delta(g)) = \chi(g).
$$
This means that the function $\chi: G \to F$ is constant on conjugacy classes of $G$. Any such function is called a class function or a central function on $G$. The class functions $f: G \to F$ form an $F$-vector space $\text{CF}(G, F)$ with the usual addition and scalar multiplication. The dimension of $\text{CF}(G, F)$ is equal to the number $k(G)$ of conjugacy classes of $G$. In fact, the characteristic class functions which have value one on one particular conjugacy class and value zero on all others form an $F$-basis of $\text{CF}(G, F)$.

(b) Let $\Delta_1: G \to GL_{n_1}(F)$ and $\Delta_2: G \to GL_{n_2}(F)$ be two representations. Then, for every $g \in G$, we have

$$\chi_{\Delta_1 \oplus \Delta_2}(g) = \text{tr} \left( \begin{array}{cc}
\Delta_1(g) & 0 \\
0 & \Delta_2(g)
\end{array} \right) = \text{tr}(\Delta_1(g)) + \text{tr}(\Delta_2(g)) = \chi_{\Delta_1}(g) + \chi_{\Delta_2}(g).$$

Thus, $\chi_{\Delta_1 \oplus \Delta_2} = \chi_{\Delta_1} + \chi_{\Delta_2}$ in the vector space $\text{CF}(G, F)$.

(c) The $F$-characters and representations of degree 1 are precisely the group homomorphisms in $\text{Hom}(G, F^\times)$. They form an abelian group under the product defined by $(\phi \cdot \psi)(g) = \phi(g) \psi(g)$, for $\phi, \psi \in \text{Hom}(G, F^\times)$ and $g \in G$. Recall that we have an isomorphism of abelian groups

$$\text{Hom}(G/G', F^\times) \to \text{Hom}(G, F^\times), \ f \mapsto f \circ \nu,$$

where $G'$ denotes the commutator subgroup of $G$, generated by all commutators $[x, y] := xyx^{-1}y^{-1}$, $x, y \in G$, and where $\nu: G \to G/G'$, $g \mapsto gG'$, denotes the natural epimorphism.

(d) Assume from now on that $F \subseteq \mathbb{C}$. Note that

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

Thus, the character of $\Delta$ 'knows' the degree of the representation $\Delta$. We call $\chi(1)$ the degree of the character $\chi$.

Let $g \in G$ and assume that $g^k = 1$. Then, by Corollary 1.8 we have

$$\Delta(g) = S \begin{pmatrix}
\zeta^{i_1} & & \\
& \ddots & \\
& & \zeta^{i_n}
\end{pmatrix} S^{-1},$$

for some $S \in \text{GL}_n(\mathbb{C})$, with $\zeta := e^{2\pi i/k}$ and $i_1, \ldots, i_n \in \mathbb{Z}$. Therefore,

$$\chi(g) = \zeta^{i_1} + \cdots + \zeta^{i_n} \in F \cap \mathbb{Z}[\zeta] \subset F \cap \mathbb{Q}(\zeta).$$
The triangle inequality implies that
\[ |\chi(g)| \leq \sum_{j=1}^{n} |\zeta^{ij}| = n \]
with equality if and only if \( \zeta^{i1} = \cdots = \zeta^{in} \). Thus, we have
\[ |\chi(g)| = \chi(1) \iff \Delta(g) \text{ is a scalar matrix.} \]
The set of elements \( g \in G \) with \( |\chi(g)| = \chi(1) \) is called the center of the character \( \chi \) and is denoted by \( Z(\chi) \). In particular, we obtain
\[ \chi(g) = \chi(1) \iff \Delta(g) = I_n \iff g \in \ker(\Delta). \]
Thus, the character \( \chi \) ‘knows’ the kernel of \( \Delta \). The set of elements \( g \in G \) with \( \chi(g) = \chi(1) \) is called the kernel of \( \chi \) and is denoted by \( \ker(\chi) \).

Finally, we will show that
\[ \chi(g^{-1}) = \overline{\chi(g)}. \]
In fact, from above we have
\[ \Delta(g^{-1}) = \Delta(g)^{-1} = S \begin{pmatrix} \zeta^{i1} & & \\ & \ddots & \\ & & \zeta^{in} \end{pmatrix}^{-1} S^{-1} = S \begin{pmatrix} \zeta^{-i1} & & \\ & \ddots & \\ & & \zeta^{-in} \end{pmatrix} S^{-1}. \]
Taking the trace yields
\[ \chi(g^{-1}) = \zeta^{-i1} + \cdots + \zeta^{-in} = \overline{\zeta^{i1}} + \cdots + \overline{\zeta^{in}} = \overline{\chi(g)}. \]

1.15 Examples

(a) The character of the trivial representation is the constant function \( G \to \mathbb{C} \) with value 1. It is called the trivial character and it is often denoted by \( \chi_G \) or just \( 1 \). More generally, any group homomorphism \( \varphi : G \to \mathbb{C}^\times = \text{GL}_1(\mathbb{C}) \) is a representation of degree 1 and at the same time a character of \( G \).

(b) For the regular character \( \rho_G \), the character of the regular representation (cf. Example 1.3(e)), we find that \( \rho_G(1) = |G| \) and \( \rho_G(g) = 0 \) for all \( g \in G \) with \( g \neq 1 \). In fact, in the latter case one has for all elements
$g_i \in G$ that $gg_i \neq g_i$. This means that all the diagonal entries in the regular representation of $g$ are equal to 0.

(c) Let $G = \text{Sym}(3)$. Since we have an isomorphism

\[
\text{Hom}(G, \mathbb{C}^\times) \cong \text{Hom}(G/G', \mathbb{C}^\times) = \text{Hom}(G/\langle(1,2,3)\rangle, \mathbb{C}^\times),
\]

see Remark 1.14, the group $G$ has exactly two representations of degree 1, namely, the trivial representation and the sign representation $\varepsilon: G \to \{\pm 1\} \leq \mathbb{C}^\times$. Moreover, from Example 1.3(b), since $\text{Sym}(3) \cong D_6$, we have a representation of degree 2 with the property that

\[
(1,2,3) \mapsto \begin{pmatrix}
\cos 120^\circ & -\sin 120^\circ \\
\sin 120^\circ & \cos 120^\circ
\end{pmatrix} = \begin{pmatrix}
-\frac{1}{2} & -\frac{\sqrt{3}}{2} \\
\frac{\sqrt{3}}{2} & -\frac{1}{2}
\end{pmatrix},
\]

\[
(1,2) \mapsto \begin{pmatrix}
-1 & 0 \\
0 & 1
\end{pmatrix}.
\]

Its character $\chi$ is given by $\chi(1) = 2$, $\chi(1,2,3) = -1$, $\chi(1,2) = 0$. Since every other element in $G$ is conjugate to $(1,2,3)$ or $(1,2)$, these three values determine $\chi$. We arrange these values in a table:

<table>
<thead>
<tr>
<th>$g_i$</th>
<th>(1)</th>
<th>(1,2)</th>
<th>(1,2,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\varepsilon$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi$</td>
<td>2</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>

Since $\chi \neq 1 + 1$, $\chi \neq \varepsilon + \varepsilon$, and $\chi \neq 1 + \varepsilon$, we obtain that every representation whose character is equal to $\chi$ is an irreducible representation. Here we used Corollary 1.10 and the property in Remark 1.14(b). In particular, $\chi$ is an irreducible character. We will see in Section 2 that there are no other irreducible characters for $\text{Sym}(3)$.

(d) Let $G = \langle g \rangle$ be a cyclic group of order $k$ and let $\zeta := e^{2\pi i/k}$. Then every homomorphism in $\text{Hom}(G, \mathbb{C}^\times)$ is uniquely determined by its value on $g$ and the possible values are the $k$-th roots of unity, namely $1, \zeta, \zeta^2, \ldots, \zeta^{k-1}$. Thus we obtain $k$ characters of degree 1 which we arrange in the following
table.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>g</th>
<th>g²</th>
<th>...</th>
<th>gᵢ</th>
<th>...</th>
<th>gᵏ⁻¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>...</td>
<td>1</td>
<td>...</td>
<td>1</td>
</tr>
<tr>
<td>ϕ</td>
<td>1</td>
<td>ζ</td>
<td>ζ²</td>
<td>...</td>
<td>ζᵢ</td>
<td>...</td>
<td>ζᵏ⁻¹</td>
</tr>
<tr>
<td>ϕ²</td>
<td>1</td>
<td>ζ²</td>
<td>ζ⁴</td>
<td>...</td>
<td>ζ²ᵢ</td>
<td>...</td>
<td>ζ²(k⁻¹)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td>...</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>ϕⁱ</td>
<td>1</td>
<td>ζⁱ</td>
<td>ζ²ⁱ</td>
<td>...</td>
<td>ζⁱᵢ</td>
<td>...</td>
<td>ζⁱ(k⁻¹)</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td></td>
<td>...</td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>ϕᵏ⁻¹</td>
<td>1</td>
<td>ζᵏ⁻¹</td>
<td>ζᵏ⁻²</td>
<td>...</td>
<td>ζᵏ⁻ʲ</td>
<td>...</td>
<td>ζ</td>
</tr>
</tbody>
</table>

Note note that \( \text{Hom}(G, \mathbb{C}^*) \) is again a cyclic group of order \( k \), generated by the character \( ϕ \).

Exercises

1. Let \( D_{2n} = \langle x, y \mid x^n = y^2 = 1, xy = yx^{-1} \rangle \) be the dihedral group of order \( 2n \).
   (a) Show that \( \Delta_1: D_{2n} \to \text{GL}_2(\mathbb{C}) \), \( x \mapsto \begin{pmatrix} ζ_n & 0 \\ 0 & ζ_n \end{pmatrix} \), \( y \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \),

with \( ζ_n := e^{2πi/n} \) defines a representation.

   (b) Decide if the representation \( \Delta_1 \) is equivalent to the representation

   \( \Delta_2: D_{2n} \to \text{GL}_2(\mathbb{C}) \), \( x \mapsto \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \), \( y \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \).

2. Let \( G = \langle g \rangle \) be a cyclic group of order 3.
   (a) Show that

   \( \Delta: G \to \text{GL}_2(\mathbb{Q}) \), \( g \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \),

defines a representation.

   (b) Show that \( \Delta \) is irreducible over \( \mathbb{Q} \).

   (c) Show that \( \Delta \) is decomposable over \( \mathbb{C} \).

3. Let \( \Delta: G \to \text{GL}_n(\mathbb{C}) \) be a representation and let \( χ \) be its character. The center of \( \Delta \) is defined as

   \( Z(\Delta) := \{ g \in G \mid \Delta(g) = α \cdot 1_n \text{ for some } α \in \mathbb{C} \} \),
and the center of $\chi$ is defined as

$$Z(\chi) := \{ g \in G \mid |\chi(g)| = n \}$$

(a) Show that $Z(\chi) = Z(\Delta)$.
(b) Show that $Z(\chi)$ is a normal subgroup of $G$.

4. Let $G = \langle g \rangle$ be a cyclic group of prime order $p$ and let $F := \mathbb{Z}/p\mathbb{Z}$.
(a) Show that there exists a unique representation $\Delta : G \rightarrow \text{GL}_2(F)$ with

$$\Delta(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$ 

(b) Show that the representation $\Delta$ is indecomposable but not irreducible.

5. (a) Let $G$ be a cyclic group of order 2. Try to explicitly decompose the regular representation of $G$ over $\mathbb{C}$ into a direct sum of irreducible representations, i.e., find an equivalent representation which is a direct sum of irreducible representations.
(b) Do the same as in (a) for a cyclic group of order 3.

6. Let $E/F$ be a Galois extension of degree 2 and set $G := \text{Gal}(E/F)$. Consider the representation $(E, \rho)$ where $E$ is considered as $F$-vector space, and $G$ as a subgroup of $\text{Aut}_F(E)$, cf. Remark 1.2 and Example 1.3(g). Show that any matrix representation associated to this representation is equivalent to the regular representation of $G$.
(This statement remains true for any Galois extension. It follows from the ‘normal basis theorem’ which states that there exists an element $x \in E$ such that $\{ \sigma(x) \mid \sigma \in G \}$ is an $F$-basis of $E$.)

7. Prove the statements in Remark 1.2.
2 Orthogonality Relations

Throughout this section, $G$ denotes a finite group. If there is no base field specified, representations are considered to be complex representations.

2.1 Lemma (Schur) Let $\Delta_1: G \to \text{GL}_m(\mathbb{C})$ and $\Delta_2: G \to \text{GL}_n(\mathbb{C})$ be irreducible representations and let $A \in \text{Mat}_{m \times n}(\mathbb{C})$ be an intertwining matrix, i.e., a matrix satisfying

$$\Delta_1(g)A = A\Delta_2(g) \quad \text{for all } g \in G. \quad (2.1.a)$$

(a) If $\Delta_1$ and $\Delta_2$ are not equivalent then $A = 0$.

(b) If $\Delta_1 = \Delta_2$ then $A$ is a scalar matrix, i.e., there exists $\lambda \in \mathbb{C}$ such that $A = \lambda \cdot I_n$.

Proof (a) Assume that $A \neq 0$. From this we will derive a contradiction. Let $U := \ker(A) \subseteq \mathbb{C}^n$. Then $U$ is a $\Delta_2$-invariant subspace. In fact, for $u \in U$ and $g \in G$ we have $\Delta_2(g)u \in U$, since $A\Delta_1(g)u = \Delta_1(g)Au = 0$. Since $A \neq 0$, we have $U \neq \mathbb{C}^n$. Since $\Delta_2$ is irreducible, this implies $U = \{0\}$. Thus, the linear map $\mathbb{C}^n \to \mathbb{C}^m$, $x \mapsto Ax$ is injective. Next consider $V := \text{im}(A) \subseteq \mathbb{C}^m$. This is a $\Delta_1$-invariant subspace. In fact, let $v \in V$ and $g \in G$. We need to show that $\Delta_1(g)v \in V$. Since $v \in V$, there exists $x \in \mathbb{C}^n$ with $Ax = v$. Therefore, $\Delta_1(g)v = \Delta_1(g)Ax = A\Delta_2(g)x \in V$. Since $A \neq 0$, we have $V \neq \{0\}$. Since $\Delta_1$ is irreducible, we obtain $V = \mathbb{C}^m$. Therefore, the linear map $\mathbb{C}^n \to \mathbb{C}^m$, $x \mapsto Ax$, is also surjective, and consequently an isomorphism. Thus, $m = n$ and $A \in \text{GL}_n(\mathbb{C})$. Now Equation (2.1.a) implies $\Delta_1(g) = A\Delta_2(g)A^{-1}$ for all $g \in G$. Thus, $\Delta_1$ and $\Delta_2$ are equivalent. This is a contradiction.

(b) Set $\Delta := \Delta_1 = \Delta_2$. Let $\lambda \in \mathbb{C}$ be an eigenvalue of $A$ and set $A' := A - \lambda I_n$. Then also $A'$ is an intertwining operator, i.e., it satisfies $\Delta(g)A' = A'\Delta(g)$ for all $g \in G$. Since there exists a non-zero eigenvector for $\lambda$, we obtain $U' := \ker(A') \neq \{0\}$. As in the proof of Part (a) we can see that $U'$ is a $\Delta$-invariant subspace of $\mathbb{C}^n$. Since $\Delta$ is irreducible, we obtain $U' = \mathbb{C}^n$. But this means $A' = 0$ and $A = \lambda \cdot I_n$.

We derive a sequence of three corollaries from the above lemma, the last of them showing that the number of irreducible representations of $G$ is finite and that the sum of the squares of their degrees is bounded by $|G|$.
2.2 Corollary Let $\Delta_1 : G \to \text{GL}_m(\mathbb{C})$ and $\Delta_2 : G \to \text{GL}_n(\mathbb{C})$ be irreducible representations and let $A \in \text{Mat}_{m \times n}(\mathbb{C})$. Set

$$A' := \frac{1}{|G|} \sum_{g \in G} \Delta_1(g) A \Delta_2(g^{-1}) \in \text{Mat}_{m \times n}(\mathbb{C}).$$

(a) If $\Delta_1$ and $\Delta_2$ are not equivalent then $A' = 0$.

(b) If $m = n$ and $\Delta_1 = \Delta_2$ then $A' = \frac{\text{tr}(A)}{n} \cdot I_n$.

Proof We first show that $A'$ satisfies Equation (2.1.a). Let $h \in G$. Then

$$\Delta_1(h) A' = \frac{1}{|G|} \sum_{g \in G} \Delta_1(hg) A \Delta_2(g^{-1}) = \frac{1}{|G|} \sum_{\tilde{g} \in G} \Delta_1(\tilde{g}) A \Delta_2(\tilde{g}^{-1} h) = A' \Delta_2(h).$$

Here we made the substitution $\tilde{g} = hg$.

(a) This follows immediately from Lemma 2.1(a).

(b) Set $\Delta := \Delta_1 = \Delta_2$. By Lemma 2.1(b), there exists $\lambda \in \mathbb{C}$ such that $A' = \lambda \cdot I_n$. Taking traces, we obtain

$$n \lambda = \text{tr}(\lambda \cdot I_n) = \frac{1}{|G|} \sum_{g \in G} \text{tr}(\Delta(g) A \Delta(g^{-1})) = \text{tr}(A'),$$

and the desired equation holds. $\square$

2.3 Corollary Let $\Delta_1 : G \to \text{GL}_m(\mathbb{C})$ and $\Delta_2 : G \to \text{GL}_n(\mathbb{C})$ be irreducible unitary representations and write

$$\Delta_1(g) = \left( r_{ij}(g) \right)_{1 \leq i, j \leq m} \quad \text{and} \quad \Delta_2(g) = \left( s_{kl}(g) \right)_{1 \leq k, l \leq n}$$

for $g \in G$.

(a) If $\Delta_1$ and $\Delta_2$ are not equivalent then

$$\frac{1}{|G|} \sum_{g \in G} r_{ij}(g) s_{kl}(g) = 0$$

for all $1 \leq i, j \leq m$ and $1 \leq k, l \leq n$.  

16
(b) If $m = n$ and $\Delta_1 = \Delta_2$ then
\[
\frac{1}{|G|} \sum_{g \in G} r_{ij}(g) s_{kl}(g) = \begin{cases} 
\frac{1}{n} & \text{if } (i, j) = (k, l), \\
0 & \text{if } (i, j) \neq (k, l),
\end{cases}
\]
for all $i, j, k, l \in \{1, \ldots, n\}$.

**Proof** Let $A := (a_{uv}) \in \text{Mat}_{m \times n}(\mathbb{C})$ be arbitrary and let $A' = (a'_{ik}) \in \text{Mat}_{m \times n}(\mathbb{C})$ be defined as in Corollary 2.2. Then, since $s_{vk}(g^{-1}) = s_{kv}(g)$, the $(i, k)$-entry of $A'$ is given by
\[
a'_{ik} = \frac{1}{|G|} \sum_{u=1}^{m} \sum_{v=1}^{n} \sum_{g \in G} r_{iu}(g) a_{uv} s_{kv}(g).
\]

(a) By Corollary 2.2(a), we have $a'_{ik} = 0$ for every choice of $A$ and for every choice of $1 \leq i \leq m$ and $1 \leq k \leq n$. We choose $A = E_{jl}$, the matrix all of whose entries are 0, except for the $(j, l)$-entry which is equal to 1. This gives the desired equation.

(b) By Corollary 2.2(b), we obtain
\[
a'_{ik} = \begin{cases} 
\frac{\text{tr}(A)}{n} & \text{if } i = k, \\
0 & \text{if } i \neq k.
\end{cases}
\]

Now Choose $A = E_{jl}$ and the result follows.

\[\square\]

**2.4 Corollary** Let $G$ be a group. The number of equivalence classes of irreducible representations of $G$ is finite. If $\Delta_i : G \to \text{GL}_{n_i}(\mathbb{C})$, $i = 1, \ldots, k$, are representatives of these equivalence classes then one has $\sum_{i=1}^{k} n_i^2 \leq |G|$.

**Proof** Let $\Delta_t : G \to \text{GL}_{n_t}(\mathbb{C})$, $t \in T$, be a set of representatives of the equivalence classes of irreducible representations of $G$. We may choose them to be unitary representations by Proposition 1.7. Write $\Delta_t(g) = (r_{ij}^t(g)) \in \text{GL}_{n_t}(\mathbb{C})$ for every $t \in T$ and $g \in G$. We consider triples $(t, i, j)$ with $t \in T$ and $i, j \in \{1, \ldots, n_t\}$. For each such triple we consider the vector $(r_{ij}^t(g)) \in \mathbb{C}^{|G|}$. By Corollary 2.3, these vectors are non-zero and pairwise orthogonal in $\mathbb{C}^{|G|}$, and therefore the set of these vectors is linearly independent. Thus, the number of triples $(t, i, j)$, namely $\sum_{t \in T} n_t^2$, is bounded by $|G|$. This implies that $T$ is finite and the result follows. \[\square\]
2.5 Definition On the \(\mathbb{C}\)-vector space \(\text{CF}(G, \mathbb{C})\) of class functions from \(G\) to \(\mathbb{C}\) we introduce the Schur inner product

\[
(f_1, f_2) := \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}.
\]

It is a straightforward verification that \((-,-)\) is a hermitian scalar product on \(\text{CF}(G, \mathbb{C})\). For characters \(\chi_1, \chi_2\) of \(G\) we also have

\[
(\chi_1, \chi_2) = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \chi_2(g^{-1}),
\]

since \(\chi_2(g) = \chi_2(g^{-1})\) as observed in Remark 1.14(d). This implies

\[
(\chi_1, \chi_2) = (\chi_2, \chi_1),
\]

i.e., the Schur inner product is symmetric on characters.

2.6 Notation From now on, for the rest of the section, we fix the following notation. We choose unitary representatives \(\Delta_1, \ldots, \Delta_k\) of the equivalence classes of irreducible representations of \(G\). We write \(n_1, \ldots, n_k\) for their respective degrees and we denote by \(\chi_1, \ldots, \chi_k\) their respective characters. Then \(\chi_i(1) = n_i\) for \(i = 1, \ldots, k\) and \(\sum_{i=1}^k n_i^2 \leq |G|\) by Corollary 2.4. We denote by \(\text{Irr}(G)\) the set of irreducible characters of \(G\); thus, \(\text{Irr}(G) = \{\chi_1, \ldots, \chi_k\}\). Finally, for \(t \in \{1, \ldots, k\}\) and \(g \in G\), we write

\[
\Delta_t(g) = (r_{ij}^t(g))_{1 \leq i,j \leq n_t}.
\]

2.7 Theorem (First orthogonality relation) The irreducible characters \(\chi_1, \ldots, \chi_k\) form a set of orthonormal vectors in \(\text{CF}(G, \mathbb{C})\) with respect to the Schur inner product. In other words,

\[
(\chi_i, \chi_j) = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_j(g^{-1}) = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j \end{cases}
\]

Proof From Corollary 2.3 we obtain, for \(s,t \in \{1, \ldots, k\}\),

\[
(\chi_s, \chi_t) = \frac{1}{|G|} \sum_{g \in G} \left( \sum_{i=1}^{n_s} r_{ii}^s(g) \right) \left( \sum_{k=1}^{n_t} r_{kk}^t(g) \right)
\]

\[
= \sum_{i=1}^{n_s} \sum_{k=1}^{n_t} \frac{1}{|G|} \sum_{g \in G} r_{ii}^s(g) r_{kk}^t(g)
\]

\[
= \delta_{st} \sum_{i=1}^{n_s} \frac{1}{n_s} = \delta_{st}
\]
and the theorem is proven.

2.8 Corollary The irreducible characters $\chi_1, \ldots, \chi_k$ of $G$ form a set of $\mathbb{C}$-linearly independent vectors in $\text{CF}(G, \mathbb{C})$. Moreover, one has $k \leq k(G)$, where $k(G)$ denotes the number of conjugacy classes of $G$.

Proof The first statement is a general fact about a set of orthogonal vectors in a $\mathbb{C}$-vector space with hermitian scalar product. The second statement follows immediately, since $\dim_{\mathbb{C}} \text{CF}(G, \mathbb{C}) = k(G)$.

The following theorem is an amazing fact: Although in general it is impossible to reconstruct a square matrix just from the knowledge of its trace, a representation of $G$ is determined up to equivalence by its character. However, given a character $\chi$ of $G$, it is in practice difficult to construct a representation $\Delta$ with character $\chi$.

2.9 Theorem Let $\Delta$ and $\Gamma$ be (complex) representations of $G$ which have the same character, i.e., $\chi_{\Delta} = \chi_{\Gamma}$. Then $\Delta$ and $\Gamma$ are equivalent.

Proof By Corollary 1.10(a), we know that $\Delta$ is equivalent to a direct sum of irreducible representations. Moreover, each of these irreducible representations is equivalent to one of our representatives $\Delta_i$, $1 \leq i \leq k$. Thus, altogether, $\Delta$ is equivalent to a direct sum of the form

$$\bigoplus_{i=1}^{k} \Delta_i \oplus \cdots \oplus \Delta_i. \quad (2.9.a)$$

Similarly, $\Gamma$ is equivalent to a direct sum of the form

$$\bigoplus_{i=1}^{k} \Delta_i \oplus \cdots \oplus \Delta_i. \quad (2.9.b)$$

Here, $l_i, m_i \in \mathbb{N}_0$ for $i = 1, \ldots, k$. Remark 1.14(b) implies that

$$l_1\chi_1 + \cdots + l_k\chi_k = \chi_\Delta = \chi_{\Gamma} = m_1\chi_1 + \cdots + m_k\chi_k.$$

The linear independence of $\chi_1, \ldots, \chi_k$ now implies that $l_i = m_i$ for all $i$. But this implies that the representations in (2.9.a) and (2.9.b) coincide. Thus, $\Delta$ is equivalent to $\Gamma$. □
2.10 Remark Let $\Delta : G \to \text{GL}_n(\mathbb{C})$ be a representation and let $\chi$ denote its character. By the argument in the proof of Theorem 2.9 we see that one can write $\chi$ as

$$\chi = m_1\chi_1 + \cdots + m_k\chi_k,$$

with unique coefficients $m_1, \ldots, m_k \in \mathbb{N}_0$. One can determine the coefficient $m_i$ quickly from the knowledge of the character $\chi$ and the irreducible character $\chi_i$ by

$$m_i = (\chi, \chi_i), \quad \text{for } i = 1, \ldots, k. \quad (2.10.a)$$

In fact, $(\chi, \chi_i) = \sum_{j=1}^k m_i(\chi_j, \chi_i) = m_i$, by Theorem 2.7. The number $m_i$ is called the \textit{multiplicity} of $\chi_i$ in $\chi$.

2.11 Proposition For the regular character $\rho_G$ of $G$ one has

$$\rho_G = n_1\chi_1 + \cdots + n_k\chi_k,$$

where $n_i = \chi_i(1)$ for $i = 1, \ldots, k$. In particular, evaluating at the identity element, one obtains

$$|G| = n_1^2 + \cdots + n_k^2.$$ 

\textbf{Proof} Recall from Example 1.15(b) that $\rho_G(1) = |G|$ and $\rho_G(g) = 0$ for $g \neq 1$. Therefore, the definition of the Schur inner product yields $(\rho_G, \chi_i) = \chi_i(1) = n_i$. Now equation (2.10.a) implies the formula for $\rho_G$. The second statement is clear. \qed

2.12 Lemma Let $\Delta : G \to \text{GL}_n(\mathbb{C})$ be an irreducible representation with character $\chi$ and let $f \in \text{CF}(G, \mathbb{C})$. Then the matrix

$$\Delta_f := \sum_{g \in G} f(g)\Delta(g^{-1}) \in \text{Mat}_n(\mathbb{C})$$

is a scalar matrix $\lambda \cdot I_n$ with $\lambda = \frac{|G|}{n} (f, \chi)$.

\textbf{Proof} For any $x \in G$ we have

$$\Delta(x)\Delta_f \Delta(x^{-1}) = \sum_{g \in G} f(g)\Delta(xg^{-1}x^{-1}) = \sum_{g \in G} f(xgx^{-1})\Delta(xg^{-1}x^{-1})$$

$$= \sum_{g \in G} f(\tilde{g})\Delta(\tilde{g}^{-1}) = \Delta_f,$$

20
where we substituted $\tilde{g} = xgx^{-1}$. Therefore we have $\Delta(x)\Delta_f = \Delta_f\Delta(x)$ for all $x \in G$. Now Corollary 2.2 implies that $\Delta_f = \lambda \cdot I_n$ with

$$
\lambda = \frac{\text{tr}(\Delta_f)}{n} = \frac{1}{n} \sum_{g \in G} f(g) \chi(g^{-1}) = \frac{1}{n} \sum_{g \in G} f(g) \overline{\chi(g)} = \frac{|G|}{n} \langle f, \chi \rangle.
$$

**2.13 Corollary** The set $\text{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ is an orthonormal basis of $\text{CF}(G, \mathbb{C})$ with respect to the Schur inner product. In particular, $|\text{Irr}(G)| = \dim_{\mathbb{C}} \text{CF}(G, \mathbb{C}) = k(G)$, the number of conjugacy classes of $G$. Moreover, for every class function $f \in \text{CF}(G, \mathbb{C})$ we have

$$
f = \sum_{i=1}^{k} (f, \chi_i) \chi_i,
$$

with the Schur inner product $(f, \chi_i) \in \mathbb{C}$, for $i = 1, \ldots, k$.

