GEIR ELLINGSRUD

MA4270—REPRESENTATION THEORY
Contents

1  Basics about representations   7

2  Representations of Abelian groups   37

3  Complete reducibility   49

4  Characters   83

5  Induction and Restriction   131

6  Induction theorems   163

7  Frobenius Groups   181

8  Some algebra   187

9  The symmetric groups   191
Introduction
1 Basics about representations

Preliminary version 0.2 as of 14th November, 2017
Changes: 22/8. Have tidied up here and there. Expanded the text on the Burnside ring. Corrected misprints. Added an example (1.6) and an exercise (1.9)
18/9: Corrected a stupidity in paragraph (1.8) on page 15.

The first time I gave this course, back in 2012, was initiated by students interested in physics; some were master- or phd-students in physics. Naturally this influenced the attitude toward the content, certainly with Lie-groups and their complex (or real) representations being center stage. However, this time I was approached by students in topology (with a bias towards number theory) to give the course, and naturally this changes the attitude. Still the complex representations will be the leading stars, but we shall to some extent pursue the theory over general fields (including fields of positive characteristic).

I also think it is appropriate to use the language of categories, it is not essential but clarifies things enormously (at least if you speak the language). And for those with intension of pursuing the subject in an algebraic direction, it will be essential.

Prerequisite knowledge:

• Basics of algebra (commutative and non-commutative)

• Basics of group theory

• Rudiments of categories and functors

• rudiments of topology and manifolds.

and of course a good bit of mathematical maturity.

(1.1) In this first part of the course groups will will tacitly be assumed to be finite. The order of a group $G$, that is the number of its elements, will be denoted by $|G|$. Groups are, with few exceptions, multiplicatively written, and
the group law will be denoted by juxtaposition (or occasionally with the classical dot), i.e., the product of $g$ and $h$ is denoted by $gh$ (or $g \cdot h$). The unit element will be denoted by $1$.

(1.2)—About ground fields. We fix a ground field $k$. To begin with no restrictions are imposed on $k$. We shall however not dig very deep into the theory when $k$ is of positive characteristic—our main interest will be in the case when $k$ is of characteristic zero—but we do what easily can be done in general without to much additional machinery. But of course when $k$ is algebraically closed, the theory is particularly elegant and simple.

The relation between the field and the group has a strong influence on the theory, basically in two different ways. Firstly, if the characteristic of $k$ is positive and divides the order $|G|$ the situation is markedly more complicated then if not. In the good case we call $k$ a field friendly for $G$; that is, when the characteristic of $k$ either is zero or relatively prime to the order $|G|$ of $G$.

Secondly, when $k$ in addition to being friendly is “sufficiently large”, the theory tends to be uniform and many features are independent of the field. In this case $k$ is called a big friendly field for $G$. For the moment, this is admittedly very vague, but in the end (after having proved a relevant theorem of Burnside), a field will be friendly if it contains $n$ different $n$-th roots of unity where $n$ is the exponent of $G$; equivalently the polynomial $t^n - 1$ splits into a product of $n$ different linear factors over $k$.

Every algebraically closed field of characteristic zero is big and friendly for every group. The all important example to have in mind is of course the field of complex numbers $\mathbb{C}$. Another field important in number theory, is the field of algebraic numbers $\mathbb{Q}$.

(1.3) To give a twist to a famous sentence from Animal Farm: “All groups are equal, but some groups are more equal that others”. Among the “more equal groups”, we shall meet the symmetric groups $S_n$, the alternating groups $A_n$, the dihedral groups $D_n$, the linear groups $\text{Gl}(\mathbb{F}_q, n)$ and $\text{Sl}(\mathbb{F}_q, n)$ over finite fields, the generalized quaternionic groups. And of course the cyclic groups $\mathbb{C}_n$. 

---

1 This is highly non-standard terminology, but a name is needed to avoid repeating the phrase “a field whose characteristic either is zero or positive and not dividing $|G|$”.

2 Recall: The exponent is smallest elements killing the whole $G$; or in less murderous terms, it is the least common multiple of the order of elements in $G$. The exponent divides the order $|G|$, but they are not necessary equal.
1.1 Definitions

In the beginning there will of course be lots of definition to make. The fundamental one is to tell what a representation is. When that is in place, we introduce the basic concepts related to representations, and the operations they can be exposed to. The development follows more or less a unifying pattern: Well known concepts from linear algebra are interpreted in the category of representations.

The first and fundamental concept

Given a finite group and a field $k$. A representation of $G$ afforded by the vector space $V$ over $k$ is a group homomorphism $\rho: G \rightarrow \text{Aut}(V)$; that is, a map such that $\rho(gh) = \rho(g) \circ \rho(h)$ and $\rho(1) = \text{id}_V$.

Equivalently one may consider a map $G \times V \rightarrow V$, temporarily denoted by $r$, satisfying the three requests

- $r(gh,v) = r(g,h,v)$ for all $g, h \in G$ and $v \in V$,
- $r(e,v) = v$ for all $v \in V$,
- $r(g,v)$ is $k$-linear as a function of $v$.

Or in short, the map $r$ is a $k$-linear action of $G$ on $V$. The link between the two notions is the relation $\rho(g) \cdot v = r(g,v)$. The two first conditions above are equivalent to $\rho$ being a homomorphism; and the third ensures that $\rho$ takes values in $\text{Aut}(V)$. Frequently and indiscriminately we shall use the term a linear $G$-action for a representation, and a third term will be a $G$-module—the reason for which will be clear later.

(1.1) In most of this course $V$ will be of finite dimension over $k$ and we say that $V$ is a finite representation. In the few cases when $V$ will be of infinite dimension, the field $k$ will either be $\mathbb{R}$ or $\mathbb{C}$, and both the vector space $V$ and the group $G$ will be equipped with some (nice) topologies. One says that the action is continuous if the map $r$ is continuous.

As a matter of convenience the reference to the map $\rho$ will most often be skipped and the action written as $gv$ or $g \cdot v$ in stead of $\rho(g)v$; also the notation $g|v$ for $\rho(v)$ will be in frequent use. In the same vein, we say that $V$ is a...
representation, the action of \( G \) being understood, and even the base field will sometimes be understood.

(1.2) Any vector space \( V \) affords a trivial action; i.e., one such that \( g \cdot v = v \) for all \( g \in G \) and all \( v \in V \). In case \( V = k \) we call it the trivial representation and denote it by \( k_G \) (or just by \( k \) if there is no imminent danger of confusion). The zero representation is, as the name indicates, the zero vector space with the trivial action.

The set of vectors \( v \in V \) that are invariant under all elements in \( G \) plays a special role in the story. It is a linear subspace denoted by \( V^G \). One has

\[
V^G = \{ v \in V \mid g \cdot v = v \text{ for all } g \in G \}.
\]

The notation is in concordance with the general notation \( X^G \) for the set of fixed points of an action of \( G \) on a set \( X \).

Examples

1.1. Let \( G \) be the symmetric group \( S_n \) on \( n \)-letters. Assume that \( V_n \) is a vector space of dimension \( n \) over \( k \) with a basis \( \{ e_i \}_{1 \leq i \leq n} \). Letting \( \sigma \in S_n \) act on basis elements \( \sigma \cdot e_i = e_{\sigma(i)} \) and extending this by linearity, one obtains a representation of \( G \) on \( V_n \).

1.2. Let \( x_1, \ldots, x_n \) be variables and let the symmetric group \( S_n \) act on the \( x_i \)-s by permutation; i.e., \( \sigma(x_i) = x_{\sigma(i)} \) for \( \sigma \in S_n \). For every natural number \( r \) this induces a representation of \( S_n \) on the space of homogenous of degree \( r \) polynomials in the \( x_i \) with coefficients in a field \( k \).

1.3. The (cyclic) subgroup \( \mu_n \) of the multiplicative group \( \mathbb{C}^* \) of non-zero complex numbers consisting of the \( n \)-th roots of unity acts by multiplication on \( \mathbb{C} \). The corresponding representation is one-dimensional and denoted by \( L(1) \).

1.4. Continuing the previous example, let \( m \) be an integer. One defines a representation \( \mu_n \) on \( \mathbb{C} \) by by letting a root of unity \( \eta \in \mu_n \) act via multiplication by the power \( \eta^m \). This representation is denoted by \( L(m) \).

1.5. —Permutation representations. Let \( G \) act on the finite set \( X \), and denote by \( L_k(X) \) the set of maps from \( X \) to \( k \). Then \( L_k(X) \) is a vector space over \( k \) whose dimension equals the number of elements in \( X \). The group \( G \) acts on
L_k(X) by the rule $g \cdot \phi(x) = \phi(g^{-1}(x))$. The inversion is there to make this an action; without it, we get an action of the opposite group $G^{op}$ frequently denoted by $\phi^g$.

1.6. Let $k$ be a field and $G = \text{Gl}(2, k)$ (so that $G$ is not finite unless $k$ is finite), then $G$ acts on polynomials in two variables $x$ and $y$ with coefficients in $k$ according to the formula

$$g \cdot f(x, y) = f(ax + by, cx + dy)$$

when

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The vector space $V_n$ of homogenous polynomials of degree with coefficients in $k$ is a representation of $G$ of dimension $n + 1$ over $k$.

**Problem 1.1.** Let $\delta_x$ be the indicator function of the singleton $\{x\}$; i.e., the function on $X$ that takes the value 1 on $x$ and vanishes elsewhere. Show that $\delta_x$’s for $x \in X$ form a basis for $L(X)$, and that the representation map expressed in that basis takes values in the set of permutation matrices, matrices with just one non-zero entry in each row and each column and that entry equaling one. Show that $g \cdot \delta_x = \delta_{gx}$.

**Equivariant maps**

As almost always is the case in mathematics, any new concept is accompanied by a corresponding new class of “maps”, which are the means to compare different species of the new objects. In short, one works with categories.

1.3—**Morphisms.** So also with representations. Let $V$ and $W$ be two representations of $G$ over $k$. A $k$-linear map $\phi: V \to W$ is said to be a morphism or a $G$-equivariant map if it is compatible with the $G$-actions; that is, if $\phi(g \cdot v) = g \cdot \phi(v)$ for all group elements $g \in G$ and all vectors $v \in V$. For short we shall often say a $G$-map or out of laziness even just a map.

The composition of two composable $G$-equivariant maps is $G$-equivariant, and of course, all identity maps are as well. So the representations form a category, and the finitely generated ones constitute a full subcategory. We shall denote the latter by $\text{Rep}_{G,k}$.

1.4 The set of $G$-equivariant maps from $V$ to $W$ is denoted by $\text{Hom}_G(V, W)$. It is the subspace of $\text{Hom}_k(V, W)$ consisting of the linear maps that commute with the two actions. In symbols, such a $\phi$ satisfies $g|_V \circ \phi = \phi \circ g|_V$ for all $g$. 

$$
\begin{array}{ccc}
V & \xrightarrow{\phi} & W \\
\downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\
V & \xrightarrow{\phi} & W
\end{array}
$$
The composition of two $G$-maps is a bilinear operation since composition of linear maps is; whence the representations form a $k$-linear category: The hom-sets are vector spaces over $k$ and composition is bilinear.

**Proposition 1.1** One has $\text{Hom}_G(V, W) = \text{Hom}_k(V, W)^G$.

In particular, taking for $W$ the trivial one dimensional representation $k_G$, one obtains a representation of $G$ on the dual space $V^* = \text{Hom}_k(V, k_G)$, which sometimes is called the contragredient representation.

**Problems**

1.2. Assume that $X$ and $Y$ are two finite $G$-sets and $f: X \to Y$ is an $G$-equivariant map (i.e., a map that commutes with the actions). Show that $\phi \mapsto \phi \circ f$ is a $G$-equivariant map $f^*: L(Y) \to L(X)$. Conclude that $L$ is a contravariant functor $\text{Sets}_G \to \text{Rep}_G$.

1.3. In the same context as the previous exercise let $f_*$ be the map $L(X) \to L(Y)$ that “integrates along the fibres of $f$”; that is

$$f_*(\phi)(y) = \begin{cases} 0 & \text{ if } y \notin f(X); \\ \sum_{f(x) = y} \phi(x) & \text{ else} . \end{cases}$$
Show that \( f_* : L(X) \to L(Y) \) is \( G \)-equivariant. Show that in case \( f \) is the inclusion of a subset \( X \) in \( Y \), then \( f_* \) identifies \( L(X) \) with the subspace of those functions that vanish on \( X \).

1.4. When \( L(X) \) is equipped with the “pointwise product” it becomes a ring. Let \( f : X \to Y \) is \( G \)-equivariant, show that \( f^* \) is a ring homomorphism and that the formula
\[
 f_*(\phi \cdot f^* \psi) = f_*(\phi) \cdot \psi
\]
holds.

1.5. Show that there is a natural \( G \)-equivariant isomorphism \( \text{Hom}_G(k_G, V) \cong V^G \).

Subrepresentations and direct sums

Given two representations \( V \) and \( W \), their direct sum is the representation having \( V \oplus W \) as underlying vector space and being endowed with the componentwise action \( G \) acting; that is, the action of and element \( g \) on the pair \((v, w)\) is \( g \cdot (v, w) = (g \cdot v, g \cdot w) \).

A \( k \)-linear subspace \( W \subseteq V \) is said to be invariant under \( G \) if \( g \cdot w \in W \) whenever \( g \in G \) and \( w \in W \). Clearly \( G \) acts linearly on \( W \), and gives a representation of \( G \) in \( W \). One calls \( W \) a subrepresentation of \( V \). The quotient space \( V/W \) of \( V \) by an invariant subspace \( W \) inherits in the obvious way an action of \( G \); the action of a group element \( g \) on a coset \( v + W \) is \( g \cdot v + W \).

Recall that a complement of subspace \( W \subseteq V \) is another subspace \( W' \) such that \( W + W' = V \) and \( W \cap W' = 0 \). Every element \( v \) is represented in a unique fashion as a sum of an element from \( W \) and one from \( W' \), and this allows \( V \) to be identified with the direct sum \( W \oplus W' \). An invariant subspace \( W \) may have an invariant complement or not, in case \( W \) has, one says that \( W \) lies split in \( V \). The decomposition of \( V \) as the direct sum \( W \oplus W' \) is then respected by the action of \( G \).

Example 1.7. Referring to the representation \( V_n \) from example 1.1 above, the subspace whose members \( \sum_i a_i e_i \) satisfy \( \sum_i a_i = 0 \), is a subrepresentation. In
case $k$ is a friendly field for $S_n$ (i.e., the characteristic of $k$ does not divide $n$), it lies split in $V_n$ with the subspace generated by the vector $\sum_i e_i$ as a complement.

**Problem 1.6.** Assume that $X$ is a finite $G$-set that is the disjoint union of two $G$-invariant subsets $X'$ and $X''$. Show that $G$-modules it holds true that $L(X) = L(X') \oplus L(X')$ as $G$-modules. Conclude that if $X = \bigcup_i X_i$ is the decomposition of $X$ into orbits, then $L(X) = \bigoplus_i L(X_i)$. *

**Kernels and cokernels**

The kernel of a $G$-equivariant map $\phi : V \to W$ is obviously a subrepresentation of $V$; indeed, $\phi(g \cdot v) = g \cdot \phi(v) = 0$ for vectors $v \in \ker \phi$. Similarly, the image $\text{im} \phi$ is a subrepresentation of $W$ and the cokernel $\phi$ is a quotient representation of $W$. For those with the terminology of categories as mother tongue: The category $\text{Rep}_{G,k}$ is an abelian $k$-linear category.

**Tensor products**

The tensor product $V \otimes_k W$ of two representations $V$ and $W$ of $G$ has the tensor product of the two underlying linear spaces as representation space, and the action of $G$ is given on decomposable tensors by $g \cdot v \otimes w = (g \cdot v) \otimes (g \cdot w)$ and subsequently extended by linearity (possible since the expression $(g \cdot v) \otimes (g \cdot w)$ is bilinear in $v$ and $w$).

(1.7) All the usual formulae, like additivity and associativity, for tensor products of vector spaces carry over to tensor products of representations. Notably, one has the important relation

$$\text{Hom}_k(V, W) \simeq V^* \otimes W$$

(1.1)

between the hom-space $\text{Hom}_k(V, W)$ and the product of the contragredient $V^*$ with $W$. The isomorphism is canonical, inherited from the vector space case, and is most easily defined as a map from the right side to the left. One sends a decomposable tensors $\phi \otimes w$ to $\phi(w)$ and then extends by linearity (which is possible since $\phi \otimes w$ is bilinear in $\phi$ and $w$). The isomorphism is functorial and additive in both variables, and it is straightforward to check that it is compatible with the action of $G$. 
Another important relation among vector spaces is the “adjoint relation” stating that there is natural (i.e., functorial in all three variables) isomorphism

\[ \Psi: \text{Hom}(U \otimes V, W) \simeq \text{Hom}(U, \text{Hom}(V, W)). \]

A map \( \phi: U \otimes V \to W \) is sent to the map \( \Psi \phi: U \to \text{Hom}(V, W) \) with \( \Psi \phi(u)(v) = \phi(u \otimes v) \). To check it is an isomorphism, one uses that \( \Psi \) is additive in \( U \) and induction on \( \dim U \). The induction takes off since \( U \) being one dimensional, obviously entails that \( \Psi \) is an isomorphism. In our context, when all three \( U, V \) and \( W \) are \( G \)-modules, the map \( \Psi \) will be \( G \)-equivariant, and so the “adjoint relation” continuous to hold in the category \( \text{Rep}_G, k \).

**Problem 1.7.** Show that there is a natural isomorphism \( V \otimes k_G \simeq V \). *

**Problem 1.8.** Assume that \( X \) and \( Y \) are two finite \( G \)-sets. Show that \( L(X \times y) = L(X) \otimes L(Y) \). *

### Symmetric and alternating products

In the category of vector spaces over a field there are two important constructions, namely symmetric powers and alternating powers. They are both quotient of the tensor algebra \( T(V) = \bigotimes_{n \geq 0} V^\otimes n \). If \( V \) is a \( G \)-module over the field \( k \) we are going to endow the symmetric and the alternating powers of \( V \) by actions of \( G \). Hence the category \( \text{Rep}_G, k \) has alternating and symmetric powers.

1.9—**Symmetric powers.** Recall the definition of \( \text{the symmetric power} \ Sym^n(V) \) of the vector space \( V \). It is the tensor power \( V^\otimes n = V \otimes V \ldots V \otimes V \) divided out by the linear subspace generated by tensors of the form

\[ v_1 \otimes \ldots \otimes v_i \otimes \ldots \otimes v_j \otimes \ldots \otimes v_n - v_1 \otimes \ldots \otimes v_j \otimes \ldots \otimes v_i \otimes \ldots \otimes v_n, \]

that is the difference of two decomposable tensors whose factors coincide except that two have been swapped. Because elements \( g \in G \) act on \( V^\otimes n \) by acting in each slot; that is

\[ g \cdot (v_1 \otimes \ldots \otimes v_n) = (g \cdot v_1) \otimes \ldots \otimes (g \cdot v_n), \]

this subspace is evidently invariant under \( G \), and consequently there is a \( G \)-action induced on the quotient \( \text{Sym}^n(V) \).

If \( v_1, \ldots, v_r \) are vectors from \( V \), not necessarily different, the nonomial \( m = v_1 \cdot \ldots \cdot v_r \) is the image of the decomposable tensor \( v_1 \otimes \ldots \otimes v_r \). The order of the \( v_i \)'s is immaterial since by definition of the subspace above any two factors
in $m$ can be swapped, and a repeated application shows that $m$ is invariant under any permutation of the factors. The action of an element $g$ on $m$ is given as $g \cdot m = (g \cdot v_{i_1}) \cdot \ldots \cdot (g \cdot v_{i_r})$.

In particular if $v_1, \ldots, v_r$ constitute a basis for $V$, the monomials $v_1^{i_1} \cdot \ldots \cdot v_r^{i_r}$ for the different choices of non-negative integers $n_i$ such that $\sum_i n_i = n$ form a basis for $\text{Sym}^n(V)$. The symmetric algebra $\text{Sym}(V) = \bigoplus_{n \geq 0} \text{Sym}^n(V)$ can then be identified with the polynomial algebra $k[v_1, \ldots, v_r]$, the graded piece of degree $n$ corresponding to $\text{Sym}^n(V)$.

**1.10—Alternating powers.** In a similar fashion (but with a *plus* in (1.2) above in stead of a minus) one obtains the *alternating powers* $\Lambda^n(V)$.

In this case, the image of $v_1 \otimes \ldots \otimes v_r$ is denoted by $v_1 \wedge \ldots \wedge v_r$. This monomial changes sign when two of the factors are swapped, and in particular it will vanish if two factors are equal. A general permutation of the factors gives a sign changes or not according to the permutation being even or odd.

One has

$$v_{\sigma(1)} \wedge \ldots \wedge v_{\sigma(r)} = \text{sign}(\sigma) v_1 \wedge \ldots \wedge v_r.$$ 

for any permutation $\sigma$ of $r$ letters.

Contrary to the symmetric powers, the alternating powers of $V$ are finite in number. When $n > \dim V$, it holds true that $\Lambda^n V = 0$. Indeed, in a monomial $m = v_1 \wedge \ldots \wedge v_n$, one of the vectors, say $v_i$, must be a linear combination of the others, and replacing $v_i$ with that combination expresses $m$ as a linear combination of monomials all with repeating factors; hence they all vanish.

Assume that $\{v_i\}_{1 \leq i \leq n}$ is a basis for $V$. One then has a basis for $\Lambda^r V$ formed by the vectors $\Lambda_{i \in I} v_i = v_{i_1} \wedge \ldots \wedge v_{i_r}$ where the set $\{i_j\}_{1 \leq j \leq r} = I$ runs over all subsets $I \subseteq [1, n]$ having $r$ elements. Notice that in this definition an order of $I$ must be chosen, so the basis elements are defined only to sign. In particular, the dimension of $\Lambda^r V$ equals the number of such subsets which is the binomial coefficient $\binom{n}{r}$; that is, one has $\dim \Lambda^r V = \binom{n}{r}$.