**Proof** By Theorem 2.7 it suffices to show that $\text{Irr}(G)$ generates $\text{CF}(G, \mathbb{C})$. For this it suffices to show that the orthogonal complement $\langle \text{Irr}(G) \rangle_C^\perp$ of $\langle \text{Irr}(G) \rangle_C$ is equal to 0, since $\text{CF}(G, \mathbb{C}) = \langle \text{Irr}(G) \rangle_C \oplus \langle \text{Irr}(G) \rangle_C^\perp$. So let $f \in \langle \text{Irr}(G) \rangle_C^\perp$. Then $(f, \chi_i) = 0$ for all $i = 1, \ldots, k$. Lemma 2.12 implies that $(\Delta_i)f = 0$ for every irreducible representation $\Delta_i$ of $G$, $i = 1, \ldots, k$. Set

$$
\Delta := \bigoplus_{i=1}^{k} \Delta_i \oplus \cdots \oplus \Delta_i
$$

and form $\Delta_f$ as in Lemma 2.12. Then, $\Delta_f$ is a block diagonal matrix with $n_i$ blocks equal to $(\Delta_i)f$. Therefore $\Delta_f = 0$. This implies that $\Delta'_f = \{0\}$ for every representation $\Delta'$ which is equivalent to $\Delta$. By Proposition 2.11 and Theorem 2.9, the representation $\Delta$ is equivalent to the regular representation $\Gamma$ with respect to any ordering $g_1, \ldots, g_n$ of the elements of $G$. We may assume that $g_1 = 1$. Thus $\Gamma_f = 0$ and we obtain the following equation in $\mathbb{C}^n$, where $e_i$ denotes the standard basis vector for $i = 1, \ldots, n$:

$$
0 = \Gamma_f e_1 = \sum_{i=1}^{n} f(g_i) \Gamma(g_i^{-1}) e_1 = \sum_{i=1}^{n} f(g_i^{-1}) \Gamma(g_i) e_1 = \sum_{i=1}^{n} f(g_i^{-1}) e_i.
$$

This implies that $f(g_i^{-1}) = 0$ for all $i = 1, \ldots, n$. Thus, $f = 0$ and the proof is complete. 

21
2.14 Remark One arranges the values of the irreducible characters $\chi_1, \ldots, \chi_k$ of $G$ in a quadratic table, the character table of $G$:

$$
\begin{array}{cccc}
  & g_1 & \cdots & g_j & \cdots & g_k \\
\chi_i & \chi_i(g_1) & \cdots & \chi_i(g_j) & \cdots & \chi_i(g_k) \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
\chi_i & \chi_i(g_1) & \cdots & \chi_i(g_j) & \cdots & \chi_i(g_k) \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
\chi_k & \chi_k(g_1) & \cdots & \chi_k(g_j) & \cdots & \chi_k(g_k) \\
\end{array}
$$

Here, $g_1, \ldots, g_k$ are representatives of the conjugacy classes of $G$. Often one also writes the cardinality $c_j$ of the conjugacy class of $g_j$ in a row below $g_j$. Note that $c_j = [G : C_G(g_j)]$ for $j = 1, \ldots, k$. Sometimes it is also useful to add a row with the orders $o(g_j)$ of the group elements $g_j$, $j = 1, \ldots, k$. Usually the elements $g_j$ are ordered in ascending element order, and the irreducible characters are ordered according to ascending character degree. Thus, usually $g_1 = 1$. One also usually has $\chi_1 = 1$, the trivial character.

2.15 Example For $G = \text{Sym}(3)$ (which is isomorphic to $D_6$) we obtain the character table

$$
\begin{array}{ccc}
g_j & 1 & (1, 2) & (1, 2, 3) \\
c_j & 1 & 3 & 2 \\
o(g_j) & 1 & 2 & 3 \\
1 = \chi_1 & 1 & 1 & 1 \\
\epsilon = \chi_2 & 1 & -1 & 1 \\
\chi_3 & 2 & 0 & -1 \\
\end{array}
$$

from our work in in Example 1.15(c), since we now know that $|\text{Irr}(G)| = k(G) = 3$.

2.16 Theorem (Second orthogonality relation) For any $g, h \in G$ one has

$$
\sum_{i=1}^{k} \chi_i(g)\chi_i(h^{-1}) = \begin{cases} |C_G(g)|, & \text{if } g \text{ and } h \text{ are conjugate}, \\ 0, & \text{otherwise}. \end{cases}
$$

Proof Write $f_h \in \text{CF}(G, \mathbb{C})$ for the class function which is equal to 1 on the class of $h$ and 0 everywhere else. By Corollary 2.13, we have

$$
f_h = \sum_{i=1}^{k} (f_h, \chi_i)\chi_i
$$
with
\[ (f_h, \chi_i) = \frac{1}{|G|} \cdot \frac{|G|}{|C_G(h)|} \cdot \chi_i(h^{-1}) = \frac{1}{|C_G(h)|} \cdot \chi_i(h^{-1}). \]

This implies
\[
\frac{1}{|C_G(h)|} \sum_{i=1}^{k} \chi_i(g) \chi_i(h^{-1}) = \sum_{i=1}^{k} \left( \frac{1}{|C_G(h)|} \chi_i(h^{-1}) \chi_i(g) \right) = \left( \sum_{i=1}^{k} (f_h, \chi_i) \chi_i \right)(g)
\]
\[ = f_h(g) = \begin{cases} 
1 & \text{if } g \text{ and } h \text{ are conjugate,} \\
0 & \text{otherwise},
\end{cases} \]

and the proof is complete.

The following remark introduces some new operations on representations and shows how those and the ones that were already established translate to operations on characters.

**2.17 Remark** Let \( F \) be an arbitrary field.

(a) **Tensor product of representations.** Let \( f: V \to V' \) and \( g: W \to W' \) be \( F \)-linear maps between \( F \)-vector spaces and let \( v_1, \ldots, v_n, v'_1, \ldots, v'_m \), \( w_1, \ldots, w_s, \) and \( w'_1, \ldots, w'_r \) be \( F \)-bases of \( V \), \( V' \), \( W \), and \( W' \), respectively. Moreover, let \( A \in \text{Mat}_{m \times n}(F) \) and \( B \in \text{Mat}_{r \times s}(F) \) be the representing matrices of \( f \) and \( g \) with respect to these bases, respectively. Then the representing matrix of the \( F \)-linear map \( f \otimes g: V \otimes_F W \to V' \otimes_F W' \), \( v \otimes w \mapsto f(v) \otimes g(w) \), with respect to the bases \( v_i \otimes w_j \) of \( V \otimes_F W \) and \( v'_i \otimes w'_j \) of \( V' \otimes_F W' \) in lexicographic order is given by the **Kronecker product** (also called **tensor product**) \( A \otimes B \) of \( A \) and \( B \). It is defined by

\[
A \otimes B = \begin{pmatrix}
  a_{11}B & \cdots & a_{1n}B \\
  \vdots & \ddots & \vdots \\
  a_{m1}B & \cdots & a_{mn}B
\end{pmatrix} \in \text{Mat}_{mr \times ns}(F).
\]

Note that if \( m = n \) and \( r = s \) then

\[
\text{tr}(A \otimes B) = a_{11}\text{tr}(B) + \cdots + a_{nn}\text{tr}(B) = \text{tr}(A) \cdot \text{tr}(B). \quad (2.17.a)
\]

Since the composition of linear maps corresponds to multiplication of matrices and since \( (f_1 \otimes g_1) \circ (f \otimes g) = (f_1 \circ f) \otimes (g_1 \circ g) \), we obtain for any additional matrices \( C \in \text{Mat}_{l \times m}(F) \) and \( D \in \text{Mat}_{q \times r}(F) \) that

\[
(C \otimes D)(A \otimes B) = (CA) \otimes (DB) \in \text{Mat}_{lq \times ns}(F). \quad (2.17.b)
\]
If $\Delta_1: G \to \text{GL}_m(F)$ and $\Delta_2: G \to \text{GL}_n(F)$ are representations of $G$ we define their tensor product $\Delta_1 \otimes \Delta_2$ by

$$\Delta_1 \otimes \Delta_2: G \to \text{GL}_{mn}(F), \quad g \mapsto \Delta_1(g) \otimes \Delta_2(g).$$

Equation (2.17.b) implies that $\Delta_1 \otimes \Delta_2$ is in fact a homomorphism, and Equation (2.17.a) implies that

$$\chi_{\Delta_1 \otimes \Delta_2}(g) = \chi_{\Delta_1}(g) \cdot \chi_{\Delta_2}(g),$$

for all $g \in G$. If we define the product of class functions $f_1, f_2 \in \text{CF}(G, \mathbb{C})$ in the usual way, by $(f_1 \cdot f_2)(g) := f_1(g)f_2(g)$ for $g \in G$, then the above equation shows that

$$\chi_{\Delta_1} \cdot \chi_{\Delta_2} = \chi_{\Delta_1 \otimes \Delta_2}.$$

In particular, the set of characters of $G$, as a subset of $\text{CF}(G, \mathbb{C})$, is multiplicatively closed: The product of two characters is again a character.

(b) Contragredient representation. If $\Delta: G \to \text{GL}_n(F)$ is a representation then also

$$\Delta^*: G \to \text{GL}_n(F), \quad g \mapsto (\Delta(g)^{-1})^t = (\Delta(g^{-1}))^t = \Delta(g^{-1})^t,$$

is a representation, called the contragredient representation of $\Delta$. One has

$$\chi_{\Delta^*}(g) = \text{tr}(\Delta(g^{-1})^t) = \text{tr}(\Delta(g^{-1})) = \chi_{\Delta}(g^{-1}),$$

for all $g \in G$. If $F \subseteq \mathbb{C}$ then one also has $\chi_{\Delta^*}(g) = \overline{\chi_{\Delta}(g)}$. Thus, in this case,

$$\chi_{\Delta^*} = \overline{\chi_{\Delta}},$$

where $\overline{\cdot}: \text{CF}(G, \mathbb{C}) \to \text{CF}(G, \mathbb{C})$ denotes the function defined by $f(g) := \overline{f(g)}$, for all $g \in G$. In particular, the set of characters of $G$, as a subset of $\text{CF}(G, \mathbb{C})$, is closed under complex conjugation. For any character $\chi$ of $G$, we call $\overline{\chi}$ the contragredient character of $\chi$.

(c) Inflation. Let $N \triangleleft G$ and let $\nu: G \to G/N =: \bar{G}$, $g \mapsto gN$, denote the canonical epimorphism. For any representation $\Gamma: G/N \to \text{GL}_n(F)$ we write

$$\text{Inf}^G_{G/N}(\Gamma) := \text{Res}_\nu(\Gamma) := \Gamma \circ \nu: G \to \text{GL}_n(F).$$

This representation of $G$ is called the inflation of the representation $\Gamma$. For instance, the trivial representation of $G$ is the inflation of the trivial representation of $G/N$. By the fundamental theorem of homomorphisms, the
map $\Gamma \mapsto \text{Inf}_{G/N}^G(\Gamma)$, defines a bijection between the representations $\Gamma$ of $G/N$ over $F$ of given degree $n$ and the representations $\Delta$ of $G$ over $F$ of degree $n$ with $N \leq \ker(\Delta)$. Moreover, since $\nu$ is surjective, one has $\Gamma(G/N) = (\Gamma \circ \nu)(G) = \Delta(G)$. It follows that two representations $\Gamma_1$ and $\Gamma_2$ of $G/N$ are equivalent if and only if their inflations $\text{Inf}_{G/N}^G(\Gamma_1)$ and $\text{Inf}_{G/N}^G(\Gamma_2)$ are equivalent. Furthermore, a representation $\Gamma$ of $G/N$ is irreducible (resp. indecomposable) if and only if its inflation $\text{Inf}_{G/N}^G(\Gamma)$ is irreducible (resp. indecomposable). This way, specializing to $F = \mathbb{C}$, inflation induces a bijection $\text{inf}_{G/N}^G : \text{Irr}(G/N) \to \{\chi \in \text{Irr}(G) \mid N \leq \ker(\chi)\}, \theta \mapsto \theta \circ \nu$.

(d) The character ring. We set $R(G) := \{a_1\chi_1 + \cdots + a_k\chi_k \mid a_1, \ldots, a_k \in \mathbb{Z}\} = \langle \text{Irr}(G) \rangle \subseteq \text{CF}(G, \mathbb{C})$, the $\mathbb{Z}$-span of the irreducible characters of $G$ in the $\mathbb{C}$-vector space of class functions of $G$. The elements of $R(G)$ are called generalized characters or also virtual characters. Every virtual character can be written as a difference of two characters. Conversely, the difference of two characters is always a virtual character. By Part (a), the product of two virtual characters is again a virtual character. Therefore, $R(G)$ is a subring of the $\mathbb{C}$-algebra of class functions $\text{CF}(G, \mathbb{C})$. It is called the character ring of $G$. Note that since $\text{Irr}(G)$ is a $\mathbb{C}$-linearly independent set in $\text{CF}(G, \mathbb{C})$ it is a $\mathbb{Z}$-basis of $R(G)$.

Previously defined constructions for representations induce structural maps on character rings and maps between character rings:

- direct sum $\oplus \rightarrow$ abelian group structure on $R(G)$
- tensor product $\otimes \rightarrow$ ring structure on $R(G)$
- contragredient $\ast \rightarrow$ ring automorphism $\bar{\cdot} : R(G) \to R(G), \chi \mapsto \bar{\chi}$
- $\text{Res}_f : R(G) \to R(\tilde{G}), \chi \mapsto \chi \circ f$
- $\text{Res}_H^G : R(G) \to R(H), \chi \mapsto \chi|_H$
- $\text{Inf}_{G/N}^G : R(G/N) \to R(G)$

Here, $f : \tilde{G} \to G$ denotes a group homomorphism, $H$ denotes a subgroup of $G$, and $N$ denotes a normal subgroup of $G$. The functions $\text{res}_H^G$ and $\text{inf}_{G/N}^G$ are special cases of $\text{res}_f$.

In the following proposition we give a criterion for when a generalized character $\chi \in R(G)$ is an irreducible character. Note that $\chi(1)$ is always an integer.

25
2.18 Proposition For every \( \chi \in R(G) \) the following are equivalent:

(i) \( \chi \in \text{Irr}(G) \).

(ii) \( (\chi, \chi) = 1 \) and \( \chi(1) > 0 \).

Proof If \( \chi \) is irreducible then the properties in (ii) are clearly satisfied. Conversely, assume that \( \chi \) satisfies the properties in (ii) and write \( \chi = a_1\chi_1 + \cdots + a_k\chi_k \) as a \( \mathbb{Z} \)-linear combination of the irreducible characters \( \chi_1, \ldots, \chi_k \) of \( G \). Then, by the first orthogonality relation (Theorem 2.7), we have

\[
1 = (\chi, \chi) = (a_1\chi_1 + \cdots + a_k\chi_k, a_1\chi_1 + \cdots + a_k\chi_k) = \sum_{i=1}^{k} \sum_{j=1}^{k} a_i a_j (\chi_i, \chi_j) = \sum_{i=1}^{k} a_i^2.
\]

This implies that there exists a unique index \( i \in \{1, \ldots, k\} \) such that \( a_i \neq 0 \) and moreover that \( a_i \in \{1, -1\} \). In otherwords, \( \chi = \pm \chi_i \). Now \( \chi(1) > 0 \) implies that \( \chi = \chi_i \in \text{Irr}(G) \).

Exercises

1. Let \( G \) be a finite group and let \( \chi \in \text{Irr}(G) \). Show that \( Z(G) \leq Z(\chi) \).

2. (a) Determine all the irreducible characters of the dihedral group \( D_8 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle \) of order 8.

(b) Determine all the irreducible characters of the quaternion group \( Q_8 = \langle x, y \mid x^4 = y^4 = 1, x^2 = y^2, yxy^{-1} = x^3 \rangle \) of order 8.

3. Assume that \( \Delta: G \to \text{GL}_n(F) \) is a representation of a finite group \( G \) over a field \( F \) and let \( \varphi: G \to F^\times \) be a homomorphism.

(a) Show that also \( \varphi \cdot \Delta: G \to \text{GL}_n(F), g \mapsto \varphi(g)\Delta(g) \) is a representation of \( G \) over \( F \), the twist of \( \Delta \) by \( \varphi \).

(b) Show that \( \Delta \) is irreducible (resp. indecomposable) if and only if \( \varphi \cdot \Delta \) is irreducible (resp. indecomposable).

4. Determine the irreducible representations of \( D_{10} \) (up to equivalence) and their characters.

5. Determine the irreducible characters of \( \text{Alt}(4) \).

6. (a) Let \( f: G \to H \) be a surjective group homomorphism and let \( \Delta: H \to \text{GL}_n(F) \) be a representation of \( H \) over an arbitrary field \( F \). Show that \( \Delta \) is
irreducible (resp. indecomposable) if and only if $\text{Res}_f(\Delta)$ is irreducible (resp. indecomposable).

(b) Determine the character table of the symmetric group $\text{Sym}(4)$. (Hint: Use (a) with $H$ a factor group of $\text{Sym}(4)$.)

7. Let $G$ be a finite group and write $\text{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$.

(a) Let $\chi$ and $\chi'$ be characters of $G$. Show that $\ker(\chi + \chi') = \ker(\chi) \cap \ker(\chi')$.

(b) Show that $\bigcap_{i=1}^k \ker(\chi_i) = \{1\}$.

(c) Let $N \trianglelefteq G$. Show that there exists a subset $I \subseteq \{1, \ldots, k\}$ such that

$$N = \bigcap_{i \in I} \ker(\chi_i).$$

In particular, one can determine from the character table the partially ordered set of normal subgroups of $G$. 

27
3 Algebraic Integers

Throughout this section, we denote by $S$ a commutative ring and by $R \subseteq S$ a subring with $1_S \in R$. We introduce and study elements of $S$ which are integral over $R$. We specialize to the situation where $R = \mathbb{Z}$ and $S = \mathbb{C}$ to obtain consequences for characters. Again, throughout this section, $G$ denotes a finite group. The main goal of this section is to show that the degrees of the irreducible characters of a finite group $G$ are divisors of $|G|$.

Recall that a polynomial $f = a_nX^n + \cdots + a_1X + a_0 \in R[X]$ of degree $n$ is called monic if $a_n = 1$. Thus, a monic polynomial is always non-zero.

3.1 Definition An element $s \in S$ is called integral over $R$ if there exists a monic polynomial $f \in R[X]$ such that $f(s) = 0$.

3.2 Remark For $s \in S$ one denotes by $R[s]$ the set of all finite $R$-linear combinations of the elements $1, s, s^2, \ldots$. In other words, one has $R[s] = \{ f(s) \mid f \in R[X] \} = \langle 1, s, s^2, \ldots \rangle_R$. Clearly, $R[s]$ is a subring of $S$. Moreover, it is the smallest subring of $S$ which contains $R$ and $s$. In other words, whenever $R' \subseteq S$ is a subring with $R \subseteq R'$ and $s \in R'$ then $R[s] \subseteq R'$.

More generally, for elements $s_1, \ldots, s_n \in S$, one writes $R[s_1, \ldots, s_n]$ for the set of all $R$-linear combinations of elements $s_1a_1^1 \cdots s_n^a_n$ with $a_1, \ldots, a_n \in \mathbb{N}_0$. In other words, $R[s_1, \ldots, s_n] = \{ f(s_1, \ldots, s_n) \mid f \in R[X_1, \ldots, X_n] \}$. Again it is easy to see that $R[s_1, \ldots, s_n]$ is a subring of $S$ and that it is the smallest subring of $S$ which contains $R$ and $\{ s_1, \ldots, s_n \}$. Thus, $R[s_1, \ldots, s_n]$ is independent of the order of the elements $s_1, \ldots, s_n$. It only depends on the set $\{ s_1, \ldots, s_n \}$. Moreover, if also $t_1, \ldots, t_m$ are elements in $S$ one has $(R[s_1, \ldots, s_n])[t_1, \ldots, t_m] = R[s_1, \ldots, s_n, t_1, \ldots, t_m]$.

The following theorem gives useful characterizations of when an element $s \in S$ is integral over $R$. Note that any subring $T$ of $S$ which contains $R$ is also an $R$-module.

For the proof of the following theorem recall the following notion and fact from linear algebra: If $B \in \text{Mat}_n(R)$ is a square matrix with entries $b_{ij}$ one defines its adjoint matrix $\tilde{B} \in \text{Mat}_n(R)$, also called the cofactor matrix of $B$, as the matrix with entries $\tilde{b}_{ij}$, where $\tilde{b}_{ij} := (-1)^{i+j} \det(B_{ji})$, where $B_{ji}$ is the square matrix of size $n-1$ that arises from deleting the $j$-th row and the $i$-th column from $B$. This matrix $\tilde{B}$ has the property

$$\tilde{B} \cdot B = \det(B) \cdot I_n = B \cdot \tilde{B}.$$
3.3 Theorem For $s \in S$ the following are equivalent:

(i) The element $s$ is integral over $R$.

(ii) The $R$-module $R[s]$ is finitely generated.

(iii) There exists a subring $T$ of $S$ with $R[s] \subseteq T \subseteq S$ such that $T$ is finitely generated as $R$-module.

Proof (i)⇒(ii): By definition, there exist $n \geq 1$ and $r_0, \ldots, r_{n-1} \in R$ such that $s^n + r_{n-1}s^{n-1} + \cdots + r_1s + r_0 = 0$. We will show by induction on $k \geq 1$ that $s^k \in \langle 1, s, s^2, \ldots, s^{n-1} \rangle_R$. For $k = 0, \ldots, n - 1$ this is clear and for $k = n$ this follows from

$$s^n = -r_0 \cdot 1 - r_1 s - r_2 s^2 - \cdots - r_{n-1} s^{n-1}.$$  \hspace{1cm} (3.3.a)

Now assume that $k \geq n$ and that $s^k \in \langle 1, s, s^2, \ldots, s^{n-1} \rangle_R$. Then, by Equation (3.3.a), we obtain

$$s^{k+1} = s \cdot s^k \in s \cdot \langle 1, s, s^2, \ldots, s^{n-1} \rangle_R = \langle s, s^2, \ldots, s^{n-1}, s^n \rangle_R \subseteq \langle 1, s, s^2, \ldots, s^{n-1} \rangle_R.$$  

This finishes the proof by induction and we have $R[s] = \langle 1, s, s^2, \ldots \rangle_R = \langle 1, s, s^2, \ldots, s^{n-1} \rangle_R$, which is finitely generated.

(ii)⇒(iii): This is trivial: choose $T = R[s]$.

(iii)⇒(i): Let $\{t_1, \ldots, t_n\} \subseteq T$ be a generating set of $T$ as $R$-module. Then we can express $st_i$ as an $R$-linear combination of $t_1, \ldots, t_n$ for every $i = 1, \ldots, n$. In other words, there exist elements $a_{ij} \in R$, $i, j \in \{1, \ldots, n\}$, such that

$$st_i = \sum_{j=1}^n a_{ij} t_j \quad \text{for all } i = 1, \ldots, n.$$  

One can rewrite this as a matrix equation for the matrix $A = (a_{ij}) \in \text{Mat}_n(R)$:

$$(s \cdot I_n - A) \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{in } T^n.$$  

Therefore, the matrix $B := s \cdot I_n - A \in \text{Mat}_n(R[s])$ satisfies

$$\det(B) I_n \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = \tilde{B} B \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad \text{in } T^n.$$  

29
This implies that \( \det(B) \cdot t_i = 0 \) for all \( i \in \{1, \ldots, n\} \). Since \( t_1, \ldots, t_n \) generate \( T \) as an \( R \)-module we obtain \( \det(B) \cdot T = 0 \) and \( \det(B) = \det(B) \cdot 1_T = 0 \). But, looking at the definition of \( B \), we see that there exist elements \( r_0, \ldots, r_{n-1} \in R \) such that

\[
\det(B) = s^n + r_{n-1}s^{n-1} + \cdots + r_1s + r_0.
\]

This completes the proof of the theorem.

3.4 Corollary The set \( R' \) of all elements of \( S \) that are integral over \( R \) is a subring of \( S \) containing \( R \). The ring \( R' \) is called the integral closure of \( R \) in \( S \).

Proof Clearly, \( R' \) is contained in \( S \). Moreover, it contains \( R \), since, for \( r \in R \), the monic polynomial \( f = X - r \in R[X] \) satisfies \( f(r) = 0 \). In order to show that \( R' \) is a subring of \( S \), let \( s, t \in R' \). We need to show that \( s - t \) and \( st \) are elements of \( R' \). Since \( s - t \) and \( st \) are elements of \( R' \), it suffices to show that \( R[s, t] = (R[s])[t] \) is a finitely generated \( R \)-module, cf. Theorem 3.3 (iii) \( \Rightarrow \) (i). Since \( s \) is integral over \( R \), Theorem 3.3 implies that the \( R \)-module \( R[s] \) is generated by a finite set \( \{x_1, \ldots, x_m\} \). Since \( t \) is integral over \( R \), it is also integral over \( R[s] \). Therefore, by the same argument, \( (R[s])[t] \) has a finite generating set \( \{y_1, \ldots, y_n\} \) as \( R[s] \)-module. This implies that \( (R[s])[t] \) is generated by the finite set \( \{x_iy_j \mid 1 \leq i \leq m, 1 \leq j \leq n\} \) as \( R \)-module, and the proof is complete.

3.5 Definition The elements in \( \mathbb{C} \) that are integral over \( \mathbb{Z} \) are called algebraic integers. They form a subring of \( \mathbb{C} \), the ring of algebraic integers. It is the integral closure of \( \mathbb{Z} \) in \( \mathbb{C} \).

3.6 Examples (a) For instance \( \sqrt{2}, \sqrt{3}, \sqrt{7}, (\sqrt{2} + \sqrt{3}\sqrt{7})^2 \) are algebraic integers. But \( \sqrt{2}/2 \) is not (see Exercise 1).

(b) Every \( n \)-th root of unity \( \zeta \in \mathbb{C} \) is an algebraic integer, since it is a root of the monic polynomial \( X^n - 1 \in \mathbb{Z}[X] \).

(c) Let \( \chi \in R(G) \) and let \( g \in G \). Then \( \chi(g) \) is an algebraic integer. In fact, one can write \( \chi = \chi_1 - \chi_2 \) as difference of two characters \( \chi_1 \) and \( \chi_2 \), and by Remark 1.14(d), \( \chi_i(g) \) is a sum of roots of unity for \( i = 1, 2 \).

3.7 Proposition Let \( s \in \mathbb{Q} \) and assume that \( s \) is integral over \( \mathbb{Z} \). Then \( s \in \mathbb{Z} \).
Proof We can assume that $s \neq 0$ and write $s = \frac{a}{b}$ with $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ satisfying $\gcd(a, b) = 1$. Assume that $b > 1$. Then there exists a prime $p$ which divides $b$. Since $s$ is an algebraic integer, there exist $n \geq 1$ and $r_0, \ldots, r_{n-1} \in \mathbb{Z}$ satisfying

$$\left(\frac{a}{b}\right)^n + r_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + r_1\frac{a}{b} + r_0 = 0.$$ 

Multiplication with $b^n$ yields

$$a^n + r_{n-1}a^{n-1}b + r_{n-2}a^{n-2}b^2 + \cdots + r_1ab^{n-1}r_0b^n = 0.$$ 

But this implies that $a^n$ is divisible by $p$. Therefore, also $a$ is divisible by $p$. This is a contradiction to $\gcd(a, b) = 1$. Therefore, $b = 1$ and $s \in \mathbb{Z}$. \hfill \Box

3.8 Notation Let $C_1, \ldots, C_k$ denote the conjugacy classes of the group $G$. For every $r \in \{1, \ldots, k\}$ we choose an element $z_r \in C_r$, and for $r, s, t \in \{1, \ldots, k\}$ we set

$$a_{rst} := |\{(x, y) \in C_r \times C_s \mid xy = z_t\}|.$$ 

Note that the element $a_{rst} \in \mathbb{N}_0$ does not depend on the choice of $z_r$. In fact, if also $z'_r \in C_r$ then $z'_r = gz_rg^{-1}$, for some $g \in G$, and the maps

$$\begin{align*}
\{(x, y) \in C_r \times C_s \mid xy = z_t\} &\leftrightarrow \{(x', y') \in C_r \times C_s \mid x'y' = z'_t\} \\
(x, y) &\mapsto (gxg^{-1}, gyg^{-1}) \\
(g^{-1}x'g, g^{-1}y'g) &\leftarrow (x', y')
\end{align*}$$

are mutually inverse bijections.