The representation of $G$ on $\Lambda^n V$ is one dimensional and often denoted by $\det V$.

**Problem 1.9.** Let $V$ be a two dimension vector space over $\mathbb{F}_q$. Chose a basis and argue that this gives an action of $\text{GL}(2, \mathbb{F}_q)$ on $V$. Argue that the representation in example 1.6 on page 11 is isomorphic to $\text{Sym}^2(V)$. *

**Extension of scalars**

Assume that $K$ is an extension field of $k$, and that $V$ a vector space over $k$, one then has the associated $K$-vector space $V_K = K \otimes_k V$. If $\{v_i\}$ is a basis for $V$, 

\[ 1 \]
then \(\{1 \otimes v_i\}\) is a basis for \(V_K\), and there is an obvious inclusion \(\text{Aut}_k(V) \subseteq \text{Aut}_K(V_K)\) given by \(\phi \mapsto \text{id}_K \otimes \phi\). In terms of matrices relative to a basis for \(V\), the map is just considering a matrix with entries in \(k\) to have entries in \(K\).

Any representation \(V\) over \(k\) extends to representation \(V_K = K \otimes_k V\) with \(g|_{V_K} = \text{id}_K \otimes g|_V\). The representation map is simply the composition of \(\rho_V\) with the canonical inclusion \(\text{Aut}_k(V)\) in \(\text{Aut}_K(V_K)\). Any representation over \(K\) that is isomorphic to \(V_k\) for some \(V\), is said to be defined over \(k\).

\[\text{Problem 1.10.}\] Show that “extension by scalars” is an exact, faithful and additive functor \(\text{Rep}_G, k \to \text{Rep}_G, K\) that respects tensor products and internal homs.

\[\text{Problem 1.11.}\] Show that if \(V \in \text{Rep}_G, k\) is such that \((V_K)^G \neq 0\), then \(V^G \neq 0\). Conclude that if \(V_K\) and \(W_K\) are isomorphic as representations of \(G\) over \(K\), then \(V\) and \(W\) are isomorphic (over \(k\)). \text{HINT:} The following exact sequence may be useful:

\[
0 \to V^G \to V \xrightarrow{\theta} \prod_{g \in G} V
\]

where the map \(\theta\) is defined as \(\theta(v) = (v - gv)_{g \in G}\).

\[\text{Functoriality}\]

Later on, under the heading induction and restriction, we shall intensively study the functorial properties of \(\text{Rep}_G, k\) when the group \(G\) varies. For the moment we contend ourselves to observe that any group homomorphism \(f: H \to G\) gives rise to a functor \(f^*: \text{Rep}_G, k \to \text{Rep}_H, k\). It simply composes the representations maps with \(f\); that is, if \(V\) is a representation whose representation map is \(\rho_V: H \to \text{Aut}(V)\), the the representation map of \(f^*V\) is given as \(\rho_{f^*V} = \rho_V \circ f\).

\[\text{(1.11)}\] In particular, any automorphism \(\phi\) of \(G\) induces a functor \(\phi^*\), whose image on \(V\) often will be denote by \(V^\phi\).

A frequently occurring situation, is when \(H \subseteq G\) is a normal subgroup. In that case the conjugation maps \(c_g\), defined as \(h \mapsto ghg^{-1}\), induce “auto-functors” \(c_g^*: \text{Rep}_G, k \to \text{Rep}_G, k\) and the effect of \(c_g^*\) on \(V\) will often be written \(V^g\).

\[\text{Problems}\]

\[1.12.\] Show that the the map in (1.1) above equivariant.
1.13. Show that map in (1.1) is an isomorphism. Hint: Do the vector space case by induction on the dimensions.

1.14. Show that the functor \( U \mapsto \text{Hom}_G(U \otimes V, W) \) from \( \text{Rep}_G \) to \( \text{Vect}_k \) is represented by \( \text{Hom}_k(V, W) \). This means that the representation \( \text{Hom}_k(V, W) \) is an internal hom in \( \text{Rep}_G \) in the terminology of xxx.

1.15. Referring to examples 1.3 and 1.4 above, let \( m \) and \( m' \) be two integers. Show that \( L(m) \otimes L(m') = L(m + m') \) and that \( \text{Hom}_G(L(m), L(m')) \cong L(m' - m) \). Conclude that \( L(m) \cong L(m') \) if and only if \( m \equiv m' \mod n \).

1.16. We refer to example 1.1 for the notation, but assume additionally that \( k \) is of characteristic zero. Let \( v_0 = \sum_i e_i \) and let \( V_0 \) the subspace of \( V_n \) generated by \( v_0 \). Moreover let \( \iota : V_0 \rightarrow V_n \) be the inclusion map.

Find an explicit equivariant map \( \pi : V_n \rightarrow V_0 \) with \( \pi \circ \iota = \iota \). Let \( V_{n-1} \) be the kernel of \( \pi \). Determine an explicit equivariant map \( V_n \rightarrow V_{n-1} \) being a section to the inclusion \( V_{n-1} \rightarrow V_n \). Show that \( V_0 \) is the only proper and non-zero subrepresentation of \( V_n \).

1.17. If \( \rho \) is an endomorphism of the \( n \)-dimensional space \( V \), show that \( \Lambda^n \rho : \Lambda^n V \rightarrow \Lambda^n V \) is multiplication by the determinant of \( \rho \). Conclude that if \( \rho : G \rightarrow \text{Aut}_k(V) \) is a representation, then \( \Lambda^n \rho g = \det \rho(g) \).

1.18. Assume that \( V \) a vector space of dimension \( n \) and \( \rho : G \rightarrow \text{Aut}_k(V) \) is a representation. Show that the map \( V \otimes \Lambda^{n-1} V \rightarrow \Lambda^n V \) that sends \( v \otimes \alpha \) to \( v \wedge \alpha \) is a perfect pairing respecting the action of \( G \). Conclude that \( V^* \otimes \det V = \Lambda^{n-1} V \) (which is the categorical version of what is known as Cramer’s rule in undergraduate courses in linear algebra).

1.19. Assume that \( V \) a vector space of dimension \( n \) and \( \rho : G \rightarrow \text{Aut}_k(V) \) is a representation. Let \( \{v_i\}_{1 \leq i \leq n} \) be a basis for \( v \) and let \( A(g) \) be the matrix of \( \rho(g) \) in that basis. Show that the \( n \) elements \( w_i = v_1 \wedge \ldots \wedge \widehat{v_i} \wedge \ldots \wedge v_n \) form a basis for \( \Lambda^{n-1} V \) and that the matrix of \( \Lambda^{n-1} \rho \) in that basis is the cofactor matrix \( A^{\text{cof}} \) of \( A \).

1.20. Show that \( V \otimes V \cong \text{Sym}^2(V) \oplus \Lambda^2 V \).

1.21. Assume that

\[
\begin{array}{c}
0 \rightarrow V' \rightarrow V \rightarrow V'' \rightarrow 0
\end{array}
\]

is an exact sequence of representations \( G \) over \( k \). Show that there is a canonical isomorphism \( \det V \cong \det V' \otimes \det V'' \)

*
1.2 The group algebra

We start out with a commutative ring $R$, which in most of the course will be a field. Other examples to have in mind are $\mathbb{Z}$ or the ring of integers in some number field. Their localizations or completions in prime ideals as coefficient rings are frequently found in representation theory as well—they serve as an intermediate station between representations in characteristic $p$ and in characteristic zero.

The group algebra $R[G]$ has as underlying module a free $R$-module with a basis that is in a one-to-one correspondence with the elements of the group $G$, and we shall identify the basis elements with the elements of $G$. So a typical member of $R[G]$ is shaped like $\alpha = \sum_{g \in G} \alpha_g \cdot g$ where the coefficients $\alpha_g$’s are members of the ring $R$. The product of two basis elements from $R[G]$ is of course just defined as their product in the group (recall that the basis is identified with the group) and subsequently the product is extended to the whole of $R[G]$ by linearity; that is, one has

$$a\beta = (\sum_{g \in G} \alpha_g \cdot g)(\sum_{h \in G} \beta_h \cdot h) = \sum_{g \in G} (\sum_{h \in G} \alpha_{gh^{-1}} \beta_h) \cdot g.$$  

Of course $R[G]$ is non-commutative when $G$ is, and it is worth while noticing the following formula for $\beta\alpha$:

$$\beta\alpha = \sum_{g \in G} (\sum_{h \in G} \alpha_{gh^{-1}} \beta_h) \cdot g, \quad (1.3)$$

which follows from the equalities

$$\beta\alpha = \sum_{g} (\sum_{h} \beta_{gh^{-1}} \alpha_h) \cdot g = \sum_{g} (\sum_{t} \beta_t \alpha_{t^{-1}g}) \cdot g,$$

where we in the second has performed the substitution $t = gh^{-1}$; that is, $h = t^{-1}g$.

The universal property

The group algebra enjoys a universal property. Any homomorphism from $G$ to the group of units in an $R$-algebra $A$ can be extended uniquely to an $R$-algebra homomorphism $R[G] \to A$. Because the elements of $G$ form a $R$-linear basis for $R[G]$, the homomorphism extends naturally to a $R$-linear map $R[G] \to A$, and it is a matter of a simple computation to verify that the extension respects the product rule. We have:
Proposition 1.2 Let $R$ a commutative ring and $G$ a group, and let $A$ be an $R$-algebra. Every homomorphism from $G$ into the group of units of $A$ extends uniquely to an $R$-algebra homomorphism $R[G] \to A$.

(1.1) This universal property implies that the group algebra depends functorially on the group $G$. Any group homomorphism $\phi: H \to G$ extends uniquely to an algebra homomorphism $R[H] \to R[G]$; which we, without great risk of confusion, shall continue to denote by $\phi$. Moreover, the map sending $g$ to $g^{-1}$ is a homomorphism into the units of the opposite algebra $R[G]^{op}$ and induces a homomorphism that turns out to be an isomorphism between $R[G]$ and $R[G]^{op}$; indeed, the elements from $G$ form an $R$-linear basis in both. This is a particular property of groups algebras, not shared by many non-commutative rings.

Proposition 1.3 The inversion map $G \to G$ sending $g$ to $g^{-1}$ extends to an algebra isomorphism $\iota_G: R[G] \simeq R[G]^{op}$. The group algebra $R[G]$ is functorial in $G$, in way that respect the isomorphisms $\iota_G$.