3.9 Lemma Let $C_1, \ldots, C_k$ denote the conjugacy classes of $G$ and let $g_r \in C_r$ for $r \in \{1, \ldots, k\}$. Moreover let $\Delta : G \to \text{GL}_n(\mathbb{C})$ be an irreducible representation and let $\chi$ denote the character of $\Delta$. Then, for all $r \in \{1, \ldots, k\}$, one has

$$\sum_{x \in C_r} \Delta(x) = \lambda_r I_n \quad \text{with} \quad \lambda_r = |C_r|\frac{\chi(g_r)}{n}.$$ 

Moreover, the complex numbers $\lambda_1, \ldots, \lambda_k$ are algebraic integers.
Proof For \( r \in \{1, \ldots, k\} \) we set \( A_r := \sum_{x \in C_r} \Delta(x) \in \text{Mat}_n(\mathbb{C}) \). Then we obtain, for every \( g \in G \), the equation

\[
\Delta(g) A_r \Delta(g)^{-1} = \sum_{x \in C_r} \Delta(gxg^{-1}) = \sum_{y \in C_r} \Delta(y) = A_r,
\]

after substituting \( gxg^{-1} \) with \( y \). By Corollary 2.2(b), we obtain \( A_r = \lambda_r \cdot I_n \) with

\[
\lambda_r = \frac{\text{tr}(A_r)}{n} = \sum_{x \in C_r} \frac{\text{tr}(\Delta(x))}{n} = |C_r| \chi(g_r) n.
\]

We still need to show that the numbers \( \lambda_1, \ldots, \lambda_r \) are algebraic integers. For \( r, s \in \{1, \ldots, k\} \) we have

\[
\lambda_r \lambda_s \cdot I_n = A_r A_s = \sum_{(x,y) \in C_r \times C_s} \Delta(xy) = \sum_{t=1}^k \sum_{z \in C_t} a_{rst} \Delta(z)
\]

\[
= \sum_{t=1}^k a_{rst} A_t = \left( \sum_{t=1}^k a_{rst} \lambda_t \right) \cdot I_n,
\]

where the integers \( a_{rst} \) are defined as in 3.8. This implies that \( \lambda_r \lambda_s = \sum_{t=1}^k a_{rst} \lambda_t \) and that the finitely generated \( \mathbb{Z} \)-module \( T := \langle \lambda_1, \ldots, \lambda_k \rangle \subset \mathbb{C} \) is a subring of \( \mathbb{C} \). Thus, we have \( \mathbb{Z}[\lambda_r] \subseteq T \subset \mathbb{C} \) and \( \lambda_r \) is an algebraic integer for all \( r \in \{1, \ldots, k\} \), by Theorem 3.3(iii) \( \Rightarrow \) (i).

3.10 Corollary Let \( \Delta: G \to \text{GL}_n(\mathbb{C}) \) be an irreducible representation. Then \( n \) divides \( |G| \).

Proof Let \( \chi \) denote the character of \( \Delta \). Then, with the notation from Lemma 3.9, we have

\[
\sum_{r=1}^k \lambda_r \chi(g_r^{-1}) = \sum_{r=1}^k |C_r| \chi(g_r) \chi(g_r^{-1}) = \frac{1}{n} \sum_{x \in G} \chi(x) \chi(x^{-1}) = \frac{|G|}{n} \chi(\chi) = \frac{|G|}{n}.
\]

The first term of this equality is an algebraic integer by Lemma 3.9 and by Corollary 3.4. On the other hand the last term in the equality is a rational number. Thus, by Proposition 3.7, we obtain that this number is an integer. This implies that \( n \) divides \( |G| \).

32
3.11 Remark (McKay Conjecture) Let $p$ be a prime and denote by $\text{Irr}_{p'}(G)$ the set of irreducible characters $\chi$ of $G$ whose degree is not divisible by $p$.

A longstanding conjecture in character theory, the McKay Conjecture, states the following: Let $G$ be a finite group, let $p$ be a prime, let $P \in \text{Syl}_p(G)$ and set $H := N_G(P)$. Then

$$|\text{Irr}_{p'}(G)| = |\text{Irr}_{p'}(H)|.$$  \hspace{1cm} (3.11.a)

Note that if $p$ does not divide the order of $G$ then $P = 1$, $H = G$ and the above equation holds for trivial reasons. More generally, if $G$ has a normal Sylow $p$-subgroup, Equation (3.11.a) always holds, since $H = G$.

3.12 Examples (a) Let $G = \text{Sym}(3)$. The irreducible characters of $G$ have degree 1, 1, 2. For $p = 2$ we obtain $P \cong C_2$, a cyclic group of order 2, and $H := N_G(P) = P \cong C_2$. Thus $|\text{Irr}_2(G)| = 2 = |\text{Irr}_2(H)|$. For $p = 3$ we obtain $P = \text{Alt}(3)$. Thus, $H := N_G(P) = G$ and the equation (3.11.a) holds.

(b) Let $G = \text{Sym}(4)$. The irreducible characters of $G$ have degrees 1, 1, 2, 3, 3. For $p = 2$ we obtain $P \cong D_8$ and $H := N_G(P) = P \cong D_8$. Since the character degrees of $D_8$ are 1, 1, 1, 1, 2, we obtain $|\text{Irr}_2(G)| = 4 = |\text{Irr}_2(H)|$ as predicted. For $p = 3$, we have $P \cong C_3$, a cyclic group of order 3, for instance we can choose $P = \text{Alt}(3)$. Then $H := N_G(P) = \text{Sym}(3)$ and we obtain $|\text{Irr}_3(G)| = 3 = |\text{Irr}_3(H)|$ as predicted by the conjecture.

Exercises

1. Show that $\sqrt{2}/2$ is not an algebraic integer.

2. Let $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ be the field with 3 elements and let $G := \text{SL}_2(\mathbb{F}_3)$.

   (a) Compute the order of $G$.

   (b) Compute the conjugacy classes of $G$.

   (c) Compute $Z(G)$ and determine the isomorphism type of $G/Z(G)$.

   (d) Compute the character table of $G$.

3. (a) Determine the character degrees of $\text{Alt}(5)$ and verify the McKay Conjecture for the primes 2, 3, 5.

   (b) Compute the character degrees of $\text{Sym}(5)$ as follows. Compute the commutator subgroup by using that $\text{Alt}(5)$ is simple. Show that the natural permutation character decomposes into the trivial character and an irreducible character of degree 4. Show that $\text{Sym}(5)$ has no irreducible character of degree 2 by considering the restriction to $\text{Alt}(5)$.
(c) Verify the McKay Conjecture for Sym(5) for $p = 2, 3, 5$.

4. Let $G := \text{GL}_2(\mathbb{F}_3)$.
   (a) Determine the order of $G$, the center of $G$ and the commutator subgroup of $G$.
   (b) Determine the character degrees of $G$ and verify the McKay Conjecture for the primes 2 and 3.
   (c) Show that $\bar{G} := G/Z \cong \text{Sym}(4)$. (Hint: Find some set with four elements on which $G$ acts naturally.)
   (d) Compute as much as you can of the character table of $G$.

5. Compute as much as you can of the character table of $\text{Alt}(5)$.

6. Let $p$ be a prime and let $G$ be a non-abelian group of order $p^3$.
   (a) Show that $Z(G)$ has order $p$ and that $G' = Z(G)$.
   (b) Show that $G$ has $p^2$ irreducible characters of degree 1, $p - 1$ irreducible characters of degree $p$, and no others.
4 Burnside’s $p^aq^b$-Theorem

The goal of this section is to prove a famous Theorem of Burnside which says that every finite group of order $p^aq^b$ (with primes $p$ and $q$ and with $a,b \in \mathbb{N}_0$) is solvable. The proof will use character theory and some basic facts from field theory applied to character values. We will recall these field theoretic facts first.

4.1 Remark (a) Let $\alpha$ be a complex number and consider the unique ring homomorphism

$$\varepsilon : \mathbb{Q}[X] \to \mathbb{Q}[\alpha], \quad X \mapsto \alpha.$$ 

By definition it is surjective. If it is injective, $\alpha$ is called transcendental over $\mathbb{Q}$. From now on we assume that $\varepsilon$ is not injective (in this case $\alpha$ is called algebraic over $\mathbb{Q}$). The image of $\varepsilon$ (as a subring of $\mathbb{C}$) is an integral domain. By the fundamental theorem of homomorphisms, its kernel must be a non-zero prime ideal. Since $\mathbb{Q}[X]$ is a principal ideal domain, this prime ideal is also a maximal ideal and of the form $(f)$ for a unique monic irreducible polynomial $f \in \mathbb{Q}[X]$. The polynomial $f$ is called the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Since $(f)$ is a maximal ideal, $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha]$ is a field. We set $n := \deg(f)$. Then $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha]$ are $\mathbb{Q}$-vector spaces of dimension $n$. We write $f = (X - \alpha_1) \cdots (X - \alpha_n)$ with unique complex numbers $\alpha = \alpha_1, \ldots, \alpha_n$. These numbers are pairwise distinct (every field extension of $\mathbb{Q}$ is separable, since $\mathbb{Q}$ has characteristic 0). For each $i = 1, \ldots, n$ we obtain a unique ring homomorphism

$$\sigma_i : \mathbb{Q}[\alpha] \to \mathbb{C}, \quad \alpha \mapsto \alpha_i.$$ 

Composing these $n$ ring homomorphisms with $\varepsilon^{-1} : \mathbb{Q}[\alpha] \to \mathbb{Q}[X]/(f)$, we obtain $n$ pairwise distinct ring homomorphisms

$$\sigma_i : \mathbb{Q}[\alpha] \to \mathbb{C}, \quad \alpha \mapsto \alpha_i, \quad (i = 1, \ldots, n).$$

There are no other ring homomorphisms from $\mathbb{Q}[\alpha]$ to $\mathbb{C}$, since each such homomorphism must take a root of $f$ to a root of $f$.

(b) If $\alpha$ from above is an algebraic integer then each $\alpha_i, i = 1, \ldots, n$, is an algebraic integer as well. In fact, there exist $c_0, \ldots, c_{k-1} \in \mathbb{Z}$ such that $\alpha^k + c_{k-1} \alpha^{k-1} + \cdots + c_1 \alpha + c_0 = 0$ and applying $\sigma_i$ from Part (a) to this equation yields the equation $\alpha_i^k + c_{k-1} \alpha_i^{k-1} + \cdots + c_1 \alpha_i + c_0 = 0$ as desired. Corollary 3.4 implies that the coefficients of the polynomial $f = (X - \alpha_1) \cdots (X - \alpha_n)$ are
algebraic integers. Since they are also rational numbers, Proposition 3.7 implies \( f \in \mathbb{Z}[X] \).

(c) Similar considerations as in Part (a) lead quickly to the following result: Let \( \mathbb{Q} \subseteq K \subseteq L \subseteq \mathbb{C} \) be fields with \( \dim_{\mathbb{Q}}(L) < \infty \) and let \( \sigma : K \to \mathbb{C} \) be a ring homomorphism. Then there exists a ring homomorphism \( \tau : L \to \mathbb{C} \) with \( \tau|_K = \sigma \). Simply replace \( \mathbb{Q} \) with \( K \) in (a) and make some minor adjustments where necessary. With some more effort one can show that \( \sigma \) can be extended to \( L \), even when \( [L : K] \) is infinite.

(d) Let \( k \in \mathbb{N} \) and \( \zeta := e^{2\pi i/k} \in \mathbb{C} \). Then the complete set of ring homomorphisms \( \mathbb{Q}[\zeta] \to \mathbb{C} \) can be constructed as follows: For every \( i \in \{1, \ldots, k\} \) with \( \gcd(i, k) = 1 \) there is a unique ring homomorphism

\[
\sigma_i : \mathbb{Q}[\zeta] \to \mathbb{C}, \quad \zeta \mapsto \zeta^i.
\]

One clearly has \( \sigma_i(\mathbb{Q}[\zeta]) = \mathbb{Q}[\zeta] \), and the inverse of the ring isomorphism \( \sigma_i : \mathbb{Q}[\zeta] \to \mathbb{Q}[\zeta] \) is equal to \( \sigma_j \) where \( j \in \{1, \ldots, k\} \) is the unique element with \( ij \equiv 1 \pmod{k} \). The field extension \( \mathbb{Q}[\zeta]/\mathbb{Q} \) is a Galois extension with Galois group

\[
\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) = \{ \sigma_i | i = 1, \ldots, k; \gcd(i, k) = 1 \} \cong (\mathbb{Z}/k\mathbb{Z})^\times.
\]

4.2 Lemma Let \( G \) be a finite group, let \( g \in G \) and let \( \chi \) be a character of \( G \). Then \( 0 \leq |\chi(g)/\chi(1)| \leq 1 \). Moreover, if \( \chi(g)/\chi(1) \) is an algebraic integer then \( |\chi(g)/\chi(1)| = 1 \) or \( \chi(g) = 0 \).

Proof Set \( d := \chi(1) \) for the degree of \( \chi \) and let \( k \) denote the order of \( g \). By Remark 1.14(d), we know that \( \chi(g) \) can be expressed as \( \chi(g) = \zeta^{i_1} + \cdots + \zeta^{i_d} \) with \( \zeta := e^{2\pi i/k} \) and elements \( i_1, \ldots, i_d \in \{0, \ldots, k-1\} \). The triangle inequality then yields the first assertion:

\[
0 \leq |\chi(g)/d| = \left| \frac{\zeta^{i_1}}{d} + \cdots + \frac{\zeta^{i_d}}{d} \right| \leq \left| \frac{\zeta^{i_1}}{d} \right| + \cdots + \left| \frac{\zeta^{i_d}}{d} \right| = \frac{1}{d} + \cdots + \frac{1}{d} = 1.
\]

From now on assume that \( \alpha := \chi(g)/d \) is an algebraic integer. We already know that \( 0 \leq |\alpha| \leq 1 \). Assume that \( |\alpha| < 1 \). It suffices to show that \( \alpha = 0 \).

Since \( \alpha \) is an algebraic integer, it is algebraic over \( \mathbb{Q} \) and has a minimal polynomial \( f = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \in \mathbb{Q}[X] \). Since \( \alpha \) is an algebraic integer, we even have \( f \in \mathbb{Z}[X] \), by Remark 4.1(b). Note that \( \alpha \in \mathbb{Q}[\zeta] \) and therefore \( \mathbb{Q}[\alpha] \subseteq \mathbb{Q}[\zeta] \). We can write \( f = (X - \alpha_1) \cdots (X - \alpha_n) \in \mathbb{C}[X] \) and the roots \( \alpha = \alpha_1, \ldots, \alpha_n \in \mathbb{C} \) of \( f \) are given by the images \( \sigma(\alpha) \), where \( \sigma \).
runs through the ring homomorphisms from $\mathbb{Q}[\alpha]$ to $\mathbb{C}$, cf. Remark 4.1(a). By Remark 4.1(c) and (d), each such $\sigma$ is the restriction of a ring homomorphism $\sigma_j: \mathbb{Q}[\zeta] \to \mathbb{C}$ with $\sigma_j(\zeta) = \zeta^j$. Thus, each $\alpha_i, i = 1, \ldots, n$, is of the form

$$\sigma_j(\alpha) = \frac{\zeta^{i_1j}}{d} + \cdots + \frac{\zeta^{i_dj}}{d},$$

where $j \in \{1, \ldots, k\}$ with $\gcd(j, k) = 1$. As in the first part of the proof, the triangle inequality implies that $|\alpha_i| \leq 1$ for all $i = 1, \ldots, n$. Since $|\alpha| = |\alpha_1| < 1$, we obtain that $|\alpha_1 \cdots \alpha_n| < 1$. But, on the other hand $\alpha_1 \cdots \alpha_n = \pm c_0 \in \mathbb{Z}$. Thus, we have $|c_0| < 1$ and $c_0 = 0$. But then $f = X(c_1 + c_2X + \cdots + X^{n-1})$. Since $f$ is irreducible, this implies that the second factor must be a unit in $\mathbb{Q}[X]$, i.e., a constant non-zero polynomial. Since $f$ is monic, this implies that $f = X$. Since $\alpha$ is a root of $f$, this implies $\alpha = 0$ as desired.

4.3 Lemma Assume that $G$ is a finite group which has a conjugacy class $C$ with $p^r$ elements, where $p$ is a prime and $r \geq 1$. Then $G$ has a normal subgroup $N$ with $\{1\} < N < G$, i.e., $G$ is not simple.

Proof First note that $G$ is not abelian, since it has a conjugacy class with more than 1 element. Let $g \in C$. Then $g \neq 1$, since the conjugacy class of 1 has just one element. As before, let $\chi_1, \ldots, \chi_k$ denote the irreducible characters of $G$ and assume that $\chi_1$ is the trivial character. By the second orthogonality relation applied to the elements $g$ and 1 we obtain

$$0 = \sum_{i=1}^{k} \chi_i(g)\chi_i(1) = 1 + \sum_{i=2}^{k} \chi_i(g)\chi_i(1)$$

and

$$-\frac{1}{p} = \sum_{i=2}^{k} \chi_i(g)\frac{\chi_i(1)}{p}.$$

Since $-1/p$ is not an algebraic integer (cf. Proposition 3.7), there exists an element $i \in \{2, \ldots, k\}$ such that $\chi_i(g)\chi_i(1)/p$ is not an algebraic integer. To simplify the notation, from now on we set $\chi := \chi_i$ and note that $\chi$ is not the trivial character, since $i \geq 2$. Since $\chi(g)\chi(1)/p$ is not an algebraic
integer, we obtain that \( \chi(g) \neq 0 \) and that \( p \) does not divide \( \chi(1) \). Then \( \gcd(p^r, \chi(1)) = 1 \). Thus, there exist \( a, b \in \mathbb{Z} \) such that \( 1 = ap^r + b\chi(1) \). Multiplication with \( \chi(g) / \chi(1) \) yields 
\[
\frac{\chi(g)}{\chi(1)} = a|C|\frac{\chi(g)}{\chi(1)} + b\chi(g),
\]
since \( |C| = p^r \). By Lemma 3.9, the number \( |C|\chi(g) / \chi(1) \) is an algebraic integer. Since also \( \chi(g) \) is an algebraic integer, the right hand side of the above equation is an algebraic integer and also \( \chi(g) / \chi(1) \) is an algebraic integer. Now Lemma 4.2 applies. Since \( \chi(g) \neq 0 \), we obtain \( |\chi(g) / \chi(1)| = 1 \) which is equivalent to \( g \in Z(\chi) \), the center of \( \chi \), cf. Remark 1.14(d). Since \( g \neq 1 \), the normal subgroup \( Z(\chi) \) of \( G \) is not trivial, and if \( Z(\chi) < G \) we are done. So we assume from now on that \( Z(\chi) = G \). In this case we consider the normal subgroup \( N := \ker(\chi) \) of \( G \). Recall from Remark 1.14(d) that \( Z(\chi) = G \) implies that every representation \( \Delta \) with character \( \chi \) takes values in scalar matrices. But since \( \chi \) is irreducible this implies that \( \chi \) has degree 1. Thus, \( \chi \) is a homomorphism from \( G \) to \( \mathbb{C}^\times \) and \( G/N \) is isomorphic to an abelian group. Now, since \( G \) is not abelian, we obtain \( N \neq 1 \), and since \( \chi \) is not equal to the trivial character, we obtain \( N < G \). This completes the proof.

Recall: If \( N \) is a normal subgroup of a group \( G \) such that \( N \) and \( G/N \) are solvable then \( G \) is solvable.

4.4 Theorem (Burnside’s \( p^aq^b \)-Theorem) If \( G \) is a finite group of order \( p^aq^b \) with primes \( p \) and \( q \) and with \( a, b \in \mathbb{N}_0 \) then \( G \) is solvable.

Proof We prove the statement by induction on the order of \( G \). If \( |G| = 1 \) then \( G \) is clearly solvable. Now assume that \( p^aq^b > 1 \) and that the statement holds for all groups of smaller order. We may assume that \( G \) is not abelian, because otherwise we are done. It suffices to show that \( G \) has a normal subgroup different from \( \{1\} \) and \( G \). If \( a = 0 \) or \( b = 0 \) then \( G \) is a \( p \)-group (or a \( q \)-group) and therefore \( \{1\} < Z(G) \triangleleft G \), and we are done. So we can assume that \( a, b \in \mathbb{N} \) and that \( p \neq q \). Choose a Sylow \( q \)-subgroup \( Q \) of \( G \). Then \( |Q| = q^b > 1 \) and therefore \( Z(Q) \supseteq \{1\} \). Choose \( 1 \neq g \in Z(Q) \). Then the conjugacy class of \( g \) has cardinality \( [G : C_G(g)] \). Since \( g \in Z(Q) \), we have \( Q \leq C_G(g) \leq G \) and therefore, \( [G : C_G(g)] = p^r \) for some \( 0 \leq r < a \). If \( r = 0 \) then \( 1 \neq \langle g \rangle \triangleleft G \) and we are done. If \( r > 0 \) then Lemma 4.3 implies that \( G \) has a normal subgroup \( N \) with \( \{1\} < N < G \). This completes the proof.

38
Exercises

1. Assume that $G$ is a non-abelian finite simple group. Show that $G$ has no abelian subgroup of index $p^r$, where $p$ is a prime and $r \geq 1$.

2. (Adams operations) Let $G$ be a finite group. For $i \in \mathbb{Z}$ and for a class function $f \in \text{CF}(G, \mathbb{C})$ let $\Psi^i(f)$ denote the function $G \to \mathbb{C}$, $g \mapsto f(g^i)$.
   
   (a) Show that $\Psi^i(f)$ is again a class function.
   
   (b) Show that the resulting function $\Psi^i: \text{CF}(G, \mathbb{C}) \to \text{CF}(G, \mathbb{C})$ is a $\mathbb{C}$-algebra homomorphism, i.e., a $\mathbb{C}$-linear map and a ring homomorphism. The map $\Psi^i$ is called the $i$-th Adams operation.
   
   (c) Show that for $i, j \in \mathbb{Z}$ one has $\Psi^i \circ \Psi^j = \Psi^{ij}$. Show that $\Psi^i = \Psi^j$ whenever $i \equiv j \mod \exp(G)$. (Here $\exp(G)$ denotes the exponent of $G$, i.e., the smallest positive integer $n$ with the property that $g^n = 1$ for all $g \in G$.)
   
   (d) Show that if $i \in \mathbb{Z}$ with $\gcd(i, \exp(G)) = 1$ then $\Psi^i$ is an isometry with respect to the Schur inner product, i.e., a $\mathbb{C}$-linear isomorphism satisfying $(\Psi^i(f), \Psi^i(g)) = (f, g)$ for all $f, g \in \text{CF}(G, \mathbb{C})$. What is its inverse?

3. (Galois action on characters) Let $G$ be a finite group of exponent $n$, let $\zeta := e^{2\pi i/n}$, set $K := \mathbb{Q} [\zeta]$, and for $i \in \{1, \ldots, n-1\}$ with $\gcd(i, n) = 1$ let $\sigma_i: \mathbb{Q}[\zeta] \to \mathbb{Q}[\zeta]$ denote the ring homomorphism given by $\sigma_i(\zeta) = \zeta^i$. Note that for any $\chi \in \mathcal{R}(G)$ one has $\chi(g) \in K$. Therefore, we can define the function $\sigma^\chi: G \to K$ by $g \mapsto \sigma_i(\chi(g))$.
   
   (a) Let $i \in \{1, \ldots, n\}$ with $\gcd(i, n) = 1$. Show that $(\sigma^\chi)(g) = \chi(g^i)$ for every virtual character $\chi \in \mathcal{R}(G)$ and every $g \in G$. Thus, $\sigma^\chi = \Psi^i(\chi)$.
   
   (b) Assume again that $\gcd(i, n) = 1$ and let $\chi$ be a character of $G$. Show that $\Psi^i(\chi)$ is again a character and show that $\Psi^i(\chi)$ is irreducible if and only if $\chi$ is irreducible.
   
   (c) Show that all entries of the character table of a symmetric group are integers.
5 The Group Algebra and its Modules

Throughout this section, \( k \) denotes a commutative ring and \( G \) denotes a finite group. All ring homomorphisms are unitary, i.e., they map the identity element to the identity element.

5.1 Definition A \( k \)-algebra is a pair \((R, \eta)\) consisting of a ring \( R \) together with a ring homomorphism \( \eta: k \to R \) satisfying \( \eta(k) \subseteq Z(R) \), i.e., \( \eta(\alpha)r = r\eta(\alpha) \) for all \( \alpha \in k \) and \( r \in R \). A \( k \)-algebra homomorphism between two \( k \)-algebras \((R, \eta)\) and \((R', \eta')\) is a ring homomorphism \( f: R \to R' \) such that \( f \circ \eta = \eta' \). Very often it is clear from the context what \( \eta \) is and we only write \( R \) instead of \((R, \eta)\).

5.2 Remark (a) In general, \( \eta \) need not be injective. If \( k \) is a field then \( \eta \) is always injective and \( k \) can be considered as a subring of \( R \) via \( \eta \).

(b) If \((R, \eta)\) is a \( k \)-algebra then \( R \) is a \( k \)-module via \( \alpha \cdot r := \eta(\alpha)r \). For this module structure one has \( r(\alpha \cdot s)t = \alpha \cdot (rst) \), for \( r, s, t \in R \) and \( \alpha \in k \). Conversely, if \( R \) is a ring which has also a \( k \)-module structure satisfying \( r(\alpha \cdot s)t = \alpha \cdot (rst) \), for \( r, s, t \in R \) and \( \alpha \in k \), then we can define \( \eta: k \to R \), \( \alpha \mapsto \alpha \cdot 1_R \), and obtain a \( k \)-algebra \((R, \eta)\). These two constructions are mutually inverse.

(c) Let \((R, \eta)\) and \((R', \eta')\) be \( k \)-algebras and let \( f: R \to R' \) be a function. Then, \( f \) is a \( k \)-algebra homomorphism if and only if \( f \) is a ring homomorphism and a \( k \)-module homomorphism (with respect to the \( k \)-module structures defined in (b)).

(d) \( \mathbb{Z} \)-algebras and \( \mathbb{Z} \)-algebra homomorphisms are nothing else as rings and ring homomorphisms. In fact, for every ring \( R \) there exists a unique ring homomorphism \( \eta: \mathbb{Z} \to R \) and this homomorphism satisfies \( \eta(\mathbb{Z}) \subseteq Z(R) \). Moreover, every ring homomorphism \( f: R \to R' \) satisfies \( f \circ \eta = \eta' \) for these homomorphism \( \eta: \mathbb{Z} \to R \) and \( \eta': \mathbb{Z} \to R' \). General statements about \( k \)-algebras reduce to statements about rings after specializing \( k \) to \( \mathbb{Z} \).

5.3 Examples (a) The polynomial ring \( k[X] \) is a \( k \)-algebra with \( \eta \) mapping an element \( \alpha \in k \) to the constant polynomial \( \alpha \).

(b) The matrix ring \( \text{Mat}_n(k) \) is a \( k \)-algebra with \( \eta: k \to \text{Mat}_n(k) \), \( \alpha \mapsto \alpha I_n \).

(c) If \( M \) is a \( k \)-module then the \( k \)-endomorphism ring \( \text{End}_k(M) \) is a \( k \)-algebra with \( \eta: k \to \text{End}_k(M) \), \( \alpha \mapsto l_\alpha \), where \( l_\alpha: M \to M \) is the left
multiplication by $\alpha$, i.e., $l_\alpha(m) = \alpha m$ for all $m \in M$. The multiplication on $\text{End}_k(M)$ is given by composition.

**5.4 Definition** The group algebra $kG$ is defined as the free $k$-module with basis $G$. It is a ring with the following multiplication rule:

$$(\sum_{g \in G} \alpha_g g)(\sum_{h \in G} \beta_h h) = \sum_{g \in G} \sum_{h \in G} \alpha_g \beta_h gh.$$ 

In other words, the multiplication on $kG$ is just the $k$-bilinear extension of the multiplication on $G$. The basis element $1 \in G$ is also the identity element of the ring $kG$. Moreover, every basis element $g \in G$ is invertible in $kG$. Its inverse is the basis element $g^{-1}$. Clearly, the $k$-span of 1 is contained in the center of $kG$. Therefore, $kG$ is in fact a $k$-algebra via $\eta: k \to kG$, $\alpha \mapsto \alpha 1$. This construction also works for infinite groups $G$.