Proof: It is clear that $\iota_G$ is an isomorphism of algebras since $g \to g^{-1}$ is an anti-automorphism (i.e., reverses the order of factors in products and is bijective) of the group $G$. Indeed, we have

$$\iota_G(\alpha \beta) = \iota_G(\sum_{g,h \in G} \alpha_g \alpha_h gh) = (\sum_{g,h \in G} \alpha_g \alpha_h h^{-1} g^{-1}) = \iota_G(\beta)\iota_G(\alpha).$$

If $\phi: G \to H$ is a group homomorphism it takes inverses to inverses and one has

$$\iota_H(\phi(\sum_g \alpha_g g)) = \sum_g \alpha_g \phi(g) = \sum_g \alpha_g \phi(g^{-1}) = \phi \iota_G(\sum_g \alpha_g g),$$

which shows that $\phi$ commutes with the two $\iota$-maps. \qed

(1.2) There is an $R$ algebra homomorphism $R[G] \to R$ sending $a = \sum_{g \in G} a_g g$ to $\sum_g a_g$ called the augmentation map. The kernel is a two sided ideal called the augmentation ideal. It is generated the elements of shape $g - 1$ for for $g \in G$. The augmentation map is a section of the canonical inclusion of $R$ in $R[G]$.

(1.3) When the coefficients is a field $k$, the group algebra $k[G]$ has another nice property of being a Frobenius algebra: it is self-dual. Let $A$ be an $k$-algebra of finite dimension. When we regard $A$ as a right module over itself, the space
Hom\(_k(A,k)\) of linear functionals is a left \(A\)-module with module structure given as \(a \cdot \phi(x) = \phi(xa)\). One says that \(A\) is a Frobenius algebra if \(A\) and \(A^*\) are isomorphic as \(A\)-modules.

**Lemma 1.1** A finite dimensional algebra \(A\) over a field is self-dual if there is a linear functional \(\lambda: A \to k\) which is symmetric, i.e., \(\lambda(xy) = \lambda(yx)\), and whose kernel does not contain any non-zero left ideals.

**Proof:** Define \(\Lambda: A \to A^*\) by \(\Lambda(y)(x) = \lambda(yx)\). It is an \(A\)-homomorphism since by the symmetry of \(\lambda\) one has \(a \cdot \Lambda(y)(x) = \lambda(yxa) = \lambda(axy) = \Lambda(a)(y)(x)\). That \(\Lambda(y) = 0\) means that \(\Lambda(y)(x) = \lambda(yx) = \lambda(xy) = 0\) for all \(x \in A\). Whence the principal left ideal generated by \(y\) is contained in the kernel of \(\lambda\), and one infers that \(y = 0\). So \(\Lambda\) is injective and therefore also surjective since \(A\) and \(A^*\) have the same dimension over \(k\).

The importance of being Frobenius is to self injective; that is \(A\) injective as a module over it self. Indeed, \(A^*\) is always injective; namely, if we are given a diagram of left modules

\[
\begin{array}{ccc}
0 & \to & Y & \to & X \\
\downarrow & & \downarrow & & \downarrow \\
A^* & \to & \text{X}^* & \to & 0
\end{array}
\]

where the dotted arrow is to be filled in, we dualize it to get one of right \(A\)-modules

\[
\begin{array}{ccc}
Y^* & \to & X^* & \to & 0 \\
\uparrow & & \uparrow & & \uparrow \\
A^* & \to & \text{X} & \to & 0
\end{array}
\]

Since \(A\) is projective, this second diagram can be filled in. Dualizing back we see that the first can be filled in as well.

**Proposition 1.4** For any field \(k\) the group algebra \(k[G]\) is Frobenius, and hence self-injective.

**Proof:** It suffices to exhibit a linear functional \(\lambda: k[G] \to k\) as in the lemma: Send \(\sum g \alpha_g\) to the coefficient of 1; that is to \(\alpha_1\). It is symmetric, since the coefficient of 1 in \(a\beta\) being equal to \(\sum_{h \in G} a_h \beta_h\) does not change when \(h\) and \(h^{-1}\) are swapped (since \(h\) runs through \(G\) when \(h^{-1}\) does). Moreover, if \(I\) is a left ideal lying in the kernel, and \(\alpha = \sum g \alpha_g \in I\), it follows that \(g^{-1} \alpha \in I\), but the coefficient of 1 in \(g^{-1} \alpha\) equals \(\alpha_g\). Hence \(\alpha = 0\).
Examples

1.8. Consider the cyclic group \( C_n \) of order \( n \). Sending the powers \( g^i \) of a generator \( g \) for \( C_n \) to \( t^i \) gives an isomorphism \( R[C_n] \cong R[t]/(t^n - 1) \); indeed, \( \{1, t, t^2, \ldots, t^{n-1}\} \) is a cyclic subgroup of the units in \( R[t]/(t^n - 1) \) that \( C_n \) maps isomorphically onto.

1.9. The group algebra \( R[C_2 \times C_2] \) is isomorphic to \( A = R[u, v]/(u^2 - 1, v^2 - 1) \) since \( \{1, u, v, uv\} \) is a subgroup of the units in \( A \) isomorphic to \( C_2 \times C_2 \).

1.10. We saw in the two previous examples that it holds true that \( C[C_4] \cong C[t]/(t^4 - 1) \) and \( C[C_2 \times C_2] \cong C[u, v]/(u^2 - 1, v^2 - 1) \). These two algebras are both isomorphic to the direct product \( \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \) of four copies of \( \mathbb{C} \) (See exercise 1.23 below).

The inversion maps, however, are different. In \( C[u, v]/(u^2 - 1, v^2 - 1) \) the inversion map is simply the identity (since elements in in \( C_2 \times C_2 \) are their own inverse), whereas in \( C[t]/(t^4 - 1) \) it exchanges \( t \) and \( t^3 \) and leaves \( t^2 \) invariant. This illustrates that the inversion map \( \iota_G \) is part of the group ring structure. And in the present case it distinguishes the two group algebras.

Problems

1.22. Show that the augmentation ideal is generated by elements of shape \( 1 - g \) for \( g \in G \).

1.23. Let \( k \) be a field containing a fourth root of unity which we denote by \( i \) (hence \( k \) is not of characteristic two). Show that both the \( k \)-algebras \( k[C_4] \) and \( k[C_2 \times C_2] \) are isomorphic to the product \( k \times k \times k \times k \) of four copies of \( k \).

HINT: Evaluate respectively at the four point sets \( \{ (\pm 1, \pm 1) \} \) and \( \{ i, -1, -i, 1 \} \).

The categories \( \text{Rep}_{k,G} \) and \( \text{Mod}_{k[G]} \)

The representation map \( \rho: G \to \text{Aut}_k(V) \), where \( V \) is a representation of \( G \) over a commutative ring \( R \), extends by the universal property to an algebra homomorphism \( R[G] \to \text{End}_R(V) \), which we still denote by \( \rho \). At an element \( \alpha = \sum_{g \in G} a_g \cdot g \) of the group algebra it takes the value \( \rho(\alpha) = \sum_{g \in G} a_g \rho(g) \). To ease the notation we shall frequently write \( \alpha|_V \) in stead of the heavier \( \rho(\alpha) \).
Giving a representation of $G$ in the free module $V$ over $R$ is thus equivalent to giving $V$ a $R[G]$-module structure. This is one of the main motivations for introducing the group algebra $R[G]$; it allows us to draw on the theory of finite dimensional algebras, and in the the non-friendly case that $R$ is a field whose characteristic divides $|G|$, this of is paramount importance. And of course, equally important, it makes it possible to work with linear combinations of the operators $g|_V$ in a “universal” way.

(1.4) The term a $G$-module will frequently be used synonymously with a representation of $G$, and we say that $V$ is a finite $G$-module if $V$ is finitely generated over $R$. The base ring (which mostly will be a base field) will most often tacitly be understood.

(1.5) When $V$ and $W$ are two representations of $G$ over a field $k$, one obviously has the equality $\text{Hom}_{k[G]}(V, W) = \text{Hom}_G(V, W)$—a map $\phi$ commutes with every element $g$ from $G$ if and only if it commutes with all linear combinations of the $g$’s—so that the two categories $\text{Rep}_{G,k}$ and $\text{Mod}_{k[G]}$ are equivalent:

**Proposition 1.5** There is a natural equivalence of categories $\text{Rep}_{G,k} \cong \text{Mod}_{k[G]}$

There are two natural and mutually inverse functors between them, both, are in fact, acting as the identity on the underlying $k$-vector spaces. Be aware however, that the functor from $\text{Mod}_{k[G]}$ to $\text{Rep}_{G,k}$ depends on the inclusion $G \subseteq k[G]$.

(1.6) Be aware that in general the sole algebra structure of $k[G]$ does not determine the group; different groups can have group algebras that are isomorphic as abstract algebras. We saw some examples above (example 1.10) and further will be seen below.

The group algebra carries however an extra structure, it has $G$ as a preferred subgroup of the group of units. The tensor structure of $\text{Rep}_{k,G}$ depends on this inclusion, as does the isomorphism $t_G : k[G] \rightarrow k[G]^\text{op}$. Therefore both the formation of the contragredient modules $V^*$ and the internal homs $\text{Hom}(V, W)$ in $\text{Rep}_{k,G}$ depend on the group $G$, and not merely on the structure of $k[G]$ as an $k$-algebra. The underlying vector space are of course the same, but the module structures do not necessarily coincide.

There is a result that goes under name of Tannaka-duality that one can recover the group $G$ from the category $\text{Rep}_{k,G}$ endowed with the tensor structure, the internal hom and the forgetful functor $\text{Rep}_{k,G} \rightarrow \text{Vect}_k$ (it holds not only for finite groups, but for compact groups as well).
Under which conditions the algebra structure of $k[G]$ determines the group, is a subtle question. It depends on the ground field as well as on the group as the subsequent examples illustrate. We just mention that a long-standing conjecture that the integral group ring $\mathbb{Z}[G]$ determines the group was disproved in 2001 by Martin Hertweck who gave examples of two groups of order $2^{21} \cdot 97^{28}$ whose group rings are isomorphic.

**Direct products**

The formation of the group algebras behaves very well when it comes to direct products. If $G$ and $G'$ are two groups, there are algebra homomorphisms $R[G] \to R[G \times G']$ and $R[G'] \to R[G \times G']$ induced by the natural inclusions $G \to G \times G'$ and $G' \to G \times G'$. By the universal property of the tensor product they give rise to an algebra homomorphism $R[G] \otimes_k R[G'] \to R[G \times G']$ that sends $g \otimes g'$ to $(g, g') = (g, e)(e, g')$, and this is an isomorphism:

**Proposition 1.6** There is a natural isomorphism of group algebras $R[G \times G'] = R[G] \otimes_k R[G']$.

**Proof:** The algebra $R[G \times G']$ is free over $R$ with the pairs $(g, g')$ forming a basis, and $R[G] \otimes_k R[G']$ is free with the elements $g \otimes g'$ making up a basis.

**Examples: Abelian groups**

Group algebras of cyclic groups, or more generally abelian groups, are easy to describe since they are commutative. They give nice illustrations of how the base field influences the shape of the group algebra. Basically, the description boils down to understand the behavior of the cyclotomic polynomials over different fields.

Let $C_n$ be a cyclic group of order $n$. We have seen that any choice of generator $g$ for $C_n$ gives rise to an algebra isomorphism $k[C_n] \simeq k[t]/(t^n - 1)$ that sends powers $g^i$ to powers $t^i$. The algebra structure of $k[C_n]$ depends therefore on the factorization of $t^n - 1$ into irreducibles over $k$; that is, the algebra structure is determined by which $n$-th roots of unity the field $k$ contains.

**Examples**

In the case the polynomial $t^n - 1$ splits simply and completely in linear factors in $k$, for instance if $k$ contains the cyclotomic field $\mathbb{Q}(\zeta_n)$, the group algebra $k[C_n]$ becomes isomorphic to the direct product $k \times \ldots \times k$ of $n$ copies.
of \( k \); an isomorphism being given by evaluation at the \( n \) different \( n \)-th roots of unity.

1.12. When \( t^n - 1 \) does not split completely, the group algebra is of a different shape. For instance, if \( n = p \) is a prime and \( k = \mathbb{Q} \), the factorization of \( t^p - 1 \) into irreducible factors is \( t^p - 1 = (t - 1)(t^{p-1} + \ldots + t + 1) \), and the group algebra \( \mathbb{Q}[C_n] \) becomes isomorphic to \( \mathbb{Q} \times \mathbb{Q}(p) \) where \( \mathbb{Q}(p) \) is the cyclotomic field generated over \( \mathbb{Q} \) by a primitive \( p \)-th root of unity.

Form more general integers \( n \) the polynomial \( t^n - 1 \) factors over \( \mathbb{Z} \) as the product \( t^n - 1 = \prod_{d|n} \Phi_d(t) \) where \( \Phi_d \) is the so called \( d \)-th cyclotomic polynomial. These are irreducible over \( \mathbb{Q} \), and hence one has

\[
\mathbb{Q}[C_n] = \mathbb{Q} \times \prod_{d|n} \mathbb{Q}(d),
\]

where \( \mathbb{Q}(d) \) is the cyclotomic field generated over \( \mathbb{Q} \) by the \( d \)-th roots of unity. The degree of \( \Phi_d \) is given as the value of the Euler \( \phi \)-function at \( d \). It equals the number of units in the finite ring \( \mathbb{Z}/n\mathbb{Z} \), and is a multiplicative function taking the value \( \phi(p^n) = (p - 1)p^{n-1} \) at prime powers.

1.13. When the characteristic \( p \) of \( k \) divides the order \( |G| \), the situation is quiet different from above. As an illustration let us take a look at \( C_{p^r} \), a cyclic group of order \( p^r \). As above it holds true that \( k[C_{p^r}] \cong k[t]/(t^{p^r} - 1) \) with a generator corresponding to \( t \). But putting \( u = t - 1 \), we find an isomorphism \( k[C_{p^r}] \cong k[u]/u^{p^r} \); indeed, since \( k \) is of characteristic \( p \), it holds true that \( u^{p^r} = t^{p^r} - 1 \). Hence \( k[C_{p^r}] \) is a local ring in this case, and there is only one homomorphism into \( k \).

1.14. Given two natural numbers \( n \) and \( m \) and consider the direct product \( C_n \times C_m \), which is an Abelian group of order \( nm \). It is generated by two elements \( g \) and \( h \) of order \( n \) and \( m \) respectively, and sending \( g \) to \( t \) and \( h \) to \( u \) induces an isomorphism \( k[C_n \times C_m] = k[t,u]/(t^n - 1, u^m - 1) \).

Once both polynomials \( t^n - 1 \) and \( u^m - 1 \) splits simply and completely in \( k \), this algebra is isomorphic to the direct product of \( nm \) copies of \( k \); the isomorphism being given by evaluating at the \( nm \) points with coordinates the different \( n \)-th roots respectively the different \( m \)-th roots of unity.

With \( n = m \) this shows that the two non-isomorphic groups \( C_n^2 \) and \( C_n \times C_n \) have isomorphic group algebras at least when \( k \) contains the \( n^2 \)-th roots of unity. We leave it to zealous student to write down a proof of the following generalization:

**Proposition 1.7** Let \( k \) be a field. Two abelian groups for which \( k \) is a big and friendly field have isomorphic group algebras if and only if they have the same order.

**Proof:** Induction on the order. \( \Box \)
1.15. Assume that $k$ is of characteristic $p$. By similar arguments in the two previous examples, or appealing to proposition 1.6 above, $k[C_p \times C_p]$ will be isomorphic to $k[u, v]/(u^p, v^p)$. This is a local algebra with embedding dimension two, whereas $k[C_p^2]$ is local with embedding dimension one. Whence the two are not isomorphic.

**Problem 1.24.** Let $L$ be an $G$-module over $k$. We say that $L$ is invertible if $\dim_k L = 1$. Show that the evaluation map $L \otimes L^* \to k$ is an isomorphism of $G$ modules. Infer that the set of isomorphism classes of invertible $G$-modules is a group.

**Problem 1.25.** Determine the group defined in the previous exercise for the two cases $k[C_4]$ and $C[C_2 \times C_2]$. Conclude that even if $\text{Rep}_k C_4$ and $\text{Rep}_k C_2 \times C_2$ are equivalent abelian categories, their tensor structures are different.

**An alternative description**

There is an alternative description of the group algebra as the vector space $L_k(G)$ of functions on $G$ taking values in $k$—and in fact, this is the one that generalizes nicely to compact, non-finite groups. This space becomes an $k$-algebra when equipped with the convolution product; that is, if the value of the function $\alpha$ at the group element $g$ is denoted by $\alpha_g$, one has

$$ (\alpha \cdot \beta)_g = \sum_{h \in G} \alpha_{gh^{-1}} \beta_h. $$

The isomorphism between $k[G]$ and $L_k(G)$ is established by letting $g$ correspond to the function $\delta_g$ that takes the value one at $g$ and is zero elsewhere, and the convolution product is made for this to be multiplicative.

It might be confusing that this makes $k[G]$ into a contravariant functor while above $k[G]$ was covariant! If $\phi : G' \to G$ is a group homomorphism, the map $\phi^*$ sending $\alpha$ to $\alpha \circ \phi$ is however not multiplicative with respect to the convolution product, making it less interesting in our context.

**Problem 1.26.** Show that $\mu : G \times G \to G$ denotes the multiplication, then the convolution product is nothing but the “push-forward-map” $\mu_* : L(G) \times L(G) \to L(G)$.

**Problem 1.27.** Convince yourself that $\phi^*$ does not respect the convolution product.

\footnote{Recall that the embedding dimension of a local ring with maximal ideal $m$ and residue field $k$ equals $\dim_k m/m^2$.}
The regular representation

The algebra $k[G]$ has yet another interpretation. Of course $G$ acts on $k[G]$ by multiplication from the left. The corresponding representation is called the left regular representation, customarily it is denoted by $V_{\text{reg}}$ and its degree equals the order $|G|$. And naturally, there is a right regular representation as well. Finally $k[G]$ is both a left and a right module over itself, and one has as for all algebras (possessing a unit element and being isomorphic to their opposite) a canonical isomorphism

$$\text{Hom}_G(k[G], k[G]) = \text{Hom}_{k[G]}(k[G], k[G]) \simeq k[G]^{\text{op}} \simeq k[G],$$

induced by the assignment $\phi \mapsto \phi(1)$.

**Problem 1.28.** Let $A$ be any ring (with a unit element). Show that $\text{Hom}_A(A, A) \simeq A^{\text{op}}$, where $A$ is a considered a left module over itself. **HINT:** As you can guess, the isomorphism is given by $\phi \mapsto \phi(1)$.

1.3 Irreducible and indecomposable representations

Any representation $V$ of a group $G$ has at least two subrepresentation: the zero representation and the representation $V$ itself. If these two are the only ones, one says that $V$ is irreducible or simple. A representation is said to be indecomposable if it has no non-zero and proper subrepresentation that is split in $V$; i.e., it is not isomorphic to a direct sum $W \oplus W'$ with both summands being non-zero.

(1.1) These two concepts, irreducible and indecomposable representations, are fundamental in the theory; the finite indecomposable representations will serve as building blocks for all: A self-going induction argument shows that any finite dimensional representation is a direct sum of indecomposable representations. As to irreducible, any finite dimensional representations has a composition series; that is a strictly descending chain $\{V_i\}_{0 \leq i \leq r}$ of subrepresentations with $V_0 = 0$ and such that the subquotients $V_i / V_{i+1}$ all are irreducible, and the Jordan-Hölder theorem tells us that the subquotients are determined up to isomorphism and order.
(1.2) One of the cornerstones of the theory is that the two notions irreducible and indecomposable coincide in the friendly case. This was proved by Heinrich Maschke in 1899 (see theorem 3.10 on page 66 below). However, in general—that is, if $|G|$ has $p$ as a factor—they differ considerably. For example, the group $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ has infinitely many non-isomorphic, indecomposable representations over a field of characteristic $p$, but has a single irreducible one, namely the trivial representation. (For some examples, see section 2.3 on page 44 below). And this is typical for representations $p$-groups in characteristic $p$, unless it is cyclic, it has infinitely many non-isomorphic indecomposable representations.

(1.3)—Absolute irreducible representations. One says that a representation $V$ of $G$ over $k$ is absolute irreducible if $V_k$ is irreducible for all finite extensions $K$ of $k$. This equivalent to $V_k$ being irreducible where $k$ is an algebraic closure of $k$.

We are now in the position to give a precise meaning to the property of a field $k$ to be big and friendly field for $G$. It must be friendly (i.e., if it is of positive characteristic $p$, the order $|G|$ is prime to $p$) and the new definition: Every irreducible representation is absolute irreducible. But notice that most commonly such a field is called a splitting field for $G$.

Example 1.16. Let $n$ be a non-zero integer and consider for each $m \in \mathbb{Z}$ the matrix

$$\rho(m) = \begin{pmatrix} \cos 2\pi m/n & \sin 2\pi m/n \\ -\sin 2\pi m/n & \cos 2\pi m/n \end{pmatrix}$$

which geometrically represents a rotation about the origin with an angle of rotation equal to $2\pi m/n$. The matrix $\rho(m)$ depends only of residue class of $m$ modulo $n$, and $\rho(m + m') = \rho(m)\rho(m')$, and hence it defines a representation of $\mathbb{Z}/n\mathbb{Z}$ on the real vector space $\mathbb{R}^2$. This representation is irreducible because no line through the origin is invariant. However the representation on $\mathbb{C}^2$ with the same matrix decomposes, as both $(1, i)$ and $(-i, 1)$ are common eigenvectors for all $\rho(m)$. Hence $\rho$ is not absolutely irreducible.

1.4 Rings associated to $G$

We let $K_0(G; k)$ be the Grothendieck-group associated to the category $\text{Rep}_{G, k}$ of finite dimensional representation of $G$ over $k$. Recall that the generators of
$K_0(G,k)$ are the isomorphism classes of such modules (or representations, if you want), and the class of a module $V$ will be denoted by $[V]$. There is one relation for each short exact sequence

$$0 \rightarrow V' \rightarrow V \rightarrow V'' \rightarrow 0 \quad (1.4)$$

in $\text{Rep}_{G,k}$, namely $[V] = [V'] + [V'']$, and these relations generate all relations. This means that $K_0(G,k)$ is the free abelian group on the set of isomorphism classes in $\text{Rep}_{G,k}$ modulo the subgroup generated by differences $[V] - [V'] - [V'']$, one for each short exact sequence $(1.4)$.