**5.5 Example** For $G = \text{Sym}(3) = \{1, \sigma, \sigma^2, \tau, \sigma \tau, \sigma^2 \tau\}$ with $\sigma = (1, 2, 3)$ and $\tau = (1, 2)$, one has

$$kG = k \cdot 1_G \oplus k \cdot \sigma \oplus k \cdot \sigma^2 \oplus k \cdot \tau \oplus k \cdot \sigma \tau \oplus k \cdot \sigma^2 \tau.$$ 

For $k = \mathbb{Z}$ and for $a = 2 \cdot 1_G + 3 \cdot \sigma - \tau$ and $b = \sigma^2 - 2 \cdot \sigma \tau$ in $\mathbb{Z}G$ one has

$$ab = (2 \cdot 1_G + 3 \cdot \sigma - \tau)(\sigma^2 - 2 \cdot \sigma \tau) = 2 \cdot \sigma^2 - 4 \cdot \sigma \tau + 3 \cdot \sigma^3 - 6 \cdot \sigma^2 \tau - \tau \sigma^2 + 2 \cdot \tau \sigma \tau = 3 \cdot 1_G + 4 \cdot \sigma^2 - 5 \cdot \sigma \tau - 6 \cdot \sigma^2 \tau,$$

since $\tau \sigma^2 = \sigma \tau$ and $\tau \sigma \tau = \sigma^2$.

**5.6 Remark** (a) If $f: G \to H$ is a group homomorphism then its $k$-linear extension

$$kf: kG \to kH, \quad \sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g f(g),$$

is a $k$-algebra homomorphism. In fact, it is $k$-linear by definition and it is multiplicative on a $k$-generating set, namely the set $G$. One obtains a functor $k-$ from the category of (finite) groups to the category of $k$-algebras (which are finitely generated as $k$-modules).
(b) For fixed $G$ and $n \in \mathbb{N}$, the maps
\[
\{k\text{-alg. hom. } \Gamma : kG \to \text{Mat}_n(k)\} \leftrightarrow \{\text{grp. hom. } \Delta : G \to \text{GL}_n(k)\},
\]
\[
\Gamma \mapsto \Gamma|_G,
\]
\[
\left(\sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g \Delta(g)\right) \leftrightarrow \Delta,
\]
given by restricting $\Gamma$ to $G$ and $k$-linearly extending $\Delta$ to $kG$, are mutually inverse bijections. (In category theory language one can show that the functor $k- : \text{Gr} \to k\text{Alg}$ is left adjoint to the unit group functor $U : k\text{Alg} \to \text{Gr}$, and the above bijection is the special case of this adjunction for a group $G$ and the ring $\text{Mat}_n(k)$). A $k$-algebra homomorphism $\Gamma : kG \to \text{Mat}_n(k)$ is also called a matrix representation of the $k$-algebra $kG$. Two matrix representations $\Gamma_1 : kG \to \text{Mat}_n(k)$ and $\Gamma_2 : kG \to \text{Mat}_m(k)$ are called equivalent if $m = n$ and if there exists $S \in \text{GL}_n(k)$ such that $\Gamma_2(a) = S \Gamma_1(a) S^{-1}$ for all $a \in kG$. From this it follows immediately that two matrix representations $\Gamma_1$ and $\Gamma_2$ of $kG$ are equivalent if and only if the corresponding matrix representations $\Delta_1$ and $\Delta_2$ of $G$ are equivalent. Thus, the above bijections induce mutually inverse bijections between equivalence classes:
\[
\{k\text{-alg. hom. } \Gamma : kG \to \text{Mat}_n(k)\} / \sim \leftrightarrow \{\text{grp hom. } \Delta : G \to \text{GL}_n(k)\} / \sim.
\]

(c) Let $M$ be a $kG$-module. Then, in particular, $M$ is a $k$-module via $\eta : k \to kG$. For every group element $g \in G$, the map $m \mapsto gm$ defines an element of $\text{Aut}_k(M)$, the group of $k$-module automorphisms of $M$. Altogether, one obtains this way a homomorphism $\rho : G \to \text{Aut}_k(M)$. Conversely, if $M$ is a $k$-module and if $\rho : G \to \text{Aut}_k(M)$ is a group homomorphism then we can define a $kG$-module structure on $M$ by $(\sum_{g \in G} \alpha_g g)m := \sum_{g \in G} \alpha_g (\rho(g))(m)$ for $m \in M$ and $\sum_{g \in G} \alpha_g g \in kG$. These two constructions are mutually inverse. Similarly as in (b), using $k$-linear extensions, one obtains a bijection between the set of pairs $(M, \rho)$, where $M$ is a $k$-module and $\rho : G \to \text{Aut}_k(M)$ is a group homomorphism, and the set of pairs $(M, \sigma)$, where $M$ is a $k$-module and $\sigma : kG \to \text{End}_k(M)$ is a $k$-algebra homomorphism. Thus we have natural bijections
\[
\{kG\text{-modules } M\} \leftrightarrow \{(M, \rho) \mid M \text{ k-module, } \rho : G \to \text{Aut}_k(M) \text{ hom.}\}
\]
\[
\leftrightarrow \{(M, \sigma) \mid M \text{ k-module, } \sigma : kG \to \text{End}_k(M) \text{ hom.}\}.
\]
We say that two pairs $(M, \rho)$ and $(M', \rho')$ as above are called equivalent, if there exists a $k$-module isomorphism $f : M \to M'$ such that $\rho'(g) = f^{-1} \circ \rho(g) \circ f$. 

42
\( \rho(g) \circ f \) for all \( g \in G \). Similarly, two pairs \((M, \sigma)\) and \((M', \sigma')\) are called equivalent if there exists a \( k \)-module isomorphism \( f : M \to M' \) such that \( \sigma'(a) = f^{-1} \circ \sigma(a) \circ f \) for all \( a \in kG \). It is now easy to check that two \( kG \)-modules \( M \) and \( M' \) are isomorphic if and only if the associated pairs \((M, \sigma)\) and \((M', \sigma')\) are equivalent. Consequently, we the above bijections induce bijections between isomorphism classes and equivalence classes:

\[
\{ \text{\( kG \)-modules } M \}/\sim \leftrightarrow \{ \text{\( kG \)-module hom. } \rho : G \to \text{Aut}_k(M) \}\}/\sim
\]

(d) From now on we assume that \( k = F \) is a field and fix \( n \in \mathbb{N} \). For any pair \((M, \rho)\) as in (c), consisting of an \( n \)-dimensional \( F \)-vector space \( M \) and a group homomorphism \( \rho : G \to \text{Aut}_F(M) \), we can define a representation \( \Delta : G \to \text{GL}_n(F) \) by choosing an \( F \)-basis of \( M \) and composing \( \rho \) with the isomorphism \( \text{Aut}_F(M) \to \text{GL}_n(F) \) determined by this basis. Conversely, if \( \Delta : G \to \text{GL}_n(F) \) is a representation of \( G \), we can choose any \( n \)-dimensional \( F \)-vector space \( M \) and a basis of \( M \), and use the resulting isomorphism \( \text{GL}_n(F) \to \text{Aut}_F(M) \) to define a group homomorphism \( \rho : G \to \text{Aut}_F(M) \) by composing \( \Delta \) with the described isomorphism. For each of these constructions, different choices of \( M \) and/or bases, lead to equivalent results. Therefore, altogether we obtain a bijection between equivalence classes,

\[
\{ \text{\( n \)-dim. } F \text{-vector space, } \rho : G \to \text{Aut}_F(M) \text{ hom.} \}/\sim \leftrightarrow \{ \text{group homomorphisms } \Delta : G \to \text{GL}_n(F) \}/\sim.
\]

Composing this with the previous bijection from (c), we obtain a bijection, for fixed \( G \) and \( n \),

\[
\{ \text{\( FG \)-modules } M \text{ with } \dim_F M = n \}/\sim \leftrightarrow \{ \text{group homomorphisms } \Delta : G \to \text{GL}_n(F) \}/\sim.
\]

If, under this last bijection, \( \Delta_1 \) and \( \Delta_2 \) correspond to \( M_1 \) and \( M_2 \) (for dimensions \( n_1 \) and \( n_2 \)), then \( \Delta_1 \oplus \Delta_2 \) corresponds to \( M_1 \oplus M_2 \). Moreover, if \( \Delta \) corresponds to \( M \) then we have

\[
M \text{ is indecomposable (resp. irreducible)} \iff \Delta \text{ is indecomposable (resp. irreducible)}.
\]
(e) Assume that $FG$-modules $M_1$ and $M_2$ of dimension $n_1$ and $n_2$ correspond to representations $\Delta_1 : G \to \text{GL}_{n_1}(F)$ and $\Delta_2 : G \to \text{GL}_{n_2}(F)$, respectively, via a choice of $F$-bases for $M_1$ and $M_2$. Then one obtains an isomorphism of $F$-vector spaces

$$\text{Hom}_{FG}(M_1, M_2) \sim \{ S \in \text{Mat}_{n_2 \times n_1}(F) \mid S\Delta_1(g) = \Delta_2(g)S \text{ for all } g \in G \},$$

by mapping a homomorphism $f$ to the representing matrix of $f$ with respect to the chosen bases of $M_1$ and $M_2$. In particular, if $M$ is an $FG$-module and if $\Delta : G \to \text{GL}_n(F)$ is a corresponding representation then one has an isomorphism of $F$-algebras

$$\text{End}_{FG}(M) \sim \{ S \in \text{Mat}_n(F) \mid S\Delta(g) = \Delta(g)S \text{ for all } g \in G \}.$$

(f) For $F = \mathbb{C}$ we obtain bijections

$$\begin{align*}
\{ \text{finite dimensional } \mathbb{C}G\text{-modules} \}/\text{isom.} & \sim \{ \text{representations of } G \text{ over } \mathbb{C} \}/\text{equiv.} \\
& \sim \{ \text{characters of } G \}.
\end{align*}$$

If $M$ is a finite-dimensional $\mathbb{C}G$-module, $\Delta : G \to \text{GL}_n(\mathbb{C})$ is a corresponding representation and $\chi$ is the corresponding character then we also write $\chi = \chi_M$ and say that $\chi$ is afforded by $M$ and by $\Delta$. Note that, for $g \in G$, the character value $\chi_M(g)$ is the trace of the $\mathbb{C}$-linear map $M \to M, m \mapsto gm$.

The character of the regular $\mathbb{C}G$-module, i.e., the $\mathbb{C}G$-module $\mathbb{C}G$, is equal to the regular character.

The trivial character is afforded by the trivial $\mathbb{C}G$-module, namely the module $\mathbb{C}$ with $g \cdot \alpha = \alpha$ for $g \in G$ and $\alpha \in \mathbb{C}$.

More generally, if $\phi : G \to \mathbb{C}^\times$ is a linear character (character of degree 1) then $\phi$ is afforded by the $\mathbb{C}G$-module $\mathbb{C}_\phi$ which is defined to be equal to $\mathbb{C}$ as $\mathbb{C}$-space, and whose $\mathbb{C}G$-module structure is determined by $g \cdot \alpha := \phi(g)\alpha$, for $g \in G$ and $\alpha \in \mathbb{C}$.

5.7 Lemma (Schur) Let $R$ be a ring and let $M$ be a simple $R$-module. Then the ring $\text{End}_R(M)$ is a division ring, i.e., every non-zero element is invertible.

Proof Let $0 \neq f \in \text{End}_R(M)$. We need to show that $f$ is injective and surjective. Since $f \neq 0$, we obtain $\text{im}(f) \neq \{0\}$. Since $\text{im}(f)$ is an $R$-submodule of $M$ and since $M$ is simple, we obtain $\text{im}(f) = M$ and $f$ is invertible.
surjective. Moreover, since \( f \neq 0 \), we obtain \( \ker(f) \neq M \). Since \( \ker(f) \) is an \( R \)-submodule of \( M \) and since \( M \) is simple, we obtain \( \ker(f) = \{0\} \) and \( f \) is injective. Thus, \( f \) is an isomorphism and the proof is complete.

5.8 Remark The version of Schur’s lemma in 2.1(b) can be derived from the more general version in 5.7. In fact, let \( \Delta \) be an irreducible representation of \( G \) over \( \mathbb{C} \) and let \( M \) be a corresponding \( \mathbb{C}G \)-module. By 5.7, the finite-dimensional \( \mathbb{C} \)-algebra \( D := \text{End}_{\mathbb{C}G}(M) \) is a division ring. We can view \( \mathbb{C} \) as a subfield of \( D \) via the structural homomorphism \( \eta \). The version in 2.1 amounts to the statement \( \mathbb{C} = D \). So let \( d \in D \). We will show that \( d \in \mathbb{C} \).

5.9 Definition Let \( R \) be a ring.

(a) An \( R \)-module \( M \) is called \textit{semisimple}, if for every submodule \( U \) of \( M \) there exists a submodule \( V \) of \( M \) such that \( U \oplus V = M \).

(b) The ring \( R \) is called \textit{semisimple}, if every \( R \)-module is semisimple.

5.10 Theorem (Maschke) Let \( F \) be a field. The group algebra \( FG \) is semisimple if and only if \( |G| \) is invertible in \( F \).

Proof First assume that \( |G| \) is invertible in \( F \), let \( M \) be an \( FG \)-module and let \( U \) be an \( FG \)-submodule of \( M \). We follow the idea of the proof of Theorem 1.9. Let \( W \) be an \( F \)-subspace of \( M \) such that \( U \oplus W = M \). We denote by \( p: M \to U \) the projection map with respect to the decomposition \( M = U \oplus W \). Thus, \( p \) is \( F \)-linear, but not necessarily and \( FG \)-module homomorphism. Define

\[
p'(M) \to M, \quad m \mapsto \frac{1}{|G|} \sum_{g \in G} gp(g^{-1}m).
\]

Then it is easy to see that \( p' \in \text{Hom}_{FG}(M, M) \), \( p'(M) \subseteq U \), \( p'|_U = \text{id}_U \), and \( p' \circ p' = p' \). From this it follows quickly that \( V := \ker(p') \) is an \( FG \)-submodule of \( M \) satisfying \( M = U \oplus V \).

Next assume \( FG \) is semisimple and that \( \text{char}(F) = p > 0 \) and \( p \) divides \( |G| \). We will derive a contradiction. Let \( M := FG \) be the regular left \( FG \)-module and let \( u := \sum_{g \in G} g \in M \). Then \( Fu \) is an \( FG \)-submodule of
\[ M. \text{ In fact, for every } g \in G \text{ one has } gu = u \text{ and therefore } (\sum_{g \in G} \alpha_g g)u = (\sum_{g \in G} \alpha_g)u. \text{ It also follows that } u^2 = |G|u = 0. \text{ Since } FG \text{ is semisimple, there exists a submodule } V \text{ of } FG \text{ such that } U \oplus V = FG. \text{ Write } 1 = \alpha u + v \text{ with } \alpha \in \mathbb{C} \text{ and } v \in V. \text{ Then } u = u1 = \alpha u^2 + uv = 0 + uv \text{ with } uv \in V, \text{ since } V \text{ is an } FG\text{-submodule. This implies that } u \in U \cap V = \{0\} \text{ and that } u = 0. \text{ This is a contradiction.} \]

Note that, for an arbitrary commutative ring \( k \) and an arbitrary \( kG \)-module \( M \), one has: \( M \) is finitely generated as \( kG \)-module if and only if \( M \) is finitely generated as \( k \)-module. (See Exercise 3)

5.11 Corollary Let \( F \) be a field such that \(|G|\) is invertible in \( F \). Every non-zero finitely generated \( FG \)-module \( M \) can be decomposed into a direct sum of simple submodules.

Proof We prove the result by induction on \( \dim_F M \). If \( \dim_F M = 1 \) then \( M \) is clearly simple. Now assume that \( \dim_F M = n > 1 \) and that the result holds for modules of smaller dimension. If \( M \) is simple we are done. If \( M \) is not simple then there exists a submodule \( M_1 \) of \( M \) which is different from \( \{0\} \) and \( M \). By Theorem 5.10, there exists a submodule \( M_2 \) of \( M \) such that \( M = M_1 \oplus M_2 \). By induction, both \( M_1 \) and \( M_2 \) can be written as a direct sum of simple submodules. Thus, \( M \) can be written in this form.

The following theorem is an explicit version of Wedderburn’s Theorem for the semisimple ring \( \mathbb{C}G \).

5.12 Theorem Let \( G \) be a finite group, let \( \Delta_1, \ldots, \Delta_k \) be representatives of the equivalence classes of irreducible representations of \( G \) over \( \mathbb{C} \), and let \( n_1, \ldots, n_k \in \mathbb{N} \) denote their respective degrees. Then the map

\[
\Phi: \mathbb{C}G \to \text{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \text{Mat}_{n_k}(\mathbb{C}), \quad \sum_{g \in G} \alpha_g g \mapsto \left( \sum_{g \in G} \alpha_g \Delta_1(g), \ldots, \sum_{g \in G} \alpha_g \Delta_k(g) \right)
\]

is an isomorphism of \( \mathbb{C} \)-algebras with inverse

\[
\Psi: (A_1, \ldots, A_k) \mapsto \frac{1}{|G|} \sum_{g \in G} \left( \sum_{i=1}^{k} n_i \text{tr}(\Delta_i(g^{-1})A_i) \right)g.
\]
Proof\ Clearly, \( \Phi \) and \( \Psi \) are \( \mathbb{C} \)-linear maps. Moreover, it is easy to check that \( \Phi \) is multiplicative on the basis elements \( g \in G \). Therefore, \( \Phi \) is a \( \mathbb{C} \)-algebra homomorphism. Note also that both sides of the map have the same dimension, since \( |G| = n_1^2 + \cdots + n_k^2 \). To see that \( \Phi \) is bijective and that \( \Psi \) is its inverse it suffices to show that \( \Psi(\Phi(a)) = a \) for all \( a \in \mathbb{C}G \). And it suffices to show this for the basis elements \( a = h \in G \). But, with \( \chi_i \) denoting the character of \( \Delta_i \), we have

\[
\Psi(\Phi(h)) = \Psi\left(\Delta_1(h), \ldots, \Delta_k(h)\right) = \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^k n_i \text{tr}(\Delta_i(g^{-1})\Delta_i(h))\right)
\]

with \( \sum_{i=1}^k n_i \chi_i = \rho_G \), the regular character of \( G \), by Proposition 2.11. Thus, we obtain \( \Psi(\Phi(h)) = h \), since \( \rho_G(g^{-1}h) = 0 \) if \( g \neq h \) and \( \rho_G(g^{-1}h) = |G| \) if \( g = h \).

5.13 Remark\ Let \( \Delta_1, \ldots, \Delta_k \) and \( n_1, \ldots, n_k \) be as in Theorem 5.12 and let \( \chi_1, \ldots, \chi_k \) denote the respective characters of \( \Delta_1, \ldots, \Delta_k \).

(a) Note that the \( \mathbb{C} \)-algebra \( A := \text{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \text{Mat}_{n_k}(\mathbb{C}) \) has central idempotents \( \varepsilon_i := (0, \ldots, 0, I_{n_i}, 0, \ldots, 0) \). Moreover \( \varepsilon_1 + \cdots + \varepsilon_k = 1_A \) and \( \varepsilon_i \varepsilon_j = 0 \) for \( i \neq j \) in \( \{1, \ldots, k\} \). Applying the \( \mathbb{C} \)-algebra isomorphism \( \Psi \) from Theorem 5.12 we obtain central idempotents

\[
e_i := \Psi(\varepsilon_i) = \frac{1}{|G|} \sum_{g \in G} \left(\sum_{i=1}^k n_i \chi_i(g^{-1})\right)g = \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g \in \mathbb{C}G.
\]

Thus, \( e_i^2 = e_i \), \( e_i e_j = 0 \), \( e_i a = ae_i \) and \( e_1 + \cdots + e_k = 1_{\mathbb{C}G} \), for all \( i \in \{1, \ldots, k\} \), all \( i \neq j \) in \( \{1, \ldots, k\} \), and all \( a \in \mathbb{C}G \). Since \( e_i e_j = 0 \) for \( i \neq j \), the elements \( e_1, \ldots, e_k \) are \( \mathbb{C} \)-linearly independent. Since \( \dim_{\mathbb{C}} Z(\mathbb{C}G) = k \) (see Exercise 1), these elements form a \( \mathbb{C} \)-basis of \( Z(\mathbb{C}G) \). The element \( e_i \) is called the \textit{central idempotent} associated with \( \chi_i \).

(b) Let \( M \) be a finitely generated \( \mathbb{C}G \)-module. Then the above properties of the elements \( e_1, \ldots, e_k \) imply immediately that

\[
M = e_1 M \oplus \cdots \oplus e_k M
\]

is a direct sum decomposition into \( \mathbb{C}G \)-submodules.
Recall: Let $M$ be a finitely generated $\mathbb{C}G$-modules. Then the character $\chi_M$ of $M$ is the character of any representation of $G$ which corresponds to $M$ under the constructions in Remark 5.6(d). In other words, for $g \in G$, $\chi_M(g)$ is defined as the trace of a representing matrix of the $\mathbb{C}$-linear map $M \to M$, $m \mapsto gm$, with respect to any $\mathbb{C}$-basis of $M$.

5.14 Theorem  Let $M$ be an irreducible $\mathbb{C}G$-module, let $\text{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ and let $e_1, \ldots, e_k \in Z(\mathbb{C}G)$ be the respective associated idempotents. For all $m \in M$ and $i \in \{1, \ldots, k\}$ one has

$$e_i m = \begin{cases} m & \text{if } \chi_M = \chi_i, \\ 0 & \text{if } \chi_M \neq \chi_i. \end{cases}$$

Proof Since $M$ is an irreducible $\mathbb{C}G$-module, we have $\chi_M = \chi_j$ for some $j \in \{1, \ldots, k\}$. Let $m_1, \ldots, m_{n_j}$ be a $\mathbb{C}$-basis of $M$ and let $\Delta_j : G \to \text{GL}_{n_j}(\mathbb{C})$ denote the corresponding representation, i.e., $\Delta_j(g)$ is the representing matrix of the $\mathbb{C}$-linear map $M \to M$, $m \mapsto gm$, for all $g \in G$. Then, $\chi_j = \chi_M = \chi_\Delta$. For $m = \alpha_1 m_1 + \cdots + \alpha_{n_j} m_{n_j}$ we have

$$e_i m = \left( \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1})g \right) m$$

$$= (m_1, \ldots, m_{n_j}) \left( \frac{\chi_i(1)}{|G|} \sum_{g \in G} \chi_i(g^{-1}) \Delta_j(g) \right) \left( \begin{array}{c} \alpha_1 \\ \vdots \\ \alpha_{n_j} \end{array} \right) =: A_j \in \text{Mat}_{n_j}(\mathbb{C}).$$

By the definition of the map $\Phi$ in Theorem 5.12, the matrix $A_j$ is equal to the $j$-th entry in the tuple $\Phi(e_i) = \varepsilon_i$. Thus, $A_j = I_{n_j}$ if $i = j$, and $A_j = 0$ if $i \neq j$. Now the result follows.

5.15 Corollary Let $S_1, \ldots, S_k$ denote a set of representatives of the isomorphism classes of simple $\mathbb{C}G$-modules, let $\chi_1, \ldots, \chi_k$ denote their respective characters and $e_1, \ldots, e_k \in \mathbb{C}G$ their respective central idempotents. Let $M$ be a finitely generated $\mathbb{C}G$-module and let $M = M_1 \oplus \cdots \oplus M_r$ be a decomposition of $M$ into simple submodules. For each $i \in \{1, \ldots, k\}$ one has

$$e_i M = \bigoplus_{s \in \{1, \ldots, r\} : M_s \cong S_i} M_s$$

48
and
\[(\chi_M, \chi_i) = \frac{1}{\chi_i(1)} \dim_C (e_i M).\]

In particular, every submodule \( S \) of \( M \) which is isomorphic to \( S_i \) is contained in \( e_i M \). The submodule \( e_i M \) of \( M \) is called the \( \chi_i \)-isotypic (or \( \chi_i \)-homogeneous) component of \( M \).

**Proof** This follows immediately from Theorem 5.14

---

**Exercises**

1. Let \( R \) be a commutative ring and let \( G \) be a finite group. Moreover, let \( C_1, \ldots, C_k \) denote the conjugacy classes of \( G \) and set \( e_i := \sum_{g \in C_i} g \in RG \) for \( i = 1, \ldots, k \).
   
   (a) Show that \( (c_1, \ldots, c_k) \) is an \( R \)-basis of \( Z(RG) \).

   (b) Show that the structure constants of \( Z(RG) \) (i.e., the unique elements \( a_{ijm} \in R \) satisfying \( c_i c_j = \sum_{m=1}^{k} a_{ijm} c_m \)) with respect to the basis \( c_1, \ldots, c_k \) are given by
   
   \[ a_{ijm} = |\{(x, y) \in C_i \times C_j \mid xy = z\}|, \]
   
   where \( z \in C_m \) is a fixed element.

   (c) Let \( \Gamma : \mathbb{C}G \to \text{Mat}_n(\mathbb{C}) \) be a \( \mathbb{C} \)-algebra homomorphism whose restriction to \( G \) is an irreducible representation. Show that \( \Gamma(Z(\mathbb{C}G)) = \mathbb{C} \cdot 1_n \).

2. Let \( K := \mathbb{Q}(\zeta) \) with \( \zeta := e^{2\pi i/3} \) and let \( G := \text{Sym}(3) \). Show that the multiplication by \( \zeta \) and complex conjugation define a \( \mathbb{Q}G \)-module structure on \( K \). Compute a corresponding representation and its character.

3. Let \( k \) be a commutative ring, let \( G \) be a finite group, and let \( M \) be a \( kG \)-module. Show that \( M \) is finitely generated as \( kG \)-module if and only if \( M \) is finitely generated as \( k \)-module.

4. Let \( k \) be a commutative ring, let \( G \) be a finite group and let \( S \) be a finite \( G \)-set.
   
   (a) Set \( M := kS \), the free \( k \)-module with \( k \)-basis \( S \). Construct a \( kG \)-module structure on \( M \).

   (b) Show that the character of \( M \) is given by the function
   
   \[ \chi_S : g \mapsto |\{s \in S \mid gs = s\}|, \]
Note that this gives a new way to construct characters. Such characters are called \textit{permutation characters}.

(c) Assume that \( k = \mathbb{C} \). Show that the scalar product \((\chi_S, 1)\) of \( \chi_S \) with the trivial character equals the number of orbits of \( S \).

5. Let \( G \) be a finite group and let \( M \) and \( N \) be two finitely generated \( \mathbb{C}G \)-modules. Show that

\[
(\chi_M, \chi_N) = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(M, N).
\]

(Hint: Reduce to the case that \( M \) and \( N \) are irreducible.)

6. Let \( G \) be a finite group and let \( M \) and \( N \) be finitely generated \( \mathbb{C}G \)-modules.

(a) Show that \( M^* := \text{Hom}_{\mathbb{C}}(M, \mathbb{C}) \) is a finitely generated \( \mathbb{C}G \)-module via \((g \cdot f)(m) := f(g^{-1}m)\), and show that \( \chi_{M^*} = \overline{\chi_{M}} \). (Taking duals corresponds to taking contragredient representations, and taking complex conjugate characters.)

(b) Show that the \( \mathbb{C} \)-vector space \( V := \text{Hom}_{\mathbb{C}}(M, N) \) becomes a \( \mathbb{C}G \)-module via

\[
(g \cdot f)(m) := gf(g^{-1}m)
\]

for \( g \in G, f \in V, m \in M \), and that \( \chi_V = \overline{\chi_{M}} \cdot \chi_N \).
6 The Tensor Product

In this section we first recall the definition and basic properties of the tensor product (without proofs). It will be applied at the end of the section to construct the irreducible characters of the direct product group $G \times H$ from the irreducible characters of $G$ and of $H$. Throughout this section, $R$, $S$, and $T$ denote rings.

6.1 Definition Let $M$ be a right $R$-module, let $N$ be a left $R$-module, and let $A$ be an abelian group. A map $\beta : M \times N \to A$ is called biadditive, if

$$\beta(m + m', n) = \beta(m, n) + \beta(m', n) \quad \text{and} \quad \beta(m, n + n') = \beta(m, n) + \beta(m, n'),$$

for all $m, m' \in M$ and all $n, n' \in N$. The map $\beta$ is called $R$-balanced if

$$\beta(mr, n) = \beta(m, rn),$$

for all $m \in M$, $n \in N$ and $r \in R$. (Note that for the definition of "biadditive" it would have been enough to assume that $M$ and $N$ are abelian groups.)