There is a ring structure on $K_0(G; k)$ that is induced by the tensor product in $\text{Rep}_{G,k}$. The product of two classes $[V]$ and $[W]$ in $K_0(G; k)$ is given as

$$[V][W] = [V \otimes W].$$

Corresponding properties of the tensor product imply that this product is an associative and commutative binary operation. Moreover, it is distributive over the addition; indeed, the tensor product in $\text{Rep}_{G,k}$ is exact, so tensoring the short exact sequence $(1.4)$ above by $W$, results in the short exact sequence

$$0 \rightarrow V' \otimes W \rightarrow V \otimes W \rightarrow V'' \otimes W \rightarrow 0.$$ 

One infers that $[W][V'] + [W'][V''] = [W][V'] + [W][V''].$

$(1.1)$ The ring $K_0(G,k)$ is functorial in $G$, in that any homomorphism $\phi: H \rightarrow G$ gives rise to a ring homomorphism $\phi^*: K_0(G,k) \rightarrow K_0(H,k)$. Indeed, if $V$ is a $G$-module, the $H$-module $\phi^*V$ still has $V$ as underlying vector space, only the action changes. As exactness of the sequence $(1.4)$ above only solely depends on the vector-space structures, $\phi^*$ gives a map between the Grothendieck-groups. Only easily checks (by a similar reasoning) that this map preserves tensor products.

One lets $K^0(G,k)$ be the Grothendieck group build from the category of finite projective $k[G]$-modules, and in a similar way as with $K_0(G,k)$ one endows $K^0(G,k)$ with a ring structure induced by the tensor product. These two $K$-groups coincide in the friendly case as we shall see, but in general they differ although they are tightly related.

The Grothendieck groups are also functorial in $K$, in that extending the ground field yields a ring homomorphisms $K_0(G,k) \rightarrow K_0(G,K)$ and $K^0(G,k) \rightarrow K^0(G,K)$.

$(1.2)$—Representation groups. In the literature one also meets the so called representation group $\text{Rep}(G,k)$. It is construction in a fashion similar to the Grothendieck-group, generated by isomorphism classes of representation,
but the relations are confined to those coming from the exact sequences (1.4) that are split; that is, the basic relations that generate all, are shaped like:

\[ [W \oplus V] = [V] + [W]. \]

(1.3)—The Burnside ring. The collection of finite $G$-sets, that is finite sets endowed with an action of $G$, give rise to a Grothendieck group which also has a ring structure. One calls it the Burnside ring of $G$, and we shall denote it by $B(G)$. One begins with the free abelian group on the set of isomorphism classes, and subsequently one factors out the subgroup generated by the differences $[X] + [Y] - [X \cup Y]$ and where $X$ and $Y$ are any two $G$-sets and the union is the disjoint union. The product grows out of the cartesian product of $G$-sets; the product $X \times Y$ endowed with the “parallel” action of $G$; that is, elements $g$ from $G$ act as $g \cdot (x, y) = (g \cdot x, g \cdot y)$. One puts $[X][Y] = [X \times Y]$.

**Problem 1.29.** Show that with the definitions above, the ring axioms are fulfilled. What is the zero element and what is the unit element? *

Every $G$-set is the disjoint union of its orbits, and every orbit is of the shape $G/H$ with $G$ acting by left multiplication. Two such are isomorphic if and only the corresponding subgroups are conjugate. Hence the Burnside ring has additive generators of the form $[G/H]$ where $H$ runs through a set of representative of conjugacy classes of subgroups.

In xx we constructed the permutation representation of

**Problem 1.30.** Let $p$ be a prime and let $C_p$ be cyclic of order $p$. Show that $B(C_p) = \mathbb{Z}[t]/(t^2 - pt)$.

Hence these organizes the set of isomorphism classes of the finite $G$ sets into a ring, and $L : B(G) \to K_0(G,k)$ is a ring homomorphism.

1.5 Modules over algebras I

The concepts “irreducible” and “indecomposable” representations, which we introduced for groups, have of course counterparts in the general theory of modules over rings. We find it worth while to touch upon the general theory, but without leaving our guiding principle that groups are our main concern.

We shall present two important results, both are in their essence unicity statements about “deconstruction” of modules. The first is the Jordan-Hölder theorem. The original version concerned decomposition series in groups, but there is a module version as well, which we shall prove. The theorem (about

---

* Naturally, two $G$-sets are isomorphic if there is bijection between them commuting with the actions.
groups) appeared for the first time in Camille Jordan’s famous paper *Traité des substitutions et des équations algébriques* from 1870 and found its final form in a paper by Otto Hölder from 1889.

The second theorem we had also its origin in group theory, and it concerns decompositions of groups in direct products of indecomposable groups. For groups satisfying appropriate finiteness conditions such decompositions are unique (up to order and isomorphism). We shall treat the module version, which is somehow subtler than the case for groups. Even over such nice rings as Dedekind rings decompositions into indecomposables are not unique; one has in many cases an equality \( A \oplus A = P \oplus P' \) with \( P \) and \( P' \) being modules (of rank one) that are not free. However, when \( A \) is a finite algebra over a field uniqueness holds. The theorem has many names\(^9\) attached to it, but nowadays it is mostly called the Krull-Schmidt theorem.

So let \( A \) be any ring. An \( A \)-module \( V \) is said to be irreducible or simple if it possesses no non-trivial proper submodules; that is, the only submodules are 0 and \( V \) itself. The module \( V \) is called indecomposable, if it has no non-trivial direct summands; that is, a decomposition \( V = V' \oplus V'' \) implies that \( V' = 0 \) or \( V'' = 0 \).

### Modules of finite length and the Jordan-Hölder theorem

A composition series for an \( A \)-module \( V \) is a strictly ascending and finite series \( \{ V_i \}_{0 \leq i \leq r} \) of submodules all whose subquotients \( V_i / V_{i+1} \) are simple modules, and moreover it should start with 0 and end with \( V \); that is, it holds that \( V_0 = 0 \) and \( V_r = V \). Such a series is shaped like

\[
0 = V_0 \subset V_1 \subset \ldots \subset V_r = V,
\]

and \( r \) is called the length of the series. It turns out that all composition series have the same length, which one calls the length of the module. Modules having a composition series are referred to as modules of finite length, one can prove that this is equivalent to \( V \) being both artinian and noetherian.

Moreover, the subquotients are the same up to order and isomorphism and they are called the composition factors of the module. This is the content of the

\(^9\) The first version, for finite groups, was proved by Wedderburn in 1909. Others having contributed are Remak and Asumaya, and our compatriot Øystein Ore has the most general version.
The Jordan-Hölder theorem:

**Theorem 1.1 (Jordan-Hölder)** Let $V$ be an $A$-module of finite length; i.e., one having a composition series. Then any two composition series have the same length and their subquotients are same up to order and isomorphism.

**Proof:** The proof goes by induction on the minimal length of a composition series; if this is one, the result is trivial.

So let $\{V_i\}_{0 \leq i \leq r}$ and $\{U_i\}_{0 \leq i \leq s}$ be two composition series in $V$ and assume that the first one is of minimal length; i.e., $r$ is minimal. The trick is to consider the quotient $W = V / V_1$, which sits in the short exact sequence

$$
\begin{array}{c}
0 \\ \longrightarrow
\end{array} V_1 \\ \longrightarrow V \xrightarrow{\pi} W \\ \longrightarrow 0.
$$

The series $\{V_{i+1} / V_1\}_{0 \leq i \leq r-1}$ is a composition series for $W$ with the same subquotients as the series $\{V_i\}$ has for $i \geq 2$. Whence $W$ is of length less than $V$, the induction hypothesis applies to it and all composition series of $W$ are of length $r - 1$. The series $\{\pi(U_i)\}_{0 \leq i \leq s}$ is an ascending series in $W$ whose subquotients $\pi(U_{i+1}) / \pi(U_i)$ are factors of the modules $U_{i+1} / U_i$, and they are therefore simple; in fact, they are either zero or isomorphic with $U_{i+1} / U_i$.

Now, let $j_0$ be the least $j \geq 1$ such that $\pi(U_{j-1}) = \pi(U_j)$. Then $U_{j_0-1} + V_1 = U_{j_0}$, so that $V_1 \subseteq U_j$ for $j > j_0$. There are hence strict inclusions $\pi(U_{j-1}) \subset \pi(U_j)$ for $j > j_0$. And of course, there are strict inclusions $\pi(U_{j-1}) \subset \pi(U_j)$ for an indices $j$ less than $j_0$. Hence in the series $\{\pi(U_i)\}$ there are $s - 1$ strict inclusions, and by induction $s - 1 = r - 1$; that is, $s = r$.

The statement about the composition factors follows easily by induction since at the break point $j_0$ one has $U_{j_0} / U_{j_0-1} = (U_{j_0-1} + V_1) / U_{j_0-1} = V_1$ and for all other indices $U_j / U_{j-1}$ is one of the composition factors in $W$, and these are precisely the composition factors $V_j / V_{j-1}$ with $j \geq 2$. □

**Problem 1.31.** Show that an $A$-module $V$ is of finite length if and only if it is both artinian and noetherian. *

The Krull-Schmidt theorem

With an appropriate finiteness condition on the module $V$, an induction argument shows that $V$ is the sum of indecomposable submodules:

**Proposition 1.8** An artinian $A$-module $V$ is the direct sum of finitely many indecomposable submodules.

**Proof:** The first thing we do is to establish that $V$ has a non-zero indecomposable direct summand: Consider the set of non-zero direct summands in $V$. It
is non-empty \( V \) being a summand in itself (!), and consequently, because \( V \) is artinian, this set has a minimal element \( W \). Now, \( W \) must be indecomposable, for if \( W = W' \oplus W'' \) both \( W' \) and \( W'' \) will also be direct summands in \( V \) and the minimality of \( W \) entails that one of them is zero while the other equals \( W \).

We proceed by proving that a module \( V \) not satisfying the conclusion of the proposition, possesses a strictly descending series of submodules, which is absurd since \( V \) is artinian.

A recursive process brings forth two sequences of submodules, one \( \{ V_i \} \) whose members are all indecomposable and one \( \{ W_j \} \) being the requested strictly descending series. All involved submodules are proper and non-zero, and for each natural number \( r \) there is a decomposition

\[
V = V_1 \oplus V_2 \oplus \ldots \oplus V_r \oplus W_r.
\]

The recursive step is evident: The module \( W_r \) is decomposable by the assumption that \( V \) is not a sum of indecomposable, and it is artinian as submodules of artinians are artinian, so by the first part of the proof it has an indecomposable direct summand and decomposes accordingly as \( W_r = V_{r+1} \oplus W_{r+1} \) with \( V_{r+1} \) indecomposable and both summands non-trivial. Evidently (since \( V_r \neq 0 \)) the series \( \{ W_r \} \) is strictly decreasing.

**Problem 1.32.** Show that the hypothesis of \( V \) being artinian can be replaced by the assumption that \( V \) be noetherian. **Hint:** The same proof works with little changes. In the first part consider the set of submodules having an indecomposable complement, and in the second swap the role of the series \( \{ V_i \} \) and \( \{ W_j \} \).

The Krull-Schmith theorem ensures that the summands are unique in many cases:

**Theorem 1.2** Assume that \( A \) is a ring and \( V \) is an \( A \)-module. Assume that \( V = \bigoplus_{1 \leq i \leq r} V_i = \bigoplus_{1 \leq j \leq r} W_j \) are two finite decompositions of \( V \) into sums of indecomposables. If the endomorphism rings \( \text{End}_A(V_i) \) all are local, then \( V_i \)'s and the \( W_j \)'s are the same, up to isomorphism and order.

**Proof:** Let \( e_i \) and \( f_j \) be the projections from \( V \) to \( V_i \) and \( W_j \) respectively. Then \( \sum f_j = 1 \) and hence \( (\sum e_if_j)|_{V_i} = e_i|_{V_i} = 1 \). Now, \( \text{End}_A(V_i) \) is a local ring and it is true that the sum of non-units is non-unit (the maximal ideal is precisely the set of non-units). Hence at least for one \( j \) the composition \( e_if_j|_{V_i} \) will be invertible. This map factors like

\[
V_i \xrightarrow{f_j|_{V_i}} W_j \xrightarrow{e_i|_{W_j}} V_r,
\]
and it follows that \( f_j(V_i) \) lies split in \( W_j \). Now, \( W_j \) is assumed to be irreducible and we can deduce we that \( V_i \cong W_j \).

We proceed by induction on \( r \). We just saw the \( V_1 \) is isomorphic to one of the \( W_j \)'s and by shuffling the indices we may as well assume that this is \( W_1 \). Once we can cancel \( V_1 \) and \( W_1 \) from the sums, we will be through by induction.

(1.1)—**Locality of endomorphism rings.** For this theorem to be useful a criterion for \( \text{End}_A(V) \) to be local. In our present context of a group algebra \( k[G] \) or slightly more general, that \( A \) is an algebra of finite dimension over a field this \( \text{End}_A(V) \) is however always local. The reason for this to be true is a form of Schur’s lemma valid for artinian indecomposable modules, stating that an endomorphism is either invertible or nilpotent—where as in Schur’s lemma it is either invertible or zero.

**Proposition 1.9** Assume that \( A \) is of finite dimension over a field \( k \). If \( V \) is an indecomposable \( A \)-module of finite dimension, then every endomorphism \( \phi \) of \( V \) is either invertible or nilpotent. In particular, the ring \( \text{End}_A(V) \) is a local ring.

**Proof:** Clearly the first statement entails the second: The nilpotents in \( \text{End}_A(V) \) form an ideal whose complement consists of the invertible endomorphisms. Indeed, the sum of to nilpotent endomorphisms is always nilpotent, and if \( \phi \) is nilpotent and \( \psi \) is an endomorphisms, \( \psi \circ \phi \) can not be invertible since \( \phi \) has a non-trivial kernel. Thus it is nilpotent by the first statement.

The crux of the proof of the first part is the following lemma due to xxx

**Lemma 1.2** Let \( V \) be an artinian \( A \)-module and let \( \phi : V \rightarrow V \) be an endomorphism. Then for some natural number \( n \) there is a decomposition \( V = \ker \phi^n \oplus \text{im} \phi^n \).

**Proof:** The images of the iterates of \( \phi \) form a decreasing chain \( \{ \text{im} \phi^n \}_{n \geq 1} \) and their kernels \( \{ \ker \phi^n \}_{n \geq 1} \) an ascending chain. Since \( V \) is supposed to be artinian, both these chains stabilizes, and there is \( n \) so that \( \ker \phi^{n+r} = \ker \phi^n \) and \( \text{im} \phi^{n+r} = \text{im} \phi^n \) for all non-negative integers \( r \). We claim that \( V = \text{im} \phi^n \oplus \ker \phi^n \).

On one hand, one has \( \ker \phi^n \cap \text{im} \phi^n = 0 \). Indeed, if \( \phi^n(v) \in \ker \phi^n \) it holds true that \( \phi^{2n}(v) = 0 \), which forces \( \phi^n(v) = 0 \) since \( \ker \phi^n = \ker \phi^{2n} \). On the other hand, if \( v \in V \) one has \( \phi^n(v) = \phi^{2n}(w) \) for some \( w \). Hence \( v - \phi^n(v) \) lies in the kernel \( \ker \phi^n \) and \( v \) is expressible as the sum of elements from \( \ker \phi^n \) and \( \text{im} \phi^n \).

Now, the proposition follows immediately since \( V \) being indecomposable either \( \ker \phi^n = 0 \) and \( \phi \) is nilpotent, or \( \ker \phi^n = 0 \) and \( \phi \) is injective. In the latter case one has \( \text{im} \phi^n = V \) as well, which implies that \( \phi \) is surjective, hence invertible.
**Problem 1.33.** Show that if $A$ is of finite rank over a complete DVR, then $\text{End}_A(V)$ is local ring.

**Problem 1.34.** Let $A = \mathbb{Z}[i\sqrt{5}]$ and let $I$ be the ideal $I = (2, 1 + i\sqrt{5})$. Show that $I$ is indecomposable, but not a principal ideal (so that $I$ is not isomorphic to $A$). Show that there is a decomposition $A \oplus A \simeq I \oplus I'$ with $I' = (2, 1 - i\sqrt{5})$.

**Problems**

1.35. Show that the group algebra of a direct product $G \times H$ is canonically isomorphic to the tensor product $k[G] \otimes_k k[H]$. **Hint:** The elements $g \otimes h$ with $g \in G$ and $h \in H$ constitute a $k$-linear basis for the tensor product.

1.36. Assume that $k$ is an algebraically closed field of characteristic zero. Generalize the preceding example, and show that if $G$ is abelian, the algebra $k[G]$ is isomorphic to a direct product of $|G|$ copies of the ground field. Conclude that two abelian groups with the same order have isomorphic group algebras over $k$. What are the minimal conditions on $k$ for this to be true?

1.37. Show that $\mathbb{Q}[C_n]$ is isomorphic to the product $\prod_{d|n} \mathbb{Q}(d)$. **Hint:** $t^n - 1 = \prod_{d|n} \Phi_d(t)$ where $\Phi_d(t)$ is the $d$-th cyclotomic polynomial.

1.38. Let $p$ be a prime. Show that $\mathbb{Q}[C_p \times C_p]$ is isomorphic to $\mathbb{Q} \times 2\mathbb{Q}(p) \times (p-1)\mathbb{Q}(p)$.

1.39. Show that $\mathbb{Q}[C_p^2]$ and $\mathbb{Q}[C_p \times C_p]$ are not isomorphic.
Representations of Abelian groups

In the present chapter we shall develop in an ad hoc manner the representation theory for the finite abelian groups over big and friendly fields. This hinges on rather elementary linear algebra like the Jordan-Chevalley decomposition of linear endomorphisms, and the historic development of the theory followed this line. We find it worth while doing even if the notes grows with a few pages, additionally it furnishes us with a lot of examples early in the course, and of course, the abelian case will frequently pop up in the general theory.

We touch upon the characteristic $p$-case, mostly to illustrate the complication that arises, and as well we cast a glance on representations over smaller fields in characteristic zero. That is fields of containing sufficiently many roots of unity; the basic example being $\mathbb{Q}$.

Additionally this chapter is a natural place for a short description of one-dimensional representations in general.

Jordan-Chevalley decomposition

An underlying explanation that representation theory of finite groups in characteristic zero is such a strong and beautiful theory—half the representation theory in a nutshell if you want—is that any endomorphisms of finite order of a finite dimensional vector space is semi-simple unless its order is not prime to the characteristic of the ground field. For cyclic groups this is basically the whole story, and together with the principle that commuting operators have common eigenvectors, it also explains the representations of abelian groups,
at least in the case that the order is prime to the characteristic. For general groups, of course, the interaction between non-commuting elements complicates the analysis dramatically—and a nutshell (even of a coco-nut) is too small to contain the theory.

(2.1)—JORDAN DECOMPOSITION: So, if \( \sigma \) denotes an endomorphism of the vector space \( V \), the Jordan-Chevaley\(^1\) decomposition of \( \sigma \) is a factorization \( \sigma = \sigma_s \sigma_u \) where \( \sigma_u \) is unipotent and \( \sigma_s \) is semi-simple and the two commute. Such a decomposition is unique and always exists. If \( \sigma \) is of finite order, both the semi-simple part \( \sigma_s \) and the unipotent part \( \sigma_u \) are of finite order; in fact, it follows from the unicity of the Jordan composition and the relation \( \sigma^m = \sigma_s^m \sigma_u^m \) that their orders both divide that of \( \sigma \). Hence the unipotent part \( \sigma_u \) is of finite order and the claim, that \( \sigma \) is semi-simple in the friendly case, follows from the following lemma:

**Lemma 2.1** Let \( V \) be a vector space of finite dimension over \( k \) and let \( \sigma \) be an endomorphism of \( V \). Assume that \( \sigma \) is unipotent and of finite order. Then either \( \sigma = \text{id}_V \), or \( k \) is of positive characteristic \( p \), and the order of \( \sigma \) equals some power \( p^m \).

**Proof:** The minimal polynomial of \( \sigma \) is of the form \( (T - 1)^s \) since \( \sigma \) is unipotent and of the form \( T^r - 1 \) since it is of finite order. These two polynomials being equal means \( 1 \) is the only \( r \)-th root of unity in the algebraic closure \( \bar{k} \), and that can only happen if \( r \) is a power of the characteristic.

**Proposition 2.1** Let \( V \) be a vector space of finite dimension over \( k \) and let \( \sigma \) be an endomorphism of finite order \( n \).

- In the case the order \( n \) is invertible in \( k \), then \( \sigma \) is semi-simple.
- If \( k \) is of positive characteristic \( p \) and \( n = p^m \), and the unipotent part of \( \sigma \) is of order \( p^m \).

**Proof:** The first statement is a direct consequence of the lemma. For second what remains to be seen, is that \( \sigma \) is unipotent if its order is a power \( p^m \) of \( p \), which is evident since its characteristic polynomial is \( T^{p^m} - 1 \) which equals \( (T - 1)^{p^m} \).

(2.2) Given a representation \( V \) of \( G \) over \( k \) and an element \( g \in G \). The Jordan-Chevalley decomposition of the endomorphism \( g|_V \) is in some sense inherent in the group \( G \), but depends of course on the characteristic \( p \) of \( k \) which in this paragraph assume to be positive.

One may factor \( g \) in a unique way as as product \( su \) of two commuting elements \( s \) and \( u \) such that the order of \( u \) is a power of \( p \) and that of \( s \) is prime to

\(^1\) One says that an endomorphism \( \sigma \) of \( V \) is semi-simple if \( \sigma \) can be diagonalized over some extension field of \( k \); equivalently, the minimal polynomial of \( \sigma \) has only simple zeros in the algebraic closure \( \bar{k} \). An endomorphism \( \sigma \) of \( V \) being unipotent means that \( \sigma = \text{id}_V + \tau \) where \( \tau \) is nilpotent.
p. Indeed, if the order $n$ of $G$ factors as $n = p^r p'$ with $p$ and $p'$ relatively prime, one determines integers $a$ and $a'$ so that $a p^r + a' p' = 1$ and poses $s = g^{a p^r}$ and $u = g^{a' p'}$. The element $s$ is called the $p'$-part of $g$ and $u$ the $p$-part. It holds true that $s|_V$ is the semi-simple and $u|_V$ the unipotent part of $g|_V$ for any representation $V$ of $G$ over a field of characteristic $p$. It is common usage to call an element of order $p^r$ a $p$-element and one whose order is prime to $p$ for a $p'$-element or a $p$-regular element.