6.2 Definition Let $M$ be a right $R$-module and let $N$ be a left $R$-module. A tensor product of $M$ and $N$ over $R$ is a pair $(T, \tau)$ consisting of an abelian group $T$ together with an $R$-balanced, biadditive map $\tau : M \times N \to T$ satisfying the following universal property:

If $(A, \beta)$ is a pair consisting of an abelian group $A$ and an $R$-balanced, biadditive map $\beta : M \times N \to A$ then there exists a unique group homomorphism $f : T \to A$ such that the diagram

$$\begin{array}{ccc}
T & \xrightarrow{\tau} & M \times N \\
\downarrow & & \downarrow \beta \\
A & \xrightarrow{f} & \\
\end{array}$$

commutes.

6.3 Theorem Let $M$ be a right $R$-module and let $N$ be a left $R$-module.

(a) There exists a tensor product $(T, \tau)$ of $M$ and $N$ over $R$.

(b) If both $(T, \tau)$ and $(T', \tau')$ are tensor products of $M$ and $N$ over $R$ then the unique homomorphism $f : T \to T'$ such that the diagram
The universal property implies that $M \otimes_R N$ is generated as abelian group by elements of the form $m \otimes n$ with $m \in M$ and $n \in N$. Using the fourth of the above rules, one obtains that every element $x \in M \otimes_R N$ can be written in the form

$$x = (m_1 \otimes n_1) + \cdots + (m_s \otimes n_s)$$

with $s \in \mathbb{N}$, $m_1, \ldots, m_s \in M$ and $n_1, \ldots, n_s \in N$. Warning: The elements $s \in \mathbb{N}$, $m_1, \ldots, m_s \in M$ and $n_1, \ldots, n_s \in N$ are not uniquely determined by $x$.

**6.5 Proposition** Let $M$ and $M'$ be right $R$-modules, let $N$ and $N'$ be left $R$-modules, and let $f : M \to M'$ and $g : N \to N'$ be $R$-module homomorphisms. Then there exists a unique homomorphism $h : M \otimes_R N \to M' \otimes_R N'$ such that $h(m \otimes n) = f(m) \otimes g(n)$ for all $m \in M$ and $n \in N$. This homomorphism is denoted by $f \otimes g$. Thus, $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$ for all $m \in M$ and $n \in N$.

**6.6 Remark** (a) Recall that an $(R,S)$-bimodule $M$ is an abelian group which is a left $R$-module and a right $S$-module such that $(rm)s = r(ms)$
for all \( r \in R, s \in S \) and \( m \in M \). If \( M \) is an \((R,S)\)-bimodule and \( N \) is an \((S,T)\)-bimodule then the abelian group \( M \otimes_S N \) has a unique \((R,T)\)-bimodule structure satisfying \( r(m \otimes n) = (rm) \otimes n \) and \((m \otimes n)t = m \otimes (nt)\) for \( r \in R, t \in T, m \in M \) and \( n \in N \).

(b) Let \( k \) be a commutative ring. Every left (resp. right) \( k \)-module \( M \) is automatically a \((k,k)\)-bimodule via \( m \alpha := \alpha m \) (resp. \( \alpha m := \alpha m \)), for \( \alpha \in k \) and \( m \in M \). Thus, if \( M \) and \( N \) are \( k \)-modules then \( M \otimes_k N \) is again a \( k \)-module with the module structure from Part (a).

(c) If \((A,\eta_A)\) and \((B,\eta_B)\) are \( k \)-algebras then \((A \otimes_k B,\eta)\) is again a \( k \)-algebra. The multiplication on \( A \otimes_k B \) is determined by the property \((a \otimes b)(a' \otimes b') = (aa') \otimes (bb')\), for \( a,a' \in A \) and \( b,b' \in B \). Moreover, \( \eta(\alpha) := \eta_A(\alpha) \otimes 1_B = (\alpha \cdot 1_A) \otimes 1_B = \alpha \cdot (1_A \otimes 1_B) = 1_A \otimes (\alpha \cdot 1_B) = 1_A \otimes \eta_B(\alpha)\) for \( \alpha \in k \).

(d) For finite groups \( G \) and \( H \), one has an isomorphism \( kG \otimes_k kH \cong k[G \times H] \) of \( k \)-algebras given by \( g \otimes h \mapsto (g,h) \). In fact, by the following proposition, the elements \( g \otimes h \), with \( g \in G \) and \( h \in H \), form a \( k \)-basis of \( kG \otimes_k kH \). Therefore, the above map defines a \( k \)-linear isomorphism. It is quickly checked that this is also a ring homomorphism (it suffices to check this on the basis elements).

6.7 Proposition (a) Let \( M \) be a left \( R \)-module (resp. an \((R,S)\)-bimodule). Then

\[ R \otimes_R M \cong M \]

as left \( R \)-modules (resp. \((R,S)\)-bimodules) via the map \( r \otimes m \mapsto rm \) with inverse \( m \mapsto 1_R \otimes m \), for \( r \in R \) and \( m \in M \). Similarly, if \( M \) is a right \( S \)-module (resp. an \((R,S)\)-bimodule) then

\[ M \otimes_S S \cong M \]

as right \( S \)-modules (resp. \((R,S)\)-bimodules) via the map \( m \otimes s \mapsto ms \) with inverse \( m \mapsto m \otimes 1_S \) for \( m \in M \) and \( s \in S \).

(b) Let \( M \) and \( M' \) be right \( S \)-modules (resp. \((R,S)\)-bimodules) and let \( N \) be a left \( S \)-module (resp. \((S,T)\)-bimodule). Then

\[ (M \oplus M') \otimes_S N \cong (M \otimes_S N) \oplus (M' \otimes_S N) \]

as abelian groups (resp. as \((R,T)\)-bimodules). Similarly, if also \( N' \) is a left \( S \)-module (resp. an \((S,T)\)-bimodule) then

\[ M \otimes_S (N \oplus N') \cong (M \otimes_S N) \oplus (M \otimes_S N') \]
as abelian groups (resp. as $(R,T)$-bimodules).

(c) Let $M$ be an $(R,S)$-bimodule, let $N$ be an $(S,T)$-bimodule and let $P$ be a $(T,U)$-bimodule for an additional ring $U$. Then there exists an isomorphism

$$(M \otimes_S N) \otimes_T P \cong M \otimes_S (N \otimes_T P)$$

of $(R,U)$-bimodules that maps the element $(m \otimes n) \otimes p$ to the element $m \otimes (n \otimes p)$ and whose inverse maps the element $m \otimes (n \otimes p)$ to $(m \otimes n) \otimes p$, for $m \in M$, $n \in N$ and $p \in P$.

(d) Let $M$ be a right $R$-module and let $N$ be a left $R$-module. If $M$ is free with $R$-basis $m_1, \ldots, m_d$, then every element $x \in M \otimes_R N$ can be expressed as

$$x = (m_1 \otimes n_1) + \cdots + (m_d \otimes n_d)$$

with unique elements $n_1, \ldots, n_d \in N$. Similarly, if $N$ is free with $R$-basis $n_1, \ldots, n_d$ then every element $x \in M \otimes_R N$ can be expressed as above with uniquely determined elements $m_1, \ldots, m_d \in M$.

(e) If $k$ is a commutative ring and if $M$ and $N$ are free $k$-modules with bases $m_1, \ldots, m_d$ and $n_1, \ldots, n_e$, respectively, then $M \otimes_k N$ is a free $k$-module with basis $m_i \otimes n_j$, $i = 1, \ldots, d$, $j = 1, \ldots, e$.

6.8 Remark Let $F$ be a field and let $G$ be a finite group.

(a) Let $V, V', W, W'$ be finite-dimensional $F$-vector spaces, let $f: V \to V'$ and $g: W \to W'$ be $F$-linear maps, and let $(v_1, \ldots, v_r)$, $(v'_1, \ldots, v'_s)$, $(w_1, \ldots, w_t)$, and $(w'_1, \ldots, w'_u)$ be $F$-bases of $V, V', W, W'$, respectively. Moreover, let $A \in \text{Mat}_{s \times r}(F)$ and $B \in \text{Mat}_{u \times t}(F)$ be the representing matrices of $f$ and $g$, respectively, with respect to these bases. Then $A \otimes B \in \text{Mat}_{su \times rt}(F)$ is the representing matrix of $f \otimes g: V \otimes_F W \to V' \otimes_F W'$ with respect to the bases $v_i \otimes w_j$ ($1 \leq i \leq r$, $1 \leq j \leq s$) and $v'_k \otimes w'_l$ ($1 \leq k \leq t$, $1 \leq l \leq u$) in lexicographic order.

(b) Assume now that $V$ and $W$ are finitely generated $FG$-modules. Then, $V \otimes_F W$ is again an $F$-vector space. It is even an $FG$-module with

$$(\sum_{g \in G} \alpha_g g) \cdot (v \otimes w) = \sum_{g \in G} \alpha_g (gv \otimes gw).$$

In fact, one has an $F$-algebra homomorphism

$$\delta: FG \longrightarrow FG \otimes_F FG \longrightarrow \text{End}_F(V) \otimes_F \text{End}_F(W) \longrightarrow \text{End}_F(V \otimes W)$$

54
where \( \delta \) is the \( F \)-linear extension of \( g \mapsto g \otimes g \), \( \rho \) and \( \rho' \) denote the \( F \)-algebra homomorphisms describing the \( FG \)-module structures of \( V \) and \( W \), and the last map is the \( F \)-algebra homomorphism induced by \( (f,g) \mapsto f \otimes g \). The above \( FG \)-module structure on \( V \otimes_F W \) comes from this homomorphism.

Thus, if \((v_1,\ldots,v_r)\) and \((w_1,\ldots,w_s)\) are \( F \)-bases of \( V \) and \( W \) and if \( \Delta: G \to \GL_r(F) \) and \( \Delta': G \to \GL_s(F) \) denote the representations corresponding to \( V \) and \( W \) with respect to these bases then \( \Delta \otimes \Delta': G \to \GL_{rs}(F) \), \( g \mapsto \Delta(g) \otimes \Delta'(g) \), corresponds to the \( FG \)-module \( V \otimes_F W \) with respect to the basis \( v_i \otimes w_j \) \((1 \leq i \leq r, 1 \leq j \leq s)\) in lexicographic order. In particular, since \( \text{tr}(\Delta(g) \otimes \Delta'(g)) = \text{tr}(\Delta(g))\text{tr}(\Delta'(g)) \), we obtain \( \chi_{V \otimes_F W} = \chi_V \cdot \chi_W \).

In the following definition we construct a representation of \( G \times H \) from a representation of \( G \) and a representation of \( H \).

**6.9 Definition** Let \( G \) and \( H \) be finite groups and let \( F \) be a field. If \( V \) is a finitely generated \( FG \)-module and \( W \) is a finitely generated \( FH \)-module then the \( F \)-vector space \( V \otimes_F W \) has an \( F[G \times H] \)-module structure which is uniquely determined by

\[
(g,h) \cdot (v \otimes w) = gv \otimes hw,
\]

for \((g,h) \in G \times H, v \in V \) and \( w \in W \). In fact, this module structure comes from the \( F \)-algebra homomorphism

\[
F[G \times H] \longrightarrow FG \otimes_F FH \quad \rho \otimes \rho' \longrightarrow \text{End}_F(V) \otimes_F \text{End}_F(W) \longrightarrow \text{End}_F(V \otimes_F W),
\]

where the first map is the \( F \)-linear extension of \( (g,h) \mapsto g \otimes h \), the maps \( \rho \) and \( \rho' \) denote the \( F \)-algebra homomorphisms corresponding to the module structures of \( V \) and \( W \), and the last map is induced by \((f,g) \mapsto f \otimes g \).

We will often write \( \chi_V \times \chi_W \) for the character \( \chi_{V \otimes_F W} \) of \( G \times H \). If also \( V' \) and \( W' \) are finitely generated modules for \( FG \) and \( FH \), respectively, then \( (\chi_V + \chi_V') \times \chi_W = \chi_V \times \chi_W + \chi_V' \times \chi_W \) and \( \chi_V \times (\chi_W + \chi_W') = \chi_V \times \chi_W + \chi_V \times \chi_W' \). Thus, for \( F = \mathbb{C} \), one obtains a biadditive map

\[
- \times -: R(G) \times R(H) \to R(G \times H), \quad (\chi, \psi) \mapsto \chi \times \psi,
\]

where \( (f_1 \times f_2)(g,h) := f_1(g) \cdot f_2(h) \), for arbitrary class functions \( f_1, f_2 \in CF(G, \mathbb{C}) \) and \((g,h) \in G \times H \).
6.10 Theorem Let $G$ and $H$ be finite groups, let $V$ be a finitely generated $\mathbb{C}G$-module and let $W$ be a finitely generated $\mathbb{C}H$-module. Then the following hold:

(a) One has $(\chi_V \times \chi_W)(g, h) = \chi_V(g)\chi_W(h)$.

(b) The $\mathbb{C}[G \times H]$-module $V \otimes_{\mathbb{C}} W$ is simple if and only if $V$ and $W$ are simple modules.

(c) The function $\text{Irr}(G) \times \text{Irr}(H) \mapsto \text{Irr}(G \times H)$, $(\chi, \psi) \mapsto \chi \times \psi$, is a bijection. It induces a ring isomorphism $R(G) \otimes R(H) \sim \rightarrow R(G \times H)$.

Proof Let $(v_1, \ldots, v_m)$ and $(w_1, \ldots, w_n)$ be $F$-bases of $V$ and $W$, respectively, and let $\Delta_1: G \to \text{GL}_m(F)$ and $\Delta_2: G \to \text{GL}_n(F)$ be the corresponding representations. Remark 6.8(a) implies that the representation of the $\mathbb{F}[G \times H]$-module $V \otimes_{\mathbb{F}} W$ with respect to the basis $v_i \otimes w_j$ $(1 \leq i \leq m, 1 \leq j \leq n)$ in lexicographic order is given by $(g, h) \mapsto \Delta_1(g) \otimes \Delta_2(h)$. Since $\text{tr}(A \otimes B) = \text{tr}(A)\text{tr}(B)$ for any square matrices $A$ and $B$, we obtain

$$(\chi_V \times \chi_W)(g, h) = \chi_V \otimes_{\mathbb{F}} W(g, h) = \text{tr}(\Delta_1(g) \otimes \Delta_2(h))$$
$$= \text{tr}(\Delta_1(g))\text{tr}(\Delta_2(h)) = \chi_V(g) \cdot \chi_W(h),$$

and Part (a) is proven.

Next we show that for characters $\chi, \chi'$ of $G$ and $\psi, \psi'$ of $H$, one has

$$(\chi \times \psi, \chi' \times \psi')(G \times H) = (\chi, \chi')_G \cdot (\psi, \psi')_H. \quad (6.10.a)$$

In fact, we have

$$(\chi \times \psi, \chi' \times \psi')(G \times H) = \frac{1}{|G \times H|} \sum_{(g, h) \in G \times H} (\chi \times \psi)(g, h) \cdot (\chi' \times \psi')(g^{-1}, h^{-1})$$
$$= \frac{1}{|G| \cdot |H|} \sum_{g \in G} \sum_{h \in H} \chi(g)\psi(h)\chi'(g^{-1})\psi'(h^{-1})$$
$$= \left(\frac{1}{|G|} \sum_{g \in G} \chi(g)\chi'(g^{-1})\right) \cdot \left(\frac{1}{|H|} \sum_{h \in H} \psi(h)\psi'(h^{-1})\right)$$
$$= (\chi, \chi')_G \cdot (\psi, \psi')_H.$$

For arbitrary characters $\chi$ of $G$ and $\psi$ of $H$, the irreducibility criterion in Proposition 2.18 and Equation (6.10.a) now imply the following chain of
equivalences:
\[
\chi \times \psi \in \text{Irr}(G \times H) \iff (\chi \times \psi, \chi \times \psi)_{G \times H} = 1
\]
\[
\iff (\chi, \chi)_G \cdot (\psi, \psi)_H = 1
\]
\[
\iff (\chi, \chi)_G = 1 \text{ and } (\psi, \psi)_H = 1
\]
\[
\iff \chi \in \text{Irr}(G) \text{ and } \psi \in \text{Irr}(H).
\]

This implies the statement in Part (b). It also shows that the first map in Part (c) takes values in \(\text{Irr}(G \times H)\).

Next we show that the first map in Part (c) is bijective. In order to see that it is injective, assume that \(\chi, \chi' \in \text{Irr}(G)\) and \(\psi, \psi' \in \text{Irr}(H)\) satisfy \(\chi \times \psi = \chi' \times \psi'\). Then Equation (6.10.a) implies that
\[
1 = (\chi \times \psi, \chi' \times \psi')_{G \times H} = (\chi, \chi')_G \cdot (\psi, \psi')_H,
\]
and we obtain \((\chi, \chi')_G \neq 0\) and \((\psi, \psi')_H \neq 0\). This implies \(\chi = \chi'\) and \(\psi = \psi'\).

In order to see that the first map in Part (c) is bijective it suffices now to show that \(|\text{Irr}(G \times H)| = |\text{Irr}(G)| \cdot |\text{Irr}(H)|\). This in turn is equivalent to showing that the numbers of conjugacy classes of these three groups satisfies the equation \(k(G \times H) = k(G)k(H)\). Now note that two elements \((g, h)\) and \((g', h')\) of \(G \times H\) are conjugate in \(G \times H\) if and only if \(g\) and \(g'\) are conjugate in \(G\) and \(h\) and \(h'\) are conjugate in \(H\). This implies that if \(C_1, \ldots, C_{k(G)}\) denote the conjugacy classes of \(G\) and \(D_1, \ldots, D_{k(H)}\) denote the conjugacy classes of \(H\) then \(C_i \times D_j, 1 \leq i \leq k(G), 1 \leq j \leq k(H)\), are precisely the conjugacy classes of \(G \times H\).

Finally, since the first map in Part (c) is bijective and since the sets in these maps form \(\mathbb{Z}\)-bases of the abelian groups in the second map, the second map is a group isomorphism. It is now easy to verify, using the formula in Part (a), that it is also multiplicative.

The following theorem is well-know in category theoretic terms as the adjunction between \(\text{Hom}\) and \(\otimes\). We state it here in plain language.

**6.11 Theorem** Let \(R, S, T,\) and \(U\) be rings.

(a) If \(M\) is an \((R, S)\)-bimodule and \(N\) is an \((R, T)\)-bimodule then \(\text{Hom}_R(M, N)\) is an \((S, T)\)-bimodule via \((sft)(m) := f(ms)t\) for \(f \in \text{Hom}_R(M, N), s \in S, t \in T\) and \(m \in M\).
(b) If $M$ is an $(S, R)$-bimodule and $N$ is a $(T, R)$-bimodule then $\text{Hom}_R(M, N)$ is a $(T, S)$-bimodule via $(tf)(m) := tf(sm)$ for $f \in \text{Hom}_R(M, N)$, $s \in S$, $t \in T$ and $m \in M$.

(c) If $M$ is an $(R, S)$-bimodule, $N$ is an $(S, T)$-bimodule and $P$ is an $(R, U)$-bimodule then the maps

$$\text{Hom}_R(M \otimes_S N, P) \leftrightarrow \text{Hom}_S(N, \text{Hom}_R(M, P))$$

$$f \mapsto \left(n \mapsto \left(m \mapsto f(m \otimes n)\right)\right)$$

$$(m \otimes n \mapsto (g(n))(m)) \leftrightarrow g$$

are well-defined mutually inverse isomorphisms of $(T, U)$-bimodules.

**Exercises**

1. Let $G$ be a finite group and let $M$ be a finitely generated $\mathbb{C}G$-module. Denote by $\tau: M \otimes \mathbb{C} M \to M \otimes \mathbb{C} M$ the map given by $m_1 \otimes m_2 \mapsto m_2 \otimes m_1$ for $m_1, m_2 \in M$.

   (a) Consider $M \otimes \mathbb{C} M$ as $\mathbb{C}G$-module with the diagonal action $g(m_1 \otimes m_2) = gm_1 \otimes gm_2$, for $g \in G$, $m_1, m_2 \in M$. Show that the subsets

   $$M_s := \{x \in M \otimes \mathbb{C} M \mid \tau(x) = x\} \text{ and } M_a := \{x \in M \otimes \mathbb{C} M \mid \tau(x) = -x\},$$

   the symmetric and alternating square of $M$, are $\mathbb{C}G$-submodules of $M \otimes \mathbb{C} M$ with $M_s \oplus M_a = M \otimes \mathbb{C} M$.

   (b) Let $\chi$, $\chi_s$, and $\chi_a$ be the character of $M$, $M_s$, and $M_a$, respectively. Show that

   $$\chi_s(g) = \frac{1}{2} \left(\chi^2(g) + \chi(g^2)\right) \text{ and } \chi_a(g) = \frac{1}{2} \left(\chi^2(g) - \chi(g^2)\right)$$

   for all $g \in G$. Again, this gives is a new way to construct characters.

2. Compute the character tables of $\text{Sym}(5)$ and $\text{Alt}(5)$.

3. Let $F$ be a field and let $M$ and $N$ be finitely generated $FG$-modules. Construct an $FG$-module isomorphism between $\text{Hom}_F(M, N)$ and $M^* \otimes_F N$. (The $FG$-module structures of $\text{Hom}_F(M, N)$ and $M^*$ are given in Exercise 5.6)

4. Verify the the statements in Theorem 6.11.
7 Induction

Throughout this section, $G$ denotes a finite group, $H$ denotes a subgroup of $G$, and $F$ denotes a field. Note that $FG$ is an $(FG, FH)$-bimodule.

7.1 Definition Let $W$ be an $FH$-module. The $FG$-module

$$\text{Ind}^G_H(W) := FG \otimes_{FH} W$$

is called the module induced by $W$ from $H$ to $G$, or also the induction of $W$ from $H$ to $G$.

7.2 Remark Let $W$ be a finitely generated $FH$-module and let $g_1, \ldots, g_n \in G$ denote coset representatives of $G/H$.

(a) The $F$-algebra $FG$ is free as right $FH$-module with basis elements $g_1, \ldots, g_n$. In fact, every element $\sum_{g \in G} \alpha_g g$ in $FG$ can be written as

$$\sum_{g \in G} \alpha_g g = \sum_{i=1}^n \sum_{h \in H} \alpha_{g,h} g_i h = \sum_{i=1}^n g_i \left( \sum_{h \in H} \alpha_{g,h} h \right) \in \sum_{i=1}^n g_i \cdot FH.$$ 

Moreover, if $\sum_{i=1}^n g_i \cdot x_i = 0$, with $x_i = \sum_{h \in H} \alpha_{h,i} h \in FH$, then

$$\sum_{i=1}^n \sum_{h \in H} \alpha_{h,i} g_i h = 0.$$ 

For given $i \in \{1, \ldots, n\}$ and $h \in H$, the coefficient of $g_i h$ in this element of $FG$ is equal to $\alpha_{h,i}$. Since $g_i h = g_j h'$ implies $i = j$ and $h = h'$, for $i, j \in \{1, \ldots, n\}$ and $h, h' \in H$, we have $\alpha_{h,i} = 0$. This implies $x_i = 0$ for all $i = 1, \ldots, n$. Therefore, by Proposition 6.7(d), one has an isomorphism of $F$-vector spaces

$$FG \otimes_{FH} W \cong \bigoplus_{i=1}^n W,$$

$$\sum_{i=1}^n g_i \otimes w_i \leftrightarrow (w_1, \ldots, w_n).$$

This implies

$$\dim_F \text{Ind}^G_H(W) = [G: H] \dim_F W.$$ 

(b) Let $w_1, \ldots, w_n$ be an $F$-basis of $W$, and let $\Delta : H \to \text{GL}_m(F)$ denote the corresponding representation of $H$. Then, by the isomorphism in Part (a),
the elements $g_i \otimes w_j$, $1 \leq i \leq n$, $1 \leq j \leq m$, form an $F$-basis of $FG \otimes_{FH} W$. We denote the corresponding representation (using the lexicographic order of the basis) by $\text{Ind}_H^G(\Delta)$. Our next goal is to describe the matrix $(\text{Ind}_H^G(\Delta))(g)$ for a given group element $g \in G$. We have to rewrite the element $gg_i \otimes w_j$ as linear combination of the elements $g_k \otimes w_l$. First note that $gg_i H = g_{\sigma(i)} H \in G/H$ for some $\sigma(i) \in \{1, \ldots, n\}$. This defines a permutation $\sigma_g = \sigma \in \text{Sym}(n)$ satisfying $gg_i \in g_{\sigma(i)} H$ for every $i \in \{1, \ldots, n\}$. It is the permutation induced by the action of the element $g$ by left translation on $G/H$. Thus, there exists an element $h_i \in H$ (depending on $g$) such that $gg_i = g_{\sigma(i)} h_i$.

With this we obtain

$$g(g_i \otimes w_j) = gg_i \otimes w_j = g_{\sigma(i)} h_i \otimes w_j = g_{\sigma(i)} \otimes h_i w_j.$$ 

This implies that the matrix $(\text{Ind}_H^G(\Delta))(g)$ consists of $n^2$ blocks of size $m \times m$, and that the $m \times m$ block matrix in the $i$-th block column and $k$-th block row is equal to 0 unless $k = \sigma(i)$. In the case $k = \sigma(i)$ this block matrix is equal to $\Delta(h_i) = \Delta(g_{\sigma(i)}^{-1} gg_i)$.

(c) Let $\psi$ denote the character of $W$ (or of $\Delta$). With the results from Part (b), we can compute the character of $\text{Ind}_H^G(\Delta)$ which we will denote by $\text{ind}_H^G(\psi)$. With the notation in Part (b), we obtain that

$$(\text{ind}_H^G(\psi))(g) = \sum_{i=1}^{n} \psi(g_{i}^{-1} gg_i) = \sum_{g_{i}^{-1} gg_i \in H} \psi(g_{i}^{-1} gg_i)$$

$$= \sum_{g_i \in G/H} \hat{\psi}(g_{i}^{-1} gg_i) = \frac{1}{|H|} \sum_{x \in G} \hat{\psi}(x^{-1} gx)$$

with

$$\hat{\psi}: G \to F, \quad g \mapsto \begin{cases} \psi(g) & \text{if } g \in H, \\ 0 & \text{if } g \notin H. \end{cases}$$

(d) By Proposition 6.7(b), we have

$$\text{Ind}_H^G(W \oplus W') \cong \text{Ind}_H^G(W) \oplus \text{Ind}_H^G(W')$$

if also $W'$ is a finitely generated $FH$-module. In the case that $F = \mathbb{C}$, this implies that we obtain a group homomorphism

$$\text{ind}_H^G: R(H) \to R(G), \quad \chi \mapsto \text{ind}_H^G(\chi),$$

60
between the character rings.

Now let $K \leq H \leq G$ and assume that $W$ is a finitely generated $\mathbb{C}K$-module. Parts (a) and (c) in Proposition 6.7 imply that we have a chain of isomorphisms of left $\mathbb{C}G$-modules,

\[ \text{Ind}_H^G(\text{Ind}_K^H(W)) = \mathbb{C}G \otimes_{\mathbb{C}H} (\mathbb{C}H \otimes_{\mathbb{C}K} W) \cong \mathbb{C}G \otimes_{\mathbb{C}H} (\mathbb{C}H \otimes_{\mathbb{C}K} W) \cong \mathbb{C}G \otimes_{\mathbb{C}K} W = \text{Ind}_K^G(W). \]

This transitivity property of induction for modules implies the transitivity property of induction for characters:

\[ \text{ind}_H^G \circ \text{ind}_K^H = \text{ind}_K^G : R(K) \to R(G) \]

whenever $K \leq H \leq G$.

7.3 Example Let $G = \text{Sym}(3) = \{1, x, x^2, y, xy, x^2y\}$ with $x = (1, 2, 3)$ and $y = (1, 2)$ and let $H := \text{Alt}(3) = \{1, x, x^2\} \leq G$. The character table of $H$ is given by

\[
\begin{array}{c|ccc}
\psi & 1 & x & x^2 \\
\hline
\psi_1 & 1 & 1 & 1 \\
\psi_2 & 1 & \zeta & \zeta^2 \\
\psi_3 & 1 & \zeta^2 & \zeta \\
\end{array}
\]

with $\zeta := e^{2\pi i/3}$. The elements 1 and $y$ form a set of coset representatives for $G/H$ and we can compute the character values of $\text{ind}_H^G(\psi)$ for the various $\psi \in \text{Irr}(H)$ using the formula in Remark 7.2(c). Note that $y^{-1}xy = x^2$. We include the computations of these characters in the character table of $G$:

\[
\begin{array}{c|ccc}
& 1 & y & x \\
\hline
\chi_1 & 1 & 1 & 1 \\
\chi_2 & 1 & -1 & 1 \\
\chi_3 & 2 & 0 & -1 \\
\hline
\text{ind}_H^G(\psi_1) & 2 & 0 & 2 \\
\text{ind}_H^G(\psi_2) & 2 & 0 & -1 \\
\text{ind}_H^G(\psi_3) & 2 & 0 & -1 \\
\end{array}
\]

Now it is easy to see that

\[ \text{ind}_H^G(\psi_1) = \chi_1 + \chi_2, \quad \text{ind}_H^G(\psi_2) = \chi_3, \quad \text{ind}_H^G(\psi_3) = \chi_3. \]
7.4 Proposition Let $V$ and $W$ be $\mathbb{C}G$-modules and let $\chi_V$ and $\chi_W$ denote their respective characters. Then

$$(\chi_V, \chi_W)_G = \dim \mathbb{C} \Hom_{\mathbb{C}G}(V, W).$$

Proof Exercise 5.5. Hint: Both sides of the equation are additive in $V$ and $W$ with respect to direct sums. Therefore, it suffices to prove the equation for simple $\mathbb{C}G$-modules $V$ and $W$. But in this case this follows immediately from distinguishing the two cases that $V$ is isomorphic to $W$ or not.