We summarize:

**Lemma 2.2** Let $G$ be a group and $p$ a prime. Any element $g \in G$ is in a unique way a product $g = su$ of commuting elements $s$ and $u$ with $s$ being a $p'$-element and $u$ a $p$-element. For every representation $V$ of $G$ over a field of characteristic $p$, the semi-simple part of $g|_V$ is $s|_V$ and the unipotent part is $u|_V$.

### 2.1 One dimensional representations

Let $G$ be a group and let $V$ be a one-dimensional vector space over any field $k$. Since there is a canonical isomorphism $\text{Gl}(V) \cong k^*$, a representation of $G$ on $V$ is just a group homomorphism $\chi: G \to k^*$, and for any vector $v$ of $V$ one has $g \cdot v = \chi(g) v$. Such homomorphisms are called multiplicative characters. Given one, we shall denote by $L(\chi)$ the corresponding representation afforded by the ground field itself; that is, the one dimensional space $k$ on which group elements $g$ act as multiplication by $\chi(g)$. Any one-dimensional representation is isomorphic to one of the $L(\chi)$'s; the choice of a basis element gives an isomorphism.

**Lemma 2.3** Let $k$ be any field. There is a one-to-one correspondence between multiplicative characters $\chi: G \to k^*$ of $G$ and isomorphism classes of one-dimensional representations of $G$ over $k$.

**Proof:** The only thing that remains to be checked is that two different multiplicative characters $\chi$ and $\chi'$ define non-isomorphic representations; this is
however clear, since if \( \phi : V \to V' \) is an isomorphism, one has for \( g \in G \) on the one hand \( \phi(\chi(g)v) = \chi(g)\phi(v) \), as \( \phi \) is \( k \)-linear, and on the other \( \phi(\chi(g)v) = \chi'(g)\phi(v) \) since \( \phi \) respects the \( G \)-actions. Hence \( \chi(g) = \chi'(g) \).

Notice that if \( n \) denotes the order of \( G \), a multiplicative character \( \chi \) takes values in the group \( \mu_n(k) \) of \( n \)-th roots of unity in \( k \); and by consequence the image \( \chi(G) \) is cyclic. (Recall that any finite subgroup of the multiplicative group of a field is cyclic).

Two multiplicative characters on \( G \) can be multiplied and \( k^* \) being abelian, the product is again a multiplicative character. Whence the set \( \hat{G}(k) \) of multiplicative characters is an abelian group (which certainly can be trivial, see problem 2.6 below), and as the notation indicates, it depends on the field \( k \) and what roots of unity it contains.

**Examples**

2.1. The determinant \( \text{det} : \text{Gl}(n, k) \to k^* \) is a multiplicative character for all fields \( k \).

2.2. The sign-map \( \text{sign} : S_n \to \{ \pm 1 \} \) that sends a permutations to its “sign” is a multiplicative character (in fact the only one, see exercise 2.3 below).

2.3. If \( \rho : G \to \text{Aut}_k(V) \) is a representation, its determinant \( \text{det} \rho : G \to k^* \) is a multiplicative character, and the exterior power \( \wedge^n V \) a one dimensional representation, \( n \) being the dimension of \( V \).

**Problems**

2.1. Let \( G \) be a finite group. If is of odd order, show that \( \hat{G}(Q) = \{ 1 \} \). Describe \( \hat{G}(Q) \) for a general finite group.

2.2. Assume that \( G \) is a \( p \)-group and that \( q = p^r \). Show that \( \hat{G}(\mathbb{F}_q) = \{ 1 \} \).

2.3. Show that commutator group \([S_n, S_n]\) of the symmetric group \( S_n \) is equal to the alternating group \( A_n \). Conclude that the sign is the only non-trivial multiplicative character of \( S_n \).

2.4. Let \( \chi \) and \( \chi' \) be two multiplicative characters of \( G \). Show that \( L(\chi \chi') = L(\chi) \otimes L(\chi') \).
2.5. Show that \( L(\chi)^* = L(\chi^{-1}) \) and that \( \text{Hom}_k(\chi, L(\chi')) = L(\chi'\chi^{-1}) \).

2.6. Assume that \( G \) is perfect group; i.e., it holds true that \( G = [G : G] \). Show that \( G \) does not possess any non-trivial one dimensional representations.

2.7. Show that the multiplicative characters are class functions; i.e., they are constant on the conjugacy classes of \( G \).

2.8. Let \( N \subseteq G \) be a normal subgroup and let \( \chi \in \hat{G}(k) \). Show that the restriction \( \chi|_N \) is invariant; that is, \( \chi(ng^{-1}) = \chi(n) \) for all \( n \in N \) and \( g \in G \). The invariant multiplicative characters form a subgroup of \( \hat{N}(k) \) denoted by \( \hat{N}(k)^G \).

2.9. Let \( G \) be a group being semi-direct product\(^3\) of two subgroups \( A \) and \( N \). Show that any multiplicative character \( \chi \) of \( G \) can be factored \( \chi = \chi_A \chi_N \) where \( \chi_A \) is a multiplicative character of \( A \) and \( \chi_N \) is one on \( N \) that is invariant; i.e., \( \chi_N(ana^{-1}) = \chi_N(n) \) for all \( a \in A \) and all \( n \in N \). Conclude that \( \hat{G}(k) = \hat{A}(k) \times \hat{N}(k)^A \) where \( \hat{N}(k)^A \) denotes the invariant multiplicative characters on \( N \).

2.10. With reference to problem 2.9 above, in the case that \( G \) is the direct product of \( A \) and \( N \)—that is when \( A \) and \( N \) commute—show that \( \hat{G}(k) = \hat{A}(k) \times \hat{N}(k) \).

2.2 Abelian groups

It is a fundamental fact from linear algebra that a finite collection of commuting diagonalizable operators share a basis of eigenvectors. For two operators, say \( s \) and \( s' \), any eigenspace of one is invariant under the other; indeed if \( s \cdot v = \lambda v \) one has

\[
s(s' \cdot v) = s'(s \cdot v) = s'(\lambda v) = \lambda s' \cdot v,
\]

and the eigenspace \( V_\lambda \) of \( s \) is invariant under \( s' \). But the restriction of \( s' \) to \( V_\lambda \) persists to be semi-simple (in our present setting, this is obvious since \( s'|_{V_\lambda} \) is of finite order prime to the characteristic of the ground field). Hence \( V_\lambda \) has a basis of eigenvectors of \( s' \) and these are sheared by \( s \) and \( s' \). When more than two operators are involved, the statement follows by induction on their number.
(2.1) Now, let $A$ be an abelian group and $V$ a representation of $A$ over a big friendly field $k$ (i.e., a field where $n = |A|$ is invertible which contain all $n$-th roots of unity). Hence for any element $a$ the endomorphism $a|_V$ can be diagonalized, and by the fundamental fact cited above, the space $V$ has a basis of eigenvectors common to all members of $A$.

If $v \in V$ is such an eigenvector sheared by all $a \in A$, the subspace $<v>$ is a one dimensional representation of $A$. Letting $\chi(a)$ be the corresponding eigenvector of $a|_V$ we obtain a multiplicative character $\chi : A \to k^*$; indeed, if $a'$ is another element in $A$, the following little calculation

\[ aa' \cdot v = a \cdot (a' \cdot v) = a \cdot \chi(a')v = \chi(a')a \cdot v = \chi(a')\chi(a)v, \]

shows that the eigenvalue $\chi(aa')$ of $aa'$ equals $\chi(a')\chi(a)$. Hence the representation on the subspace $<v>$ is isomorphic to $L(\chi)$. Grouping together eigenvectors with the same multiplicative character, we obtain the following structure theorem for representations of abelian groups over big and friendly fields:

**Theorem 2.1** Let $A$ be an abelian group and let $k$ a big and friendly field for $A$. Then any finite representation can be decomposed as

\[ V \simeq \bigoplus_{\chi \in \hat{A}(k)} n_{\chi} L(\chi), \]

where the $n_{\chi}$’s are natural numbers uniquely determined by $V$.

(2.2) The theorem merits a few comments. First of all it is far from true if the characteristic $p$ divides the order of $A$; we have seen examples. Neither does it hold if there are not enough $n$-th roots in $k$; we have seen examples. Decomposing $V$ into eigenspaces gives an intrinsic and canonical decomposition whereas the one in 2.1 depends on a choice of bases for the eigenspaces. One has

\[ V = \bigoplus_{\lambda} V_{\lambda} \]

where $V_{\lambda}$ is the eigenspace of $\chi$; that is, $V_{\lambda} = \{v \in V \mid g \cdot v = \chi(g)v \text{ for all } g \in G\}$.

(2.3) To complete the theorem, we need a description of the dual groups $\hat{A}(k) = \text{Hom}_{Ab}(A, k^*)$, and with the hypothesis there they are tightly related to $A$; in fact they turn out to isomorphic to $A$, although not canonically.

If $n$ is the order of $A$ all the multiplicative characters take values in the group $\mu_n(k)$ of $n$-th roots of unity. With the hypothesis in the theorem that $k$ be big and friendly$^4$, this is a cyclic group of order $n$, and $\hat{A}(k) = \text{Hom}_{Ab}(A, \mu_n(k))$.

$^4$ The hypothesis means that the polynomial $t^n - 1$ splits into $n$ distinct linear factors over $k$. 

It is a well known and easy fact that the endomorphism group $\text{Hom}_{\text{Ab}}(C_n,C_n)$ of a cyclic group $C_n$ is cyclic of order $n$; in fact, it is (even canonically) isomorphic to $\mathbb{Z}/n\mathbb{Z}$. The isomorphism sends the residue class of $i$ to the $i$-power map $g \mapsto g^i$.

**Proposition 2.2.** Let $A$ be a finite abelian group and $k$ a big and friendly field for $A$. Then the dual group $\text{Hom}_{\text{Ab}}(A,k^*)$ is isomorphic to $A$. The canonical evaluation map is an isomorphism $A \cong \text{Hom}_{\text{Ab}}(\text{Hom}_{\text{Ab}}(A,k^*),k^*)$

**Proof:** When $A$ is cyclic, the first statement follows by the remarks preceding the proposition. The general case is then a consequence of the functor $\text{Hom}_{\text{Ab}}(-,k^*)$ being additive and the fundamental theorem for finite abelian groups, they are all direct products of cyclic groups.

The biduality map sends an element $g$ in $A$ to the evaluation map $\phi \mapsto \phi(g)$ and clearly is injective. But the first statement implies that both groups have the same order and consequently the biduality map is an isomorphism.

**Problems**

2.11. Let $A$ be