7.5 Theorem (Frobenius reciprocity) For $\psi \in R(H)$ and $\chi \in R(G)$ one has

$$(\text{ind}^G_H(\psi), \chi)_G = (\psi, \text{res}^G_H(\chi))_H.$$ 

Proof Since $(-, -)$ is additive in both arguments, and since $\text{ind}^G_H$ and $\text{res}^G_H$ are group homomorphisms, it suffices to prove the equation for irreducible characters $\psi$ and $\chi$. In this case there exists a $\mathbb{C}G$-module $V$ and a $\mathbb{C}H$-module $W$ such that $\chi = \chi_V$ and $\psi = \chi_W$. By Proposition 7.4, we have

$$(\text{ind}^G_H(\psi), \chi)_G = \dim \mathbb{C} \Hom_{\mathbb{C}G}(\mathbb{C}G \otimes_{\mathbb{C}H} W, V)$$

and

$$(\psi, \text{res}^G_H(\chi))_H = \dim \mathbb{C} \Hom_{\mathbb{C}H}(W, \text{Res}^G_H(V)).$$

Therefore, it suffices to show that the $\mathbb{C}$-vector spaces $\Hom_{\mathbb{C}G}(\mathbb{C}G \otimes_{\mathbb{C}H} W, V)$ and $\Hom_{\mathbb{C}H}(W, \text{Res}^G_H(V))$ are isomorphic. Note that one has well-defined mutually inverse isomorphisms

$$\Hom_{\mathbb{C}G}(\mathbb{C}G, V) \xrightarrow{\sim} \text{Res}^G_H(V)$$

$$f \mapsto f(1)$$

$$(a \mapsto av) \leftarrow v$$

of $\mathbb{C}H$-modules, where the left $\mathbb{C}H$-module structure of $\Hom_{\mathbb{C}G}(\mathbb{C}G, V)$ comes from the right $\mathbb{C}H$-module structure of $\mathbb{C}G$, cf. Theorem 6.11(a). Therefore, it suffices to show that the $\mathbb{C}$-vector spaces $\Hom_{\mathbb{C}G}(\mathbb{C}G \otimes_{\mathbb{C}H} W, V)$ and $\Hom_{\mathbb{C}H}(W, \Hom_{\mathbb{C}G}(\mathbb{C}G, V))$ are isomorphic. But this is precisely the content of Theorem 6.11(c).
7.6 Example  Let $G = \text{Sym}(4)$. The character table of $G$ is given by

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>(ab)(cd)</th>
<th>(ab)</th>
<th>(abc)</th>
<th>(abcd)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_2$</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>3</td>
<td>-1</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>3</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

(a) Let $H := \text{Sym}(3) \leq G$. The character table of $H$ together with the restrictions $\chi_i|_H$ of the irreducible characters of $G$ is given below:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>(ab)</th>
<th>(abc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi_1$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\psi_2$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$\psi_3$</td>
<td>2</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$\text{res}^G_H(\chi_1)$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\text{res}^G_H(\chi_2)$</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$\text{res}^G_H(\chi_3)$</td>
<td>2</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>$\text{res}^G_H(\chi_4)$</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$\text{res}^G_H(\chi_5)$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

It follows immediately that

$\text{res}^G_H(\chi_1) = \psi_1$
$\text{res}^G_H(\chi_2) = \psi_2$
$\text{res}^G_H(\chi_3) = \psi_3$
$\text{res}^G_H(\chi_4) = \psi_1 + \psi_3$
$\text{res}^G_H(\chi_5) = \psi_2 + \psi_3$

Frobenius reciprocity now immediately implies that

$\text{ind}^G_H(\psi_1) = \chi_1 + \chi_4$
$\text{ind}^G_H(\psi_2) = \chi_2 + \chi_5$
$\text{ind}^G_H(\psi_3) = \chi_3 + \chi_4 + \chi_5$

7.7 Theorem (Frobenius property)  For $\psi \in R(H)$ and $\chi \in R(G)$ one has

$\text{ind}^G_H(\psi) \cdot \chi = \text{ind}^G_H(\psi \cdot \text{res}^G_H(\chi))$.

In particular, $\text{ind}^G_H(R(H))$ is an ideal in the commutative ring $R(G)$.  

63
Proof For \( g \in G \) we have

\[
(\text{ind}_H^G(\psi) \cdot \chi)(g) = (\text{ind}_H^G(\psi))(g) \cdot \chi(g) = \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \psi(x^{-1}gx) \chi(g)
\]

and

\[
\text{ind}_H^G(\psi \cdot \text{res}_H^G(\chi))(g) = \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} (\psi \cdot \text{res}_H^G(\chi))(x^{-1}gx)
\]

\[
= \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \psi(x^{-1}gx) \cdot \chi(x^{-1}gx)
\]

\[
= \frac{1}{|H|} \sum_{x \in G, x^{-1}gx \in H} \psi(x^{-1}gx) \chi(g).
\]

This completes the proof of the theorem.

7.8 Definition Let \( H \) and \( U \) be subgroups of \( G \). A double coset of \( G \) with respect to \( U \) and \( H \) is an equivalence class for the equivalence relation on \( G \) defined by

\[
g \sim g' : \iff \text{there exist } u \in U \text{ and } h \in H \text{ such that } g' = ugh.
\]

The double coset of \( g \), i.e., the set of all elements \( g' \in G \) which are equivalent to \( g \), is \( UgH = \{ ugh \mid u \in U, h \in H \} \). We write \( U \backslash G / H := \{ UgH \mid g \in G \} \) for the set of double cosets of \( G \) with respect to \( U \) and \( H \).

7.9 Remark Let \( U \) and \( H \) be subgroups of \( G \). For an element \( g \in G \) we set \( ^gH := gHg^{-1} \) and \( H^g := g^{-1}Hg \).

(a) In the sequel, by abuse of notation, a summation of the form \( \sum_{g \in U \backslash G / H} \) means that the elements \( g \) run through a set of double coset representatives of \( G \) with respect to \( U \) and \( H \).

(b) Every double coset in \( UgH \in U \backslash G / H \) is a disjoint union of left cosets in \( G / H \) and also a disjoint union of right cosets in \( U \backslash G \). If \( \{ g_1, \ldots, g_n \} \subseteq G \) is a set of representatives of the double cosets of \( G \) with respect to \( U \) and \( H \) then \( \{ g_1^{-1}, \ldots, g_n^{-1} \} \) is a set of representatives of the double cosets of \( G \).
with respect to $H$ and $U$. In fact, the bijection $G \to G$, $g \mapsto g^{-1}$, maps the double coset $UgH$ to the double coset $Hg^{-1}U$. Moreover, if $U$ is normal in $G$ then $UH$ is a subgroup of $G$ and $UgH = gUH$ for all $g \in G$. Therefore $U \backslash G/H = G/\!\!\!\backslash UH$. Similarly, if $H$ is normal in $G$ then $U \backslash G/H = U \backslash G/\!\!\!\backslash H$.

(c) Let $F$ be a field. Then
\[
FG = \bigoplus_{g \in U \backslash G/H} F[UgH]
\]
is a decomposition of the $(FU, FH)$-bimodule $FG$ into $(FU, FH)$-subbimodules.

(d) Let $F$ be a field, let $W$ be an $FH$-module and let $g \in G$. We set
\[
_qW := \text{Res}_{g^{-1}}(W),
\]
the restriction of $W$ along the isomorphism
\[
c_{g^{-1}} : \quad ^gH \xrightarrow{\sim} H, \quad x \mapsto g^{-1}xg.
\]
In other words, the $F^gH$-module $qW$ is equal to $W$ as an $F$-vector space, and for $x \in ^gH$ and $w \in qW$ one has $x \cdot w = (g^{-1}xg)w$. If $\psi \in R(H)$ denotes the character of $W$ then the character of $qW$ is denoted by $\psi^g$. It is given by
\[
(\psi^g)(x) = \psi(g^{-1}xg), \quad \text{for } x \in ^gH.
\]
This induces a ring isomorphism
\[
c_{g,H} : R(H) \to R(^gH), \quad \psi \mapsto ^g\psi,
\]
with $^g\psi$ defined as in (7.9.a) for arbitrary $\psi \in R(H)$. The map $c_{g,H}$ is an isometry with respect to the Schur inner product: One has
\[
(^g\psi_1, ^g\psi_2)^g_H = (\psi_1, \psi_2)_H,
\]
for all $\psi_1, \psi_2 \in R(H)$. In particular one has: $\psi \in \text{Irr}(H)$ if and only if $^g\psi \in \text{Irr}(^gH)$.

7.10 Theorem (Mackey decomposition formula) Let $U$ and $H$ be subgroups of $G$, let $F$ be a field, and let $W$ be an $FH$-module. Then one has an isomorphism
\[
\text{Res}_U^G(\text{Ind}_H^G(W)) \cong \bigoplus_{g \in U \backslash G/H} \text{Ind}_{U \cap ^gH}^U \left( \text{Res}_{U \cap ^gH}^g(\psi^g_W) \right)
\]
of $FU$-modules.
Proof By the decomposition $FG = \bigoplus_{g \in U \setminus G/H} F[UgH]$ of $FG$ into $(FU, FH)$-subbimodules we obtain an isomorphism

$$\text{Res}^G_U(\text{Ind}^G_H(W)) = FG \otimes_{FH} W \cong \bigoplus_{g \in U \setminus G/H} F[UgH] \otimes_{FH} W$$

of $FU$-modules. Moreover, for fixed $g \in G$, it is an easy verification that the maps

$$F[UgH] \otimes_{FH} W \rightarrowtoFU \otimes_{F[U \cap gH]} gW,$$

$$ugh \otimes w \mapsto u \otimes (ghg^{-1}) \cdot w,$$

$$ug \otimes w \leftarrowto u \otimes w,$$

are well-defined, mutually inverse isomorphisms of $FU$-modules. Note that one has to verify that the first map does not depend on the choice of $u \in U$ and $h \in H$ when expressing the element $ugh \in UgH$.

7.11 Corollary Let $U$ and $H$ be subgroups of $G$ and let $\psi \in R(H)$. Then

$$\text{res}^G_U(\text{ind}^G_H(\psi)) = \sum_{g \in U \setminus G/H} \text{ind}^U_{U \cap gH}(\text{res}^{gH}_{U \cap gH}(\psi)).$$

Proof If $\psi$ is the character of a $\mathbb{C}H$-module $W$ then the equation follows immediately from Theorem 7.10. If $\psi \in R(H)$ is arbitrary then we can write $\psi = \psi_1 - \psi_2$ with characters $\psi_1$ and $\psi_2$. Since both sides of the equation are additive in $\psi$, the result follows.

7.12 Corollary Let $U$ and $H$ be subgroups of $G$, let $\psi \in R(H)$, and let $\lambda \in R(U)$. Then

$$\text{ind}^G_U(\lambda) \cdot \text{ind}^G_H(\psi) = \sum_{g \in U \setminus G/H} \text{ind}^G_U(\text{res}^{gH}_{U \cap gH}(\lambda) \cdot \text{res}^{gH}_{U \cap gH}(\psi)).$$

Proof Using the Frobenius property (cf. Theorem 7.7) and Mackey’s de-
composition formula (cf. Corollary 7.11), we obtain
\[
\text{ind}_U^G(\lambda) \cdot \text{ind}_H^G(\psi) = \text{ind}_U^G(\lambda \cdot \text{res}_H^G(\text{ind}_H^G(\psi)))
\]
\[
= \text{ind}_U^G(\lambda \cdot \sum_{g \in U \cap G/H} \text{ind}_{U \cap gH}^G(\text{res}_{U \cap gH}^H(\psi)))
\]
\[
= \text{ind}_U^G(\sum_{g \in U \setminus G/H} \text{ind}_{U \cap gH}^G(\text{res}_{U \cap gH}^H(\lambda) \cdot \text{res}_{U \cap gH}^H(\psi)))
\]
\[
= \sum_{g \in U \setminus G/H} \text{ind}_{U \cap gH}^G(\text{res}_{U \cap gH}^H(\lambda) \cdot \text{res}_{U \cap gH}^H(\psi)),
\]
and the corollary is proved. \(\square\)

7.13 Corollary (Mackey’s irreducibility criterion) Let \(\psi \in \text{Irr}(H)\).

(a) The character \(\text{ind}_H^G(\psi)\) is irreducible if and only if
\[
(\text{res}_{H \cap gH}^H(\psi), \text{res}_{H \cap gH}^H(\psi))_{H \cap gH} = 0, \quad \text{for all} \ g \in G \setminus H.
\]

(b) Assume that \(H\) is normal in \(G\). Then \(\text{ind}_H^G(\psi)\) is irreducible if and only if
\[
\psi \neq g\psi, \quad \text{for all} \ g \in G \setminus H.
\]

Proof (a) Since the degree of \(\text{ind}_H^G(\psi)\) is positive, Proposition 2.18 implies that \(\text{ind}_H^G(\psi)\) is irreducible if and only if \((\text{ind}_H^G(\psi), \text{ind}_H^G(\psi))_G = 1\). Moreover, by Frobenius reciprocity (cf. Theorem 7.5) and the Mackey decomposition formula (cf. Corollary 7.11), we have
\[
(\text{ind}_H^G(\psi), \text{ind}_H^G(\psi))_G = (\psi, \text{res}_H^G(\text{ind}_H^G(\psi)))_H
\]
\[
= (\psi, \sum_{g \in H \cap G/H} \text{ind}_H^G(\text{res}_{H \cap gH}^H(\psi)))_H
\]
\[
= \sum_{g \in H \cap G/H} (\text{res}_{H \cap gH}^H(\psi), \text{res}_{H \cap gH}^H(\psi))_{H \cap gH}.
\]
The summand in the last sum which is indexed by \(g = 1\) is equal to \((\psi, \psi) = 1\). Since all the other summands are non-negative integers, the result follows.

(b) This follows immediately from Part (a). \(\square\)
Exercises

1. Let $G$ be a finite group and let $S$ be a finite $G$-set with $G$-orbits $S_1, \ldots, S_n$. For each $i = 1, \ldots, n$, let $H_i$ be the stabilizer in $G$ of some element $s_i \in S_i$. Show that the permutation character $\chi_S$ introduced in Exercise 5.4 satisfies

$$\chi_S = \sum_{i=1}^{n} \text{ind}^G_{H_i} 1_{H_i}.$$ 

2. Compute the character table of $\text{Sym}(5)$ (and $\text{Sym}(6)$ if you want) using the following approach for general $n$. For two partitions $\lambda = (\lambda_1, \lambda_2, \ldots)$ and $\mu = (\mu_1, \mu_2, \ldots)$ of $n$, define the dominance order

$$\lambda \preceq \mu : \iff \sum_{i=1}^{j} \lambda_i \leq \sum_{i=1}^{j} \mu_i \quad \text{for all } j.$$ 

This defines a partial order on all partitions of $n$. For every partition $\lambda$ consider the corresponding Young subgroup $S_\lambda$ which is defined as the set of all permutations which permute the first $\lambda_1$ elements among themselves, the second $\lambda_2$ elements among themselves, etc. The subgroup $S_\lambda$ of $\text{Sym}(n)$ is clearly isomorphic to $\text{Sym}(\lambda_1) \times \text{Sym}(\lambda_2) \times \cdots$. Now start with the unique maximal partition $\lambda = (n)$ and compute the permutation character $\pi_\lambda := \text{ind}^{\text{Sym}(n)}_{S_\lambda}(1)$. Then go down the poset of partitions, at every step taking a new $\lambda$, maximal among the partitions that were not considered yet, compute $\pi_\lambda$ and check which of the previously constructed irreducible characters are constituents of $\pi_\lambda$ and compute their multiplicity in $\pi_\lambda$. You should be left with precisely one irreducible summand that has not been constructed before. Call this character $\chi_\lambda$ and proceed down the poset of partitions. (One can prove that this process works.)

3. (a) Assume that $S$ is a transitive $G$-set with $|S| > 1$, let $s \in S$ and set $H := \text{stab}_G(s) < G$. By Problem 1 and Frobenius reciprocity, one has $(\chi_S, 1) = (\text{ind}_H^G(1_H), 1_G) = (1_H, \text{res}_H^G(1_G)) = (1_H, 1_H) = 1$. Therefore, $\chi_S = 1_G + \psi$ for some character $\psi$ of $G$, which does not contain the trivial character as a constituent. Show that the following are equivalent:

(i) The character $\psi$ is irreducible.

(ii) The $G$-set $S \times S$ (with $g(s_1, s_2) := (gs_1, gs_2)$ for $g \in G$ and $s_1, s_2 \in S$) has exactly two orbits.

(iii) One has $(\chi_S^2, 1) = 2$.

(iv) $S$ is a doubly transitive $G$-set (i.e., for any two pairs $(s_1, s_2), (s'_1, s'_2) \in S \times S$ with $s_1 \neq s_2$ and $s'_1 \neq s'_2$ there exists $g \in G$ with $gs_1 = s'_1$ and $gs_2 = gs'_2$).

68
(v) One has $|H \setminus G/H| = 2$.

(b) Let $n \in \mathbb{N}$ and let $\lambda = (n - 1, 1)$. Show that $\pi^\lambda$ (from Exercise 2) is equal to $\text{ind}_{\text{Sym}(n-1)}^{\text{Sym}(n)}(1)$ and equal to the permutation character of $S_n$. Also show that $\pi^\lambda = 1 + \chi$ for an irreducible character $\chi$ of $\text{Sym}(n)$.

4. Let $G$ be a finite group, let $H$ be a subgroup of $G$, and let $g_1, \ldots, g_n \in G$ be coset representatives for $G/H$. Moreover, let $V$ be a finitely generated $FG$-module and let $W$ be a finitely generated $FH$-module. Show that the following are equivalent:

(i) The $FG$-modules $V$ and $\text{Ind}_H^G(W)$ are isomorphic.

(ii) There exists an $FH$-submodule $W'$ of $V$, with $W' \cong W$, such that $V = \bigoplus_{i=1}^n g_i W'$.

5. Let $G$ be a finite group, $U \leq H \leq G$, and $g \in G$. Furthermore, let $c_{g,H} : R(H) \to R(^g H)$, $\psi \mapsto ^g \psi$, be the conjugation map with $^g \psi(x) := \psi(g^{-1} x g)$ for $x \in ^g H := g H g^{-1}$.

(a) Show that $c_{h,H}$ is the identity if $h \in H$ and that $c_{g,H} c_{g,H} = c_{g',g,H}$ for $g, g' \in G$.

(b) Show that $c_{g,U} \circ \text{res}_U^H = \text{res}_{^g U}^H \circ c_{g,H}$ and $c_{g,H} \circ \text{ind}_U^H = \text{ind}_{^g U}^H \circ c_{g,U}$.

6. Let $G$ be a finite group and let $U, H \leq G$. Let $g_1, \ldots, g_n \in G$ be a set of representatives of $U \setminus G/H$ and for each $i = 1, \ldots, n$ let $u_{i,1}, \ldots, u_{i,k_i}$ be a set of representatives for $U/U \cap ^g H$. Show that the elements $u_{i,j} g_i$, $i = 1, \ldots, n$, $j = 1, \ldots, k_i$ form a set of representatives for $G/H$.

7. (a) Let $G$ be a finite group, $g_1, \ldots, g_h$ a set of representatives for the conjugacy classes of $G$,

$$n := |\{\chi \in \text{Irr}(G) \mid \chi(g) \notin \mathbb{R} \text{ for some } g \in G\}|,$$

and $m \in \mathbb{N}$ with $2m = n$. Show that the determinant $d$ of the character table satisfies

$$d^2 = (-1)^m |C_G(g_1)| \cdots |C_G(g_h)|.$$

(b) Let $p$ be an odd prime and let $\zeta := e^{2\pi i/p}$. Show that

$$\sqrt{(-1)^{\frac{p-1}{2}}} p \in \mathbb{Q}(\zeta).$$

8. Let $H$ be a subgroup of a finite group $G$ and let $\psi \in \text{CF}(H, F)$ be a class function of $H$ with values in a field $F$. For $g \in G$ set

$$\text{ind}_H^G(\psi)(g) := \frac{1}{|H|} \sum_{x \in G} \psi(x^{-1} g x).$$
Show that this defines an $F$-linear map

$$\text{ind}_{H}^{G} : \text{CF}(H, F) \to \text{CF}(G, F),$$

and verify that all the rules for induction of virtual characters is also true for induction of class functions (transitivity, Frobenius Reciprocity, Frobenius property, Mackey formula, what else?)
8 Frobenius Groups

In this section we prove Frobenius’ Theorem, Theorem 8.1, on (what are now called) Frobenius groups. The statement of this theorem is given in purely group theoretic terms. Its proof involves characters and until now there is no proof known that avoids representation theory and character theory.

For a large part of this section we assume that $G$ is a finite group and that $H$ is a subgroup of $G$ which satisfies

$$H \cap {}^gH = \{1\}, \text{ for every } g \in G \setminus H. \quad (8.0.a)$$

We will prove the following theorem.

8.1 Theorem Let $G$ and $H$ satisfy $(8.0.a)$. Then the subset $N$ of $G$, defined as

$$N := G \setminus \left( \bigcup_{g \in G} {}^gH \setminus \{1\} \right),$$

is a normal complement of $H$ in $G$, i.e., $N$ is a normal subgroup of $G$, $HN = G$ and $H \cap N = \{1\}$.

8.2 Definition If $G > H > \{1\}$ satisfy $(8.0.a)$ then $G$ is called a Frobenius group, $H$ is called a Frobenius complement and $N$ is called the Frobenius kernel of $G$.

8.3 Remark A theorem proved by John Thompson in his thesis (1960) states that if $H > \{1\}$ then the subgroup $N$ is nilpotent (i.e., a direct product of $p$-subgroups) and in fact the largest normal nilpotent subgroup of $G$ with respect to inclusion. This justifies the terminology ‘the Frobenius kernel’ of $G$. Moreover, one can show that $\text{gcd}(|H|, |G/H|) = 1$ (i.e., $H$ is a Hall-subgroup of $G$, see Exercise 1). Thus, the Frobenius complement $H$ is uniquely determined up to conjugation in $G$ by a Theorem of Schur and Zassenhaus.

We will prove Theorem 8.1 in three steps. First we establish two lemmas.

8.4 Lemma Assume that $G$ is a finite group, that $H$ is a subgroup of $G$ satisfying $(8.0.a)$ and let $\psi \in R(H)$ with $\psi(1) = 0$. Then the following hold:

(a) $\text{res}_H^G(\text{ind}_H^G(\psi)) = \psi$.

(b) For every $\psi' \in R(H)$ one has $(\psi, \psi')_H = (\text{ind}_H^G(\psi), \text{ind}_H^G(\psi'))_G$. 

71
Proof (a) We need to show that
\[ \frac{1}{|H|} \sum_{x \in G} \psi(xhx^{-1}) = \psi(h), \]
for every \( h \in H \). If \( h = 1 \) then both sides are equal to 0. If \( h \neq 1 \) and \( x \in G \) then \( xhx^{-1} \) belongs to \( H \) if and only if \( x \in H \) (by the property in (8.0.a)). This implies that the left hand side is equal to \( \frac{1}{|H|} \sum_{x \in H} \psi(xhx^{-1}) = \psi(h) \), since \( \psi \) is a class function on \( H \).

(b) This follows immediately from Part (a) and Frobenius reciprocity (cf. Theorem 7.5):
\[(\text{ind}_{H}^{G}(\psi), \text{ind}_{H}^{G}(\psi'))_{G} = (\text{res}_{H}^{G}(\text{ind}_{H}^{G}(\psi)), \psi')_{H} = (\psi, \psi')_{H}.\]

\[\square\]

8.5 Lemma Assume that \( G, H \) and \( N \) are as in Theorem 8.1 and let \( \varphi \in \text{Irr}(H) \). Then there exists an irreducible character \( \varphi^{*} \in \text{Irr}(G) \) such that \( \text{res}_{H}^{G}(\varphi^{*}) = \varphi \) and \( N \subseteq \ker(\varphi^{*}) \).

Proof We first assume that \( \varphi = 1_{H} \) is the trivial character of \( H \). Then the trivial character \( \varphi^{*} = 1_{G} \) of \( G \) has all the desired properties.

From now on we assume that \( \varphi \neq 1_{H} \) and set \( \psi := \varphi - \varphi(1) \cdot 1_{H} \). Then, by Frobenius reciprocity and by evaluation at the identity element of \( H \) we have
\[(\text{ind}_{H}^{G}(\psi), 1_{G})_{G} = (\psi, 1_{H})_{H} = -\varphi(1) \quad \text{and} \quad \psi(1) = 0.\]

Thus, the virtual character \( \varphi^{*} := \text{ind}_{H}^{G}(\psi) + \varphi(1)1_{G} \in R(G) \) satisfies
\[(\varphi^{*}, 1_{G}) = 0 \quad \text{and} \quad \varphi^{*}(1) = \varphi(1).\]

This implies that \((\text{ind}_{H}^{G}(\psi), \text{ind}_{H}^{G}(\psi))_{G} = (\varphi^{*}, \varphi^{*})_{G} + \varphi(1)^{2} \). On the other hand, by Lemma 8.4(b), we obtain
\[(\text{ind}_{H}^{G}(\psi), \text{ind}_{H}^{G}(\psi))_{G} = (\psi, \psi)_{H} = (\varphi, \varphi)_{H} + \varphi(1)^{2} = 1 + \varphi(1)^{2}.\]

This implies that \((\varphi^{*}, \varphi^{*})_{G} = 1 \). Since also \( \varphi^{*}(1) = \varphi(1) > 0 \), Proposition 2.18 implies that \( \varphi^{*} \) is an irreducible character of \( G \). Moreover, Lemma 8.4(a) implies that \( \text{res}_{H}^{G}(\text{ind}_{H}^{G}(\psi)) = \psi \), so that
\[\text{res}_{H}^{G}(\varphi^{*} - \varphi(1) \cdot 1_{G}) = \varphi - \varphi(1) \cdot 1_{H}.\]
Since \( \text{res}_{H}^G(1_G) = 1_H \), we obtain \( \text{res}_{H}^G(\varphi^*) = \varphi \).

Finally, we show that \( N \subseteq \ker(\varphi^*) \). We need to show that \( \varphi^*(x) = \varphi^*(1) \)
for every \( x \in N \). So let \( x \in N \). We may assume that \( x \neq 1 \). Then \( x \) is not conjugate in \( G \) to any element of \( H \). Therefore, \( (\text{ind}_{H}^G(\varphi))(x) = 0 \) and \( \varphi^*(x) = (\text{ind}_{H}^G(\varphi) + \varphi(1) \cdot 1_G)(x) = \varphi(1) = \varphi^*(1) \). This completes the proof of the lemma. \( \square \)

**Proof of Theorem 8.1.** For each \( \varphi \in \text{Irr}(H) \) we choose an element \( \varphi^* \in \text{Irr}(G) \) which satisfies \( \text{res}_{H}^G(\varphi^*) = \varphi \) and \( N \subseteq \ker(\varphi^*) \), as guaranteed by Lemma 8.5. Then we set

\[
M := \bigcap_{\varphi \in \text{Irr}(H)} \ker(\varphi^*).
\]

Since each \( \ker(\varphi^*) \) is a normal subgroup of \( G \) containing \( N \), also \( M \) is a normal subgroup of \( G \) with \( N \subseteq M \). Moreover, since \( \text{res}_{H}^G(\varphi^*) = \varphi \), we obtain

\[
M \cap H = \bigcap_{\varphi \in \text{Irr}(H)} (\ker(\varphi^*) \cap H) = \bigcap_{\varphi \in \text{Irr}(H)} \ker(\varphi^*) = \{1\}. \quad (8.5.a)
\]

The last equation follows immediately from the following line of argument (see also Exercise 2.7): First observe that \( \ker(\chi) \cap \ker(\chi') = \ker(\chi + \chi') \) for all characters \( \chi \) and \( \chi' \) of \( G \). This implies \( \bigcap_{\varphi \in \text{Irr}(H)} \ker(\varphi^*) = \ker(\sum_{\varphi \in \text{Irr}(H)} \varphi(1)\varphi) \). But the latter character is the regular character \( \rho_H \) of \( H \) and one has \( \ker(\rho_H) = \{1\} \), since \( \rho_H(h) = 0 \) for all \( 1 \neq h \in H \). This proves the last equation in (8.5.a).

Since \( M \) is normal in \( G \), the equation \( M \cap H = \{1\} \) also implies \( M \cap gH = gM \cap H = g(M \cap H) = \{1\} \) for every \( g \in G \). This implies that \( M \) does not contain any non-trivial element which is conjugate to an element of \( H \). In other words, we have \( M \subseteq N \). Altogether we obtain \( M = N \). Thus, \( N \) is a normal subgroup of \( G \) and \( N \cap H = \{1\} \).

We still need to show that \( NH = G \). Note that the hypothesis in (8.0.a) on \( H \) implies that \( N_G(H) = H \). Thus, \( H \) has precisely \( [G : N_G(H)] = [G : H] \) conjugate subgroups and any two distinct conjugates of \( H \) have trivial intersection. In fact if \( g_1 \) and \( g_2 \) are elements in \( G \) such that \( g_1H \neq g_2H \) then \( g_1^{-1}g_2 \notin N_G(H) \) and \( g_1^{-1}(g_1H \cap g_2H) = (H \cap g_1^{-1}g_2H) = \{1\} \). This implies that \( g_1H \cap g_2H = \{1\} \). Therefore, we obtain

\[
|N| = |G| - \left| \bigcup_{g \in G} (gH \setminus \{1\}) \right| = |G| - [G : H](|H| - 1) = [G : H].
\]
As a consequence we have $|HN| = |H||N|/|H \cap N| = |G|/1 = |G|$ and $HN = G$. This completes the proof of the theorem.

The following corollary describes a situation that leads to the hypothesis in (8.0.a). This was the original situation that Frobenius wanted to understand.

**8.6 Corollary** Let $G$ be a finite group and let $X$ be a transitive $G$-set such that no non-identity element of $G$ fixes two or more elements of $X$. Let $N$ denote the set consisting of the identity element of $G$ together with all elements of $G$ which do not fix a single element of $X$. Then $N$ is a normal subgroup of $G$ which still acts transitively on $X$.

**Proof** We fix an arbitrary element $x$ of $X$ and set $H := \text{stab}_G(x)$, the stabilizer of $x$ in $G$. For every element $y \in X$ there exists $g \in G$ such that $y = gx$. This implies $\text{stab}_G(y) = gH$. Since no non-identity element of $G$ fixes more than one element of $X$ we obtain $H \cap gH = \{1\}$ for all $g \in G \setminus H$. Moreover, an element of $G$ fixes at least one element of $X$ if and only if it is conjugate to an element in $H$. This implies that the set $N$ as defined in Theorem 8.1 is equal to the set $N$ as defined in this corollary. By Theorem 8.1 we obtain that $N$ is a normal subgroup of $G$ and that $NH = G$. To show that $N$ acts still transitively on $X$, note that $G = NH$ implies $X = Gx = NHx = Nx$, and the corollary is proved.

**Exercises**

1. Let $G$ be a finite group and let $H$ be a subgroup of $G$ satisfying $H \cap gH = \{1\}$ for all $g \in G \setminus H$. Show that $\text{gcd}(|H|, [G : H]) = 1$.

2. Let $k$ be a commutative ring.
   (a) Show that, for each $a \in k^\times$ and $b \in k$, the map $f_{a,b} : k \to k$, $x \mapsto ax + b$, is bijective.
   (b) Show that the maps in (a) form a group under composition. This group is called the *affine linear group* of $k$ and is denoted by $\text{Aff}(k)$.
   (c) Show that $\text{Aff}(k)$ is isomorphic to the semidirect product $k \rtimes k^\times$, where the unit group $k^\times$ acts by multiplication on the additive group $k$.
   (d) Show that if $k$ is a finite field then $\text{Aff}(k)$ is a Frobenius group.

3. Show that if $N_1$ and $N_2$ are nilpotent normal subgroups of a finite group $G$ then $N_1N_2$ is also a nilpotent normal subgroup of $G$. In particular there exists
a largest nilpotent normal subgroup in every finite group $G$, called the *Fitting subgroup* of $G$ and denoted by $F(G)$. 
9 Elementary Clifford Theory

Throughout this section, $G$ denotes a finite group and $N$ denotes a normal subgroup of $G$.

Recall from Remark 5.13 that for every irreducible character $\psi$ of $N$ one has an associated idempotent

$$e_\psi = \frac{\psi(1)}{|N|} \sum_{x \in N} \psi(x^{-1})x \in \mathbb{C}N.$$ 

Recall also from Remark 7.9(d) that $G$ acts on $\text{Irr}(N)$ by $g \psi(x) = \psi(g^{-1}xg)$, for $g \in G$ and $x \in N$. The following lemma shows that, for $g \in G$, the $\mathbb{C}$-algebra isomorphism $\mathbb{C}N \rightarrow \mathbb{C}N$, $a \mapsto gag^{-1}$, permutes the above idempotents as expected.

9.1 Lemma Let $\psi \in \text{Irr}(N)$ and let $g \in G$. Then $ge_\psi g^{-1} = e_{g\psi}$ in $\mathbb{C}N$.

Proof We have

$$ge_\psi g^{-1} = g\left(\frac{\psi(1)}{|N|} \sum_{x \in N} \psi(x^{-1})x\right)g^{-1} = \frac{\psi(1)}{|N|} \sum_{x \in N} \psi(x^{-1})gxg^{-1}$$

$$= \frac{q\psi(1)}{|N|} \sum_{y \in N} q\psi(y^{-1})y = e_{g\psi},$$

after substituting $y = gxg^{-1}$, and the lemma is proven. \qed

The following theorem describes the pattern that occurs when one restricts an irreducible character to a normal subgroup.

9.2 Theorem Let $V$ be an irreducible $\mathbb{C}G$-module and let $\chi \in \text{Irr}(G)$ denote its character.

(a) If $0 \neq W$ is a $\mathbb{C}N$-submodule of $V$ then $\sum_{g \in G} gW = V$.

(b) Let $W \subseteq V$ be an irreducible $\mathbb{C}N$-submodule of $V$ and let $\psi \in \text{Irr}(N)$ denote the character of $W$. Furthermore, let $H := \text{stab}_G(\psi) := \{ g \in G \mid g\psi = \psi \}$ denote the inertia group of $\psi$ in $G$, and let $1 = g_1, \ldots, g_n \in G$ be a set of representatives of $G/H$. Finally, for $i = 1, \ldots, n$, set $\psi_i := g_i \psi$ and let $V_i := e_{\psi_i} \cdot V$ be the $\psi_i$-homogeneous component of $\text{Res}_{N}^{G}(V)$. Then

$$V = \bigoplus_{i=1}^{n} V_i \quad \text{and} \quad \text{res}_{N}^{G}(\chi) = e \sum_{i=1}^{n} \psi_i$$
for some positive integer $e$, called the ramification index of $\chi$ over $N$.

(c) For each $i = 1, \ldots, n$, the $\mathbb{C}N$-submodule $V_i$ of $V$ is an irreducible $\mathbb{C}H_i$-submodule, where $H_i := g_i H g_i^{-1}$. Moreover, $\text{Ind}_{H_i}^G(V_i) \cong V$ for all $i = 1, \ldots, n$.

**Proof** (a) Set $V' := \sum_{g \in G} gW$. Then $V' \neq \{0\}$, since $W \neq \{0\}$. Moreover, it is immediate that $V'$ is a $\mathbb{C}G$-submodule of $V$. Since $V$ is a simple $\mathbb{C}G$-module, we obtain $V' = V$ as claimed.

(b) First note that, since $e_{\psi_i} \cdot e_{\psi_j} = 0$ for $i \neq j$ in $\{1, \ldots, n\}$, the sum $V_1 + \cdots + V_n$ of $\mathbb{C}N$-submodules of $V$ is a direct sum.

Next we will show that if $g \in G$ satisfies $gg_i H = g_j H$ then $gV_i = V_j$. In fact, in this case there exists $h \in H$ such that $gg_i = g_j h$ and we obtain

$$gV_i = ge_{\psi_i} V = ge_{\psi_i}g^{-1}gV = gg_i e_{\psi_i}g^{-1}g^{-1}gV = g_j h e_{\psi_i} h^{-1} g_j^{-1} gV = e_{\psi_j} V = V_j,$$

since $gV = V$ and since $g_j h e_{\psi_i} h^{-1} g_j^{-1} = e_{s_j \psi_i} = e_{\psi_j}$ by Lemma 9.1. Since $g_1 = 1 \in H$, the $\mathbb{C}N$-submodule $V_1$ contains $W$. Therefore, $V_1 \neq \{0\}$ and Part (a) applied to $V_1$ implies that $V = \sum_{g \in G} gV_1 = V_1 + \cdots + V_n$. Thus we have shown that $V$ decomposes into the direct sum $V = V_1 \oplus \cdots \oplus V_n$ of $\mathbb{C}N$-submodules. This implies that $\text{res}_N^G(\chi)$ is the sum of the characters of the $\mathbb{C}N$-modules $V_i$. Since $V_i$ is the $\psi_i$-homogeneous component of $\text{Res}_N^G(V)$, the character of $V_i$ is equal to $n_i \cdot \psi_i$ with $n_i = \dim_{\mathbb{C}}(V_i)/\psi_i(1)$. But since $V_i = g_i V_1$, we have $\dim_{\mathbb{C}} V_i = \dim_{\mathbb{C}} V_1$, and since $\psi_i(1) = g_i \psi(1) = \psi(1)$, the positive integers $n_i$, $i = 1, \ldots, n$, are all equal. If we denote this number by $e$ we obtain

$$\text{res}_N^G(\chi) = e(\psi_1 + \cdots + \psi_n)$$

and part (b) is proven.

(c) It follows from the proof of Part (b) that, for $i \in \{1, \ldots, n\}$ and every $h \in H$ and $v_i \in V_i$, one has

$$(g_i h g_i^{-1}) v_i = (g_i h) (g_i^{-1} v_i) \in g_i h V_i = g_i V_i = V_i.$$

This implies that $V_i$ is a $\mathbb{C}H_i$-submodule of $V$. Moreover, the function

$$\mathbb{C}G \otimes_{\mathbb{C}H_i} V_i \to V, \quad a \otimes v_i \mapsto av_i,$$

is a well-defined $\mathbb{C}G$-module homomorphism. It is surjective, since it contains $\sum_{g \in G} gV_i = V_1 + \cdots + V_n$, by the proof of Part (b). Moreover, since
\[ \dim_C(CG \otimes_{CH_i} V_i) = [G : H_i] \cdot \dim_C V_i = [G : H] \cdot \dim_C V_1 = n \dim_C V_1 = \dim_C(V_1 \oplus \cdots \oplus V_n), \]

we obtain that the above map is an isomorphism. Finally, since \( V \cong \text{Ind}_{H_i}^G(V_i) \) is irreducible, also the \( CH_i \)-module \( V_i \) must be irreducible.

9.3 Example Let \( G = \text{Sym}(4) \) and \( N = V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \).

The character tables of \( G \) and \( N \) are given by

\[
\begin{array}{c|ccccc}
G & 1 & (ab)(cd) & (ab) & (abc) & (abcd) \\
\hline
\chi_1 & 1 & 1 & 1 & 1 & 1 \\
\chi_2 & 1 & 1 & -1 & 1 & -1 \\
\chi_3 & 2 & 2 & 0 & -1 & 0 \\
\chi_4 & 3 & -1 & 1 & 0 & -1 \\
\chi_5 & 3 & -1 & -1 & 0 & 1 \\
\end{array}
\]

and

\[
\begin{array}{c|ccccc}
N & 1 & (1,2)(3,4) & (1,3)(2,4) & (1,4)(2,3) \\
\hline
\psi_1 & 1 & 1 & 1 & 1 \\
\psi_2 & 1 & 1 & -1 & -1 \\
\psi_3 & 1 & -1 & 1 & -1 \\
\psi_4 & 1 & -1 & -1 & 1 \\
\end{array}
\]

One can read from the character tables that

\[
\begin{align*}
\text{res}_N^G(\chi_1) &= \psi_1, \\
\text{res}_N^G(\chi_2) &= \psi_1, \\
\text{res}_N^G(\chi_3) &= 2 \cdot \psi_1, \\
\text{res}_N^G(\chi_4) &= \psi_2 + \psi_3 + \psi_4, \\
\text{res}_N^G(\chi_5) &= \psi_2 + \psi_3 + \psi_4. \\
\end{align*}
\]

One can also read from the character table of \( N \) that \( \text{Irr}(N) \) has two orbits under \( G \)-conjugation, namely \( \{\psi_1\} \) and \( \{\psi_2, \psi_3, \psi_4\} \). Moreover, \( \text{stab}_G(\psi_1) = G \) and \( \text{stab}_G(\psi_2) = H_1 := N \cdot \langle (1,2) \rangle \), \( \text{stab}_G(\psi_3) = N \cdot \langle (1,3) \rangle \) and \( \text{stab}_G(\psi_4) = N \cdot \langle (1,4) \rangle \). Note that the latter three subgroups of \( G \) have order 8. Moreover, Theorem 9.2(c) implies that \( \chi_4 = \text{ind}_{H_1}^G(\lambda) \) for some \( \lambda \in \text{Irr}(H_1) \). Comparing degrees, we obtain \( \lambda(1) = 1 \).
9.4 Remark (a) Let $K \leq H \leq G$, $\psi, \psi' \in R(K)$, $\chi \in R(H)$ and $g \in G$. Then it is easily verified (see Exercise 7.4) that
\[ q\text{ind}_K^H(\psi) = \text{ind}_K^H(g\psi), \quad q\text{res}_K^H(\chi) = \text{res}_K^H(g\chi), \quad (g\psi, g\psi')_K = (\psi, \psi')_K. \]

(b) The following notation will be used in the next theorem. For $\psi \in \text{Irr}(N)$ we set
\[ \text{Irr}(G|\psi) := \{ \chi \in \text{Irr}(G) \mid (\text{res}_N^G(\chi), \psi)_N > 0 \}. \]

Note that by the above, $\text{Irr}(G|\psi) = \text{Irr}(G|g\psi)$ for all $g \in G$. Moreover, by Theorem 9.2, one has $\text{Irr}(G|\psi) \cap \text{Irr}(G|\psi') = \emptyset$, whenever $\psi$ and $\psi'$ are not in the same $G$-orbit of $\text{Irr}(N)$. By Frobenius reciprocity, every $\chi \in \text{Irr}(G)$ belongs to a subset $\text{Irr}(G|\psi)$ for some $\psi \in \text{Irr}(N)$. Altogether, restriction and induction induce mutually inverse bijections between the set of subsets $\text{Irr}(G|\psi)$ of $\text{Irr}(G)$ and the set of $G$-orbits of $\text{Irr}(N)$.

(c) In the proof of the next theorem we will need the following result. Let $H \leq G$ and let $\chi$ and $\chi'$ be characters of $G$. Then
\[ (\chi, \chi')_G \leq \left( \text{res}_H^G(\chi), \text{res}_H^G(\chi') \right)_H. \]

In fact, let $V$ and $V'$ be $\mathbb{C}G$-modules with characters $\chi$ and $\chi'$, respectively. Then, by Proposition 7.4, we have $(\chi, \chi')_G = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}G}(V, V')$ and $\left( \text{res}_H^G(\chi), \text{res}_H^G(\chi') \right)_H = \dim_{\mathbb{C}} \text{Hom}_{\mathbb{C}H}(V, V')$. But, clearly one has an inclusion $\text{Hom}_{\mathbb{C}G}(V, V') \subseteq \text{Hom}_{\mathbb{C}H}(V, V')$.

9.5 Theorem Let $\psi \in \text{Irr}(N)$ and set $H := \text{stab}_G(\psi)$. Write
\[ \text{ind}_N^H(\psi) = m_1\theta_1 + \cdots + m_r\theta_r \]
with $m_1, \ldots, m_r \in \mathbb{N}$ and with pairwise distinct $\theta_1, \ldots, \theta_r \in \text{Irr}(H)$.

(a) One has $\text{Irr}(H|\psi) = \{ \theta_1, \ldots, \theta_r \}$, $\text{res}_N^H(\theta_i) = m_i\psi$ for $i = 1, \ldots, r$, and
\[ m_1^2 + \cdots + m_r^2 = [H : N]. \]

(b) The function $\theta \mapsto \text{ind}_N^H(\theta)$ defines a bijection $f : \text{Irr}(H|\psi) \rightarrow \text{Irr}(G|\psi)$.

Proof (a) The first statement follows immediately from Frobenius reciprocity. The second statement is immediate with Frobenius reciprocity and Theorem 9.2(b), since $\psi$ is stable under $H$. In order to prove the last statement in Part (a), consider the equations
\[ \text{res}_N^H(\text{ind}_N^H(\psi)) = \text{res}_N^H(m_1\theta_1 + m_r\theta_r) = (m_1^2 + \cdots + m_r^2)\psi. \]
Since the degree of the left hand side is equal to \([H : N]\psi(1)\) and the degree of the right hand side is equal to \((m_1^2 + \cdots + m_r^2)\psi(1)\), the result follows.

(b) For \(i = 1, \ldots, r\) we set \(\chi_i := \text{ind}_G^H(\theta_i)\). For \(g \in G \setminus H\), Remark 9.4(a), (c), and Part (a) imply

\[
0 \leq \left( \frac{\theta_i|_{H \cap gH}}{H \cap gH}, \frac{\theta_i|_{H \cap gH}}{H \cap gH} \right)_{H \cap gH} \leq \left( \frac{\theta_i|_N}{N}, \frac{\theta_i|_N}{N} \right)_N = m_i^2\langle g\psi, \psi \rangle_N = 0,
\]

since \(g\psi \neq \psi\). This implies that each term above is equal to 0. By Mackey’s irreducibility criterion for induced characters, cf. Corollary 7.13, we obtain that \(\chi_i \in \text{Irr}(G)\). Moreover,

\[
\left( \chi_i|_N, \psi \right)_N = \left( \chi_i, \text{ind}_G^H(\psi) \right)_G = \left( \chi_i, \text{ind}_H^G(\text{ind}_N^G(\psi)) \right)_G = \sum_{j=1}^r m_j \left( \chi_i, \text{ind}_H^G(\theta_j) \right)_G \\
\geq \left( \chi_i, \text{ind}_H^G(\theta_1) \right)_G = (\chi_i, \chi_i)_G = 1.
\]

Thus, the map \(f\) in the theorem takes values in the set \(\text{Irr}(G|\psi)\) as claimed. To see that the function \(f\) is surjective, let \(\chi \in \text{Irr}(G|\psi)\). Then, by Frobenius reciprocity, \(\chi\) is a constituent of \(\text{ind}_G^G(\psi) = \text{ind}_H^G(\text{ind}_N^G(\psi)) = \text{ind}_H^G(m_1\theta_1 + \cdots + m_r\theta_r) = m_1\chi_1 + \cdots + m_r\chi_r\) and \(\chi = \chi_i = f(\theta_i)\) for some \(i \in \{1, \ldots, r\}\).

Finally we will show that the map \(f\) is injective. Assume this is not the case. Then, after renumbering if necessary, we obtain that \(\chi_1 = \chi_2\). This implies

\[
\left( \text{ind}_N^G(\psi), \text{ind}_N^G(\psi) \right)_G = \sum_{i,j=1}^r (m_i\chi_i, m_j\chi_j)_G \\
\geq m_1^2 + 2m_1m_2 + m_2^2 + \cdots + m_r^2 > m_1^2 + \cdots + m_r^2 \\
= [H : N].
\]

On the other hand, the Mackey decomposition formula implies

\[
\left( \text{ind}_N^G(\psi), \text{ind}_N^G(\psi) \right)_G = \left( \psi, \text{res}_N^G(\text{ind}_N^G(\psi)) \right)_G \\
= \sum_{g \in G/N} \left( \psi, \text{ind}_N^G(\text{res}_N^G(\text{ind}_N^G(\psi))) \right)_N \\
= \sum_{g \in G/N} \left( \psi, q\psi \right)_N = \sum_{g \in H/N} \left( \psi, q\psi \right)_N = [H : N].
\]

This is a contradiction, and the theorem is proven. □
9.6 Corollary Assume that $[G : N] = 2$, that $\psi \in \text{Irr}(N)$ and $\chi \in \text{Irr}(G|\psi)$.

(a) The following are equivalent:

(i) $\text{stab}_G(\psi) = N$.

(ii) $\text{ind}_{N}^G(\psi) = \chi$.

(iii) $\text{res}_{N}^G(\chi) = \psi + \psi'$ for some $\psi \neq \psi' \in \text{Irr}(N)$.

(iv) $|\text{Irr}(G|\psi)| = 1$.

In this case, the $G$-orbit of $\psi$ is equal to $\{\psi, \psi'\}$ and $\text{ind}_{N}^G(\psi') = \chi$.

(b) The following are equivalent:

(i) $\text{stab}_G(\psi) = G$.

(ii) $\text{ind}_{N}^G(\psi) = \chi + \chi'$ for some $\chi \neq \chi' \in \text{Irr}(G)$.

(iii) $\text{res}_{N}^G(\chi) = \psi$.

(iv) $|\text{Irr}(G|\psi)| = 2$.

In this case, one has $\text{Irr}(G|\psi) = \{\chi, \chi'\}$ and $\text{res}_{N}^G(\chi') = \psi$.

Proof First note that there are only two possibilities for $\text{stab}_G(\psi)$, namely either $\text{stab}_G(\psi) = N$ or $\text{stab}_G(\psi) = G$. Also note that in any of these two cases the Mackey decomposition formula implies

$$\text{res}_{N}^G(\text{ind}_{N}^G(\psi)) = \psi + \psi'$$

(9.6.a)

with $g \in G \setminus N$.

(a) Assume that $\text{stab}_G(\psi) = N$. Then Theorem 9.5(b) implies (ii) and Equation (9.6.a) implies (iii). Moreover, Theorem 9.5(b) implies (iv). Now, (ii) and Equation (9.6.a) imply that $\psi' = \psi g$ with $g \in G \setminus N$, and Remark 9.4(a) implies that $\text{ind}_{N}^G(\psi') = \text{ind}_{N}^G(\psi) = \psi g = \psi$. 

(b) Now assume that $\text{stab}_G(\psi) = G$. Then Theorem 9.5(a) implies $r = 2$ and $m_1 = m_2 = 1$, since these are the only solutions to $m_1^2 + \cdots + m_r^2 = [G : N] = 2$. This immediately implies (ii) and (iv). Moreover, with Theorem 9.5(a) this also implies (iii). Now, since $\chi'$ occurs in $\text{ind}_{N}^G(\psi)$, Frobenius reciprocity implies that $\psi$ occurs in $\text{res}_{N}^G(\chi')$, so that $\chi' \in \text{Irr}(G|\psi)$. Thus, everything that was proved for $\chi$ also holds for $\chi'$. In particular, $\text{res}_{N}^G(\chi') = \psi$.

Finally, since each of the conditions (ii), (iii), and (iv) in (a) excludes the corresponding condition in (b) and vice-versa, each of the conditions (ii), (iii) and (iv) also implies (i) in Parts (a) and (b).
9.7 Example Consider $G = \text{Sym}(5)$ and $N = \text{Alt}(5)$. In a homework problem we determined the character degrees of $N = \text{Alt}(5)$ as 1, 3, 3, 4, 5. From the character table of $\text{Alt}(5)$ it is also easy to see that the two irreducible characters of degree 3 are $G$-conjugate. Since conjugate characters have the same degree, the characters of degree 1, 4 and 5 form $G$-orbits of size 1. Using Corollary 9.6 this implies that the character degrees of $G = \text{Sym}(5)$ are given by 1, 1, 4, 4, 5, 5 and 6.

Exercises

1. Let $G$ be a finite group, let $N$ be a normal subgroup of $G$ and assume that $\chi$ is an irreducible character of $G$ satisfying $(\text{res}_N^G(\chi), 1_N)_N \neq 0$. Show that $N \leq \ker(\chi)$.

2. Let $G$ be a finite group, let $N$ be a normal subgroup, let $\psi$ be an irreducible character of $N$ and let $\chi \in \text{Irr}(G | \psi)$. Show that $\psi(1)$ divides $\chi(1)$.

3. Let $G$ be a finite group, let $p$ be a prime, and let $P$ be a Sylow $p$-subgroup of $G$. Assume that $\chi(1)$ is a power of $p$ for every $\chi \in \text{Irr}(G)$. Show that $P$ has a normal abelian complement, i.e., that there exists a normal abelian subgroup $N$ of $G$ such that $P \cap N = \{1\}$ and $PN = G$. (Hint: Use the equation $|G| = |G : G'| + \sum_{\chi \in \text{Irr}(G), \chi(1) \neq 1} \chi(1)^2$ to show that $G$ has a normal subgroup of index $p$. Then use induction on $|G|$.)

4. (Ito’s Theorem) Let $A$ be an abelian normal subgroup of a finite group $G$ and let $\chi$ be an irreducible character of $G$. Then $\chi(1)$ divides $[G : A]$. 

82
10 Artin’s and Brauer’s Induction Theorems

Throughout this section, $G$ denotes a finite group.

10.1 Definition Let $2 \leq n \in \mathbb{N}$ and let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition of $n$, with pairwise distinct primes $p_1, \ldots, p_r$ and positive integers $e_1, \ldots, e_r$. We define

$$\mu(n) := \begin{cases} 0 & \text{if } e_i \geq 2 \text{ for some } i \in \{1, \ldots, r\}; \\ (-1)^r & \text{if } e_i = 1 \text{ for all } i = \in \{1, \ldots, r\}. \end{cases}$$

For completeness, one defines $\mu(1) := 1$. Altogether we have defined a function $\mu : \mathbb{N} \to \{-1, 0, 1\}$. This function is called the (number theoretic) M"obius function.

10.2 Lemma For every positive integer $n$ one has

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{if } n = 1; \\ 0 & \text{if } n > 1. \end{cases}$$

Here, the sum runs through the set of positive integers $d$ which divide $n$.

Proof If $n = 1$ the assertion is true by inspection. Assume now that $n > 1$ and let $n = p_1^{e_1} \cdots p_r^{e_r}$ be its prime decomposition. Then, $r \geq 1$ and

$$\sum_{d \mid n} \mu(d) = \sum_{(f_1, \ldots, f_r) \atop 0 \leq f_i \leq e_i} \mu(p_1^{f_1} \cdots p_r^{f_r}) = \sum_{(f_1, \ldots, f_r) \atop 0 \leq f_i \leq 1} \mu(p_1^{f_1} \cdots p_r^{f_r})$$

$$= \sum_{0 \leq k \leq r} \binom{r}{k} (-1)^k = (1 - 1)^r = 0.$$

Here, we counted tuples $(f_1, \ldots, f_r) \in \{0, 1\}^r$ by first fixing the number $k$ of entries that are equal to 1 and then determining the number of such tuples as the binomial coefficient $\binom{r}{k}$. \hfill \square

The explicit formula in the next theorem is due to Richard Brauer.

10.3 Theorem For every $\chi \in R(G)$ one has

$$\chi = \frac{1}{|G|} \sum_{\substack{K \leq H \leq G \\ H \text{ cyclic}}} |K| \cdot \mu([H : K]) \cdot \text{ind}_K^G(\text{res}_K^G(\chi)). \quad (10.3.a)$$
In particular, one has

\[ R(G) \subseteq \frac{1}{|G|} \sum_{\substack{H \leq G \cap \text{cyclic}}} \text{ind}_H^G(R(H)) \quad \text{and} \quad \mathbb{Q}R(G) = \sum_{\substack{H \leq G \cap \text{cyclic}}} \text{ind}_H^G(\mathbb{Q}R(H)), \]

where \( \mathbb{Q}R(G) \) denotes the \( \mathbb{Q} \)-span of \( \text{Irr}(G) \).

**Proof** First we prove the Equation (10.3.a) in the case where \( \chi = 1_G \), the trivial character of \( G \). The right hand side of the equation evaluated at the element \( x \in G \) is equal to

\[
\frac{1}{|G|} \sum_{\substack{H \leq G \cap \text{cyclic}}} |K| : \mu([H : K]) \cdot \frac{1}{|K|} \sum_{\substack{g \in G \cap \text{cyclic}}} 1
\]

\[
= \frac{1}{|G|} \sum_{\substack{H \leq G \cap \text{cyclic}}} \sum_{g \in G \cap \text{cyclic}} \sum_{g^{-1}xg \in K} \mu([H : K])
\]

\[
= \frac{1}{|G|} \sum_{\substack{H \leq G \cap \text{cyclic}}} \sum_{g \in G \cap \text{cyclic}} \sum_{g^{-1}xg \in H} \mu(d)
\]

\[
= \frac{1}{|G|} \sum_{\substack{H \leq G \cap \text{cyclic}}} \sum_{g \in G \cap \text{cyclic}} \delta_{H,g^{-1}\langle x \rangle} g
\]

\[
= \frac{1}{|G|} \sum_{g \in G \cap \text{cyclic}} 1 = 1,
\]

and the equation holds in this case. For the second equality we used that a cyclic group of order \( n \) has precisely one subgroup of order \( d \), for every divisor \( d \) of \( n \). For the third equality we used Lemma 10.2.

Next, let \( \chi \in R(G) \) be arbitrary. Using the formula for trivial character
and the Frobenius property in Theorem 7.7, we obtain

\[
\chi = \chi \cdot 1_G = \chi \cdot \frac{1}{|G|} \sum_{\substack{K \leq H \leq G \\text{cyclic}}} |K| \cdot \mu([H : K]) \cdot \text{ind}_K^G(\text{res}_K^G(1_G))
\]

\[
= \frac{1}{|G|} \sum_{\substack{K \leq H \leq G \\text{cyclic}}} |K| \cdot \mu([H : K]) \cdot (\chi \cdot \text{ind}_K^G(1_K))
\]

\[
= \frac{1}{|G|} \sum_{\substack{K \leq H \leq G \\text{cyclic}}} |K| \cdot \mu([H : K]) \cdot \text{ind}_K^G(\text{res}_K^G(\chi)) \cdot 1_K
\]

proving Equation (10.3.a) in the general case. The last two statements in the Theorem are immediate consequences of the formula for \( \chi \) in Equation (10.3.a).

The following immediate corollary is often referred to as Artin’s induction theorem. It was first proved by Emil Artin in a different way, before Brauer found the explicit formula in the above theorem.

**10.4 Corollary (Artin’s induction theorem)** For every \( \chi \in R(G) \) there exist cyclic subgroups \( H_1, \ldots, H_n \) of \( G \) (not necessarily distinct), rational numbers \( a_1, \ldots, a_n \), and irreducible characters \( \varphi_i \in \text{Irr}(H_i) \), \( i = 1, \ldots, n \), such that \( \chi \) can be expressed as

\[
\chi = \sum_{i=1}^n a_i \cdot \text{ind}_{H_i}^G(\varphi_i).
\]

**Proof** This follows immediately from the explicit formula for \( \chi \) in Equation (10.3.a).

**10.5 Definition** A finite group \( G \) is called **supersolvable** if it has a normal series

\[
1 = G_0 \leq G_1 \leq \cdots \leq G_n = G, \quad (G_i \leq G)
\]

such that \( G_i/G_{i-1} \) is cyclic for all \( i = 1, \ldots, n \).
10.6 Remark (a) Every finite nilpotent group (i.e., direct product of $p$-groups) is supersolvable. On the other hand, every supersolvable group is solvable.

(b) Subgroups and factor groups of supersolvable groups are again supersolvable. This is proved in the same way as the analogous result for solvable groups.

(c) The group Alt(4) is solvable but not supersolvable. In fact, Alt(4) does not have a normal cyclic subgroup.

10.7 Definition (a) A character $\chi$ of $G$ is called monomial if $\chi$ can be written as a sum of characters of the form $\text{ind}^G_H(\varphi)$ with $H \leq G$ and $\varphi \in \text{Irr}(H)$ of degree 1. This is equivalent to requiring that there exists a representation of $G$ with character $\chi$ which takes values in the subgroup of monomial matrices, i.e., matrices which have precisely one non-zero entry in each row and each column.

(b) The group $G$ is called monomial if every character of $G$ is monomial. This is equivalent to the condition that every irreducible character of $G$ is of the form $\text{ind}^G_H(\varphi)$ with $H \leq G$ and $\varphi \in \text{Irr}(H)$ of degree 1. Obviously, abelian groups are monomial. But for instance, Alt(5) is not monomial (since it has an irreducible character of degree 3, but no subgroup of order 20).

10.8 Remark Let $N \leq H \leq G$ with $N \trianglelefteq G$ and let $\psi \in R(H/N)$. Then

$$\inf^G_{G/N}(\text{ind}^{G/N}_H(\psi)) = \text{ind}^G_H(\inf^H_{H/N}(\psi)).$$

This is an easy verification, noting that if $g_1, \ldots, g_n \in G$ is a set of representatives of $G/H$ then $g_1 N, \ldots, g_n N \in G/N$ is a set of representatives of $(G/N)/(H/N)$.

10.9 Proposition (a) If $G$ is supersolvable and not abelian then $G$ has a normal abelian subgroup $A$ which is not contained in $Z(G)$.

(b) If $G$ is supersolvable then $G$ is monomial.

Proof (a) Set $Z := Z(G)$. Then $G/Z$ is a non-trivial supersolvable group. Therefore, it has a non-trivial normal cyclic subgroup $A/Z$. Since $Z \leq Z(A)$ and $A/Z$ is cyclic, the group $A$ is abelian, and it is clearly not contained in $Z$.

(b) We prove the statement by induction on $|G|$. If $|G| = 1$ then $G$ is monomial. Assume that $|G| > 1$. We may assume that $G$ is not abelian,
since otherwise $G$ is clearly monomial. Let $\chi \in \text{Irr}(G)$. We need to show that $\chi = \text{ind}_K^G(\varphi)$ for some $K \leq G$ and $\varphi \in \text{Irr}(K)$ with $\varphi(1) = 1$. By Remark 10.8 we may also assume that $\chi$ is faithful, i.e., $\ker(\chi) = 1$. Let $\Delta: G \to \text{GL}_n(\mathbb{C})$ be a representation with character $\chi$. Then $\Delta$ is injective. By Part (a) there exists a normal abelian subgroup $A$ of $G$ which is not contained in $Z(G)$. Let $a \in A \setminus Z(G)$. Since $a \notin Z(G)$ and since $\Delta$ is injective, we have $\Delta(a) \notin Z(\Delta(G))$. This implies that $\Delta(a)$ is not a scalar matrix. By Theorem 9.2(b), we have $\text{res}_A^G(\chi) = e \sum_{g \in G/H} g^* \psi$, for some $e \in \mathbb{N}$ and some $\psi \in \text{Irr}(A)$, where $H := \text{stab}_G(\psi)$. Note that $\psi$ is a character of degree 1, since $A$ is abelian. Since $\Delta(a)$ is not a scalar matrix, we obtain that $H < G$ is a proper subgroup. Theorem 9.2(c) implies that $\chi = \text{ind}_H^G(\theta)$ for some $\theta \in \text{Irr}(H)$. By induction, $\theta = \text{ind}_K^H(\varphi)$ for some $K \leq H$ and $\varphi \in \text{Irr}(K)$ with $\varphi(1) = 1$. Altogether, we obtain $\chi = \text{ind}_H^G(\theta) = \text{ind}_H^G(\text{ind}_K^H(\varphi)) = \text{ind}_K^G(\varphi)$. This completes the proof. 

10.10 Remark (a) In general, subgroups of monomial groups are not monomial, but factor groups of monomial groups are again monomial.

(b) One has a sequence of implications:

$$G \text{ supersolvable } \Rightarrow G \text{ monomial } \Rightarrow G \text{ solvable.}$$

In fact, the first implication is the content of Proposition 10.9(b). The second implication can be found in [I, Theorem 5.12 and Corollary 5.13]. We will not use the second one.

10.11 Definition Let $\mathcal{H}$ be a set of subgroups of $G$. We set

$$\mathcal{R}(G, \mathcal{H}) := \{ f \in \text{CF}(G, \mathbb{C}) \mid f|_H \in R(H) \text{ for all } H \in \mathcal{H} \}$$

$$= \bigcap_{H \in \mathcal{H}} (\text{res}_H^G)^{-1}(R(H))$$

and

$$\mathcal{I}(G, \mathcal{H}) := \langle \text{ind}_H^G(\psi) \mid H \leq G, \psi \in R(H) \rangle_\mathbb{Z} = \sum_{H \in \mathcal{H}} \text{ind}_H^G(R(H)).$$

Obviously, these two sets are additive subgroups of $\text{CF}(G, \mathbb{C})$ and one has

$$\mathcal{I}(G, \mathcal{H}) \subseteq R(G) \subseteq \mathcal{R}(G, \mathcal{H}). \quad (10.11.a)$$
\textbf{10.12 Lemma} Let $\mathcal{H}$ be a set of subgroups of $G$.

(a) The set $\mathcal{R}(G, \mathcal{H})$ is a subring of the ring $\mathcal{C}F(G, \mathbb{C})$.

(b) The set $\mathcal{I}(G, \mathcal{H})$ is an ideal of the ring $\mathcal{R}(G, \mathcal{H})$.

(c) One has $1_G \in \mathcal{I}(G, \mathcal{H})$ if and only if $\mathcal{I}(G, \mathcal{H}) = \mathcal{R}(G) = \mathcal{R}(G, \mathcal{H})$.

\textbf{Proof} (a) Clearly, the trivial character $1_G$ is contained in $\mathcal{R}(G, \mathcal{H})$. Moreover, since $\text{res}_H^G : \mathcal{C}F(G, \mathbb{C}) \to \mathcal{C}F(H, \mathbb{C})$ is a ring homomorphism for all $H \leq G$ and since $\mathcal{R}(H)$ is a subring of $\mathcal{C}F(H, \mathbb{C})$, the preimage $(\text{res}_H^G)^{-1}(\mathcal{R}(H))$ is a subring of $\mathcal{C}F(G, \mathbb{C})$. Since intersections of subrings of $\mathcal{C}F(G, \mathbb{C})$ are again subrings, also $\mathcal{R}(G, \mathcal{H})$ is a subring of $\mathcal{C}F(G, \mathbb{C})$.

(b) Let $\chi \in \mathcal{R}(G, \mathcal{H})$ and let $\sum_{H \in \mathcal{H}} a_H \text{ind}_H^G(\psi_H) \in \mathcal{I}(G, \mathcal{H})$ with $a_H \in \mathbb{Z}$ and $\psi_H \in \mathcal{R}(H)$ for $H \in \mathcal{H}$. Then the Frobenius Property, cf. Theorem 7.7, implies

$$
\chi \cdot \sum_{H \in \mathcal{H}} a_H \text{ind}_H^G(\psi_H) = \sum_{H \in \mathcal{H}} a_H \text{ind}_H^G(\text{res}_H^G(\chi) \cdot \psi_H) \in \mathcal{I}(G, H),
$$

since $\text{res}_H^G(\chi) \in \mathcal{R}(H)$.

(c) This follows immediately from Part (b) and the chain of inclusions in (10.11.a).

\textbf{10.13 Definition} Let $p$ be a prime. A finite group is called a $p'$-group if its order is not divisible by $p$. A finite group $E$ is called $p$-elementary if $E = C \times P$ is the direct product of a cyclic $p'$-subgroup $C$ of $E$ and a $p$-subgroup $P$ of $E$. A group is called elementary if it is $p$-elementary for some prime $p$. We write $\mathcal{E}_p(G)$, resp. $\mathcal{E}(G)$, for the set of $p$-elementary, resp. elementary, subgroups of $G$. Note that elementary groups are nilpotent and therefore supersolvable and monomial. Note also that subgroups and factor groups of $p$-elementary groups are again $p$-elementary.

\textbf{10.14 Theorem (Brauer’s induction theorem, 1947)} (a) One has

$$
\mathcal{I}(G, \mathcal{E}(G)) = \mathcal{R}(G) = \mathcal{R}(G, \mathcal{E}(G)).
$$

(b) Every virtual character $\chi \in \mathcal{R}(G)$ can be written in the form

$$
\chi = \sum_{i=1}^n a_i \cdot \text{ind}_{E_i}^G(\varphi_i)
$$
with $a_i \in \mathbb{Z}$, $E_i \in \mathcal{E}(G)$ (not necessarily distinct), and $\varphi_i \in \text{Irr}(E_i)$ of degree 1, for $i = 1, \ldots, n$.

(c) A class function $f \in \text{CF}(G, \mathbb{C})$ is a virtual character of $G$ if and only if, for every elementary subgroup $E$ of $G$, its restriction $f|_E$ is a virtual character of $E$.

10.15 Remark Part (b) in the above theorem (usually referred to as Brauer's induction theorem) follows immediately from Part (a) and Proposition 10.9(b). Part (c) in the above theorem (usually referred to as Brauer's characterization of virtual characters) is just a reformulation of the equation $R(G) = \mathcal{R}(G, \mathcal{E}(G))$ in Part (a). Therefore, it suffices to prove Part (a) of the above theorem. In order to prove Part (a) it suffices, by Lemma 10.12, to show that the trivial character $1_G$ of $G$ is contained in $\mathcal{I}(G, \mathcal{E}(G))$. The remainder of this section is devoted to prove this. The eventual proof will proceed by induction on $|G|$.

10.16 Lemma (Banaschewski) Let $X$ be a finite non-empty set and let $R$ be a non-unitary subring of the ring $F(X, \mathbb{Z})$ of functions from $X$ to $\mathbb{Z}$ (i.e., a multiplicatively closed additive subgroup which does not contain the constant function $1_X$ with value 1). Then there exists an element $x \in X$ and a prime $p$ such that $p \mid f(x)$ for all $f \in R$.

Proof For each $x \in X$, consider the additive subgroup

$$I_x := \{f(x) \mid f \in R\}$$

of $\mathbb{Z}$. If, for some $x \in X$, the subgroup $I_x$ is a proper subgroup of $\mathbb{Z}$ then there exists a prime $p$ such that $I_x \subseteq p\mathbb{Z}$ and we are done. So assume that $I_x = \mathbb{Z}$ for all $x \in X$. We will derive a contradiction. In fact, in this case, for every $x \in X$, there exists a function $f_x \in R$ such that $f_x(x) = 1$. Thus, for every $x \in X$, the function $f_x - 1_X$ vanishes at $x$. This implies that the the function $\prod_{x \in X}(f_x - 1_X)$ is the 0-element in $R$. But expanding this product, yields an expression of $1_X$ as a $\mathbb{Z}$-linear combination of products of some of the elements $f_x \in R$. Since $R$ is multiplicatively closed and also an additive subgroup, we obtain $1_X \in R$. This is a contradiction, and the proof of the lemma is complete.

10.17 Definition We set

$$P(G) := \langle \text{ind}_H^G(1_H) \mid H \leq G \rangle_{\mathbb{Z}} \subseteq R(G).$$
The set \( P(G) \) is called the ring of \textit{virtual permutation characters} of \( G \). (It is the subgroup of \( R(G) \) generated by characters of permutation representations, i.e., representations which take values in permutation matrices.) More generally, if \( \mathcal{H} \) is a set of subgroups of \( G \) we set

\[
P(G, \mathcal{H}) := \langle \text{ind}^G_H(1_H) \mid H \in \mathcal{H} \rangle \subseteq P(G).
\]

Note that, for each \( H \leq G \), the character \( \text{ind}^G_H(1_H) \) takes values in \( \mathbb{Z} \). Thus \( P(G) \subseteq F(G, \mathbb{Z}) \). Note also that \( P(G, \mathcal{H}) \subseteq I(G, \mathcal{H}) \).

10.18 Lemma (a) The subgroup \( P(G) \) is a unitary subring of \( R(G) \).

(b) Assume that \( \mathcal{H} \) is a set of subgroups of \( G \) which is closed under taking subgroups, i.e., if \( H \in \mathcal{H} \) and \( K \leq H \) then \( K \in \mathcal{H} \). Then \( P(G, \mathcal{H}) \) is an ideal of \( P(G) \).

\textbf{Proof} First note that \( 1_G = \text{ind}^G_G(1_G) \in P(G) \). Moreover, for any subgroups \( H \) and \( K \) of \( G \), by Corollary 7.12, we have

\[
\text{ind}^G_H(1_H) \cdot \text{ind}^G_K(1_K) = \sum_{g \in H \setminus G/K} \text{ind}^G_{H \cap gK}(1_{H \cap gK}).
\]

This proves both Part (a) and Part (b) of the Lemma. \( \square \)

10.19 Definition Let \( p \) be a prime. A finite group \( H \) is called \textit{\( p \)-quasi-elementary} if \( H \) has a normal cyclic \( p' \)-subgroup \( C \) such that \( H/C \) is a \( p \)-group. Note that this implies that \( H = C \times P \) for any Sylow \( p \)-subgroup \( P \) of \( H \). Moreover, \( H \) is called \textit{quasi-elementary} if \( H \) is \( p \)-quasi-elementary for some prime \( p \). We denote by \( \mathcal{QE}_p(G) \) and \( \mathcal{QE}(G) \) the set of \( p \)-quasi-elementary and the set of quasi-elementary subgroups of \( G \), respectively. Note that subgroups and factor groups of \( p \)-quasi-elementary groups are again \( p \)-quasi-elementary. Also note that every \( p \)-elementary group is \( p \)-quasi-elementary. Thus, \( \mathcal{E}_p(G) \subseteq \mathcal{QE}_p(G) \) and \( \mathcal{E}(G) \subseteq \mathcal{QE}(G) \).

10.20 Lemma Let \( x \in G \) and let \( p \) be a prime. Then there exists \( H \in \mathcal{QE}_p(G) \) such that \( p \nmid (\text{ind}^G_H(1))(x) \).

\textbf{Proof} We can write \( \langle x \rangle = C \times D \), with \( C \) a cyclic \( p' \)-subgroup and \( D \) a cyclic \( p \)-subgroup of \( \langle x \rangle \). Set \( N := N_G(C) \) and note that \( \langle x \rangle \trianglelefteq N \). Since \( \langle x \rangle/C \cong D \) is a \( p \)-group, we may choose a Sylow \( p \)-subgroup \( H/C \) of \( N/C \) containing \( \langle x \rangle/C \). Then \( \langle x \rangle \trianglelefteq H \) and \( H \in \mathcal{QE}_p(G) \).
We will show that $p$ does not divide the character value $(\text{ind}_H^G(1_H))(x)$. This character value is given by

$$(\text{ind}_H^G(1_H))(x) = |\{gH \in G/H \mid g^{-1}xg \in H\}|.$$ 

But, for $g \in G$, we have

$$xgH = gH \iff g^{-1}xg \in H \iff g^{-1}(x)g \leq H \Rightarrow g^{-1}Cg \leq H$$

$$\Rightarrow g^{-1}Cg = C \Rightarrow g \in N \Rightarrow gH \in N/H.$$

Therefore, the character value $(\text{ind}_H^G(1_H))(x)$ is equal to the number of fixed points of the $\langle x \rangle$-set $N/H$ under the usual action by left multiplication. For $c \in C$ and $n \in N$ we have $cnH = n(n^{-1}cn)H = nH$, since $n^{-1}cn \in C$. Thus, every element of $N/H$ is fixed by $C$, and the number of $\langle x \rangle$-fixed points of $N/H$ is equal to the number of $D$-fixed points of $N/H$. Since $D$ is a $p$-group, the number of $D$-fixed points of $N/H$ is congruent to $|N/H|$ modulo $p$. Since $|N/H|$ is not divisible by $p$, the number of $D$-fixed points is not divisible by $p$, and the proof is complete.

10.21 Proposition (L. Solomon) The trivial character $1_G$ of $G$ is contained in $P(G, \mathcal{Q}\mathcal{E}(G))$.

Proof The additive subgroup $P(G, \mathcal{Q}\mathcal{E}(G))$ of the ring of functions $F(G, \mathbb{Z})$ is multiplicatively closed by Lemma 10.18(b). Assume that $1_G \notin P(G, \mathcal{Q}\mathcal{E}(G))$. Then, Lemma 10.16 implies that there exists $x \in G$ and a prime $p$ such that $p \mid \chi(x)$ for all $\chi \in P(G, \mathcal{Q}\mathcal{E}(G))$. But Lemma 10.20 implies that for this prime $p$ and this element $x$ there exists $H \in \mathcal{Q}\mathcal{E}_p(G)$ such that $p$ does not divide $(\text{ind}_H^G(1_H))(x)$. Since $\text{ind}_H^G(1_H) \in P(G, \mathcal{Q}\mathcal{E}(G))$, this is a contradiction, and the proof of the proposition is complete.

10.22 Lemma Assume that $G$ is $p$-nilpotent, i.e., $G$ has a semidirect product decomposition $G = N \rtimes P$ with $P \in \text{Syl}_p(G)$. Assume further that $\varphi \in \text{Irr}(N)$ with $\varphi(1) = 1$ and $^g \varphi = \varphi$ for all $g \in G$. Finally assume that $C_N(P) \leq \ker(\varphi)$. Then $\varphi = 1_N$, the trivial character of $N$.

Proof Set $K := \ker(\varphi) \trianglelefteq N$. Then $\varphi$ induces an injective homomorphism $\bar{\varphi} : N/K \to \mathbb{C}^\times$. Let $x \in N$. We will show that $x \in K$.

Since $^g \varphi = \varphi$ for all $g \in G$, we have $K \trianglelefteq G$ and obtain $\bar{\varphi}(g^{-1}xgK) = \bar{\varphi}(g^{-1}xKg) = \varphi(x) = \bar{\varphi}(xK)$. Thus, $xK = g^{-1}xgK = g^{-1}xKg$ for every
$g \in G$. This implies that $G$ and by restriction also $P$ acts on the coset $xK$ by conjugation, for every $x \in N$. Since $P$ is a $p$-group, the number of non-fixed points of $xK$ under this action is divisible by $p$. Since $|xK| = |K|$ is not divisible by $p$, $xK$ has at least one fixed point. Thus, $xK \cap C_N(P) \neq \emptyset$. But $C_N(P) \leq K$ by assumption. Thus, $xK \cap K \neq \emptyset$. This implies that $xK = K$. Since $x \in N$ was arbitrary, we have $K = N$ and $\varphi = 1_N$. \hfill $\Box$

Proof of Theorem 10.14. By Remark 10.15 it suffices to show that $1_G \in \mathcal{I}(G, \mathcal{E}(G))$. We will show this by induction on $|G|$. Using the transitivity of induction together with Lemma 10.12(e), it suffices to show that $1_G$ is a $\mathbb{Z}$-linear combination of characters of the form $\text{ind}_H^G(\psi)$ with $\psi \in \text{Irr}(H)$ and $H < G$. If $G$ is not quasi-elementary, we are done by Proposition 10.21. Therefore, we may assume that $G$ is quasi-elementary.

Then there exists a prime $p$ and a cyclic normal $p'$-subgroup $N$ of $G$ such that $G = NP$ and $N \cap P = \{1\}$ for all $P \in \text{Syl}_p(G)$. Set

$$Z := C_N(P) = \{x \in N \mid xy = yx \text{ for all } y \in P\} = Z(G) \cap N.$$ 

And note that $Z$ is normal in $G$. If $Z = N$ then $G$ is elementary and we are done. Hence, we may assume that $Z < N$. We choose $P \in \text{Syl}_p(G)$ and set $E := ZP < G$. Note that $E$ is elementary and that $NE = G$, since $P \leq E$.

We can write $\text{ind}_E^G(1_E) = 1_G + \theta$ with some character $0 \neq \theta$ of $G$ and we let $\chi \in \text{Irr}(G)$ denote an irreducible constituent of $\theta$. It suffices to show that $\chi$ is induced from a proper subgroup, since then $1_G = \text{ind}_E^G(1_E) - \theta \in \mathcal{I}(G, \mathcal{E}(G))$ by previous arguments.

This is what we show in this last paragraph. We have

$$1_N + \text{res}_N^G(\theta) = \text{res}_N^G(1_G + \theta) = \text{res}_N^G(\text{ind}_E^G(1_E))$$

$$= \sum_{g \in N \cap G/E} \text{ind}_N^E(\text{res}_N^E(\theta))$$

$$= \text{ind}_N^{N \cap E}(1_{N \cap E}) = \text{ind}_Z^N(1_Z),$$

since $N \cap E = N \cap PZ = (N \cap P)Z = Z$. Therefore,

$$(1_N + \text{res}_N^G(\theta), 1_N)_N = (\text{ind}_Z^N(1_Z, 1_N)_N = (1_Z, \text{res}_Z^N(1_N))_Z = (1_Z, 1_Z)_Z = 1.$$ 

This implies that $(1_N, \text{res}_N^G(\theta))_N = 0$ and also that $(1_N, \text{res}_N^G(\chi))_N = 0$. Now let $\varphi \in \text{Irr}(N)$ be an irreducible constituent of $\text{res}_N^G(\chi)$. Then $\varphi \neq 1_N$. We claim that $Z \leq \ker(\chi)$. In fact,

$$\text{res}_Z^G(\text{ind}_E^G(1_E)) = \sum_{g \in Z \cap G/E} \text{ind}_Z^Z(\chi, 1_{Z \cap E}) = |Z \cap G/E| \cdot 1_Z = |G/E| \cdot 1_Z,$$
since \( Z \cap gE = gZ \cap gE = (Z \cap E) = gZ = Z \), for every \( g \in G \), and since \( Z \) is normal in \( G \) and \( Z \trianglelefteq E \). But since \( \chi \) is a constituent of \( \text{ind}^E_G(1_E) \), also \( \text{res}^Z_G(\chi) \) is a multiple of \( 1_Z \). This proves the claim that \( Z \trianglelefteq \ker(\chi) \). Now, by Lemma 10.22, \( \varphi \) cannot be invariant under \( G \) and we have \( U := \text{stab}_G(\varphi) < G \). This implies that \( \chi = \text{ind}^U_G(\psi) \) for some \( \psi \in \text{Irr}(U) \) by Clifford theory, cf. Theorem 9.5. This completes the proof of Brauer’s induction theorem.

We finish with a few remarks related to Brauer’s Induction Theorem.

10.23 Remark (a) The motivation for Brauer’s Induction Theorem came from a question of E. Artin who asked if it is possible to write every character of \( G \) as a \( Z \)-linear combination of induced degree-1 characters (no restriction on the type of subgroups one induces from). Brauer’s Theorem gives a positive answer and it implies that so-called Artin L-functions (generalizations of the Riemann zeta-function) have nice properties predicted by Artin.

(b) A consequence of the theory of ”canonical induction formulas”, developed by the instructor, is that one has the explicit formula

\[
\chi = \sum_{(H_0, \varphi_0), \ldots, (H_n, \varphi_n) \text{ strict}} (-1)^n (\chi|_{H_n}, \varphi_n) \text{ ind}_{H_0}(\varphi_0)
\]

for all \( \chi \in R(G) \). Here the sum is taken over \( G \)-conjugacy classes of strictly ascending chains of pairs \((H, \varphi)\), where \( H \subseteq G \) and \( \varphi \in \text{Hom}(H, \mathbb{C}^\times) \). The partial order \((K, \psi) \leq (H, \varphi)\) is defined by \( K \leq H \) and \( \psi = \varphi|_H \). The same formula still holds if one only considers pairs \((H, \varphi)\), where \( H \) is a solvable subgroup of \( G \).

(c) The class of elementary subgroups of \( G \) is best possible in the following sense: Let \( \mathcal{H} \) be a class of subgroups of \( G \) which is closed under conjugation and taking subgroups and which satisfies \( R(G) = \sum_{H \in \mathcal{H}} \text{ind}_H^G(R(H)) \). Then \( \mathcal{E}(G) \subseteq \mathcal{H} \). This was proven by Green.

(d) A consequence of Brauer’s Induction Theorem is that every representation \( \Delta : G \to \text{GL}_n(\mathbb{C}) \) is equivalent to a representation \( \Delta' : G \to \text{GL}_n(\mathbb{Q}(\zeta)) \), where \( \zeta \) is a root of unity of order \( \exp(G) \).

Exercises

1. (a) Show that every finite nilpotent group is supersolvable.

   (b) Show that subgroups and factor groups of supersolvable groups are supersolvable.
2. (a) Show that $\text{SL}_2(\mathbb{F}_3)$ is not monomial. Is $\text{SL}_2(\mathbb{F}_3)$ solvable?
(b) Decide which of the irreducible characters of $\text{Alt}(5)$ is monomial.

3. (a) Show that subgroups and factor groups of $p$-elementary groups are again $p$-elementary.
(b) Show that subgroups and factor groups of $p$-quasi-elementary groups are again $p$-quasi-elementary.

4. Let $\Delta: G \to \text{GL}_n(\mathbb{C})$ be a representation of a finite group $G$. Show that the following are equivalent.
   (i) The representation $\Delta$ is equivalent to a representation with values in permutation matrices.
   (ii) There exists a $G$-set $X$ such that $\Delta$ corresponds to the $\mathbb{C}G$-module $\mathbb{C}X$.
   (iii) The character of $\Delta$ is of the form $\sum_{i=1}^{r} \text{ind}_{H_i}^{G}(1)$, for some $r \in \mathbb{N}$ and subgroups $H_1, \ldots, H_r$ of $G$.

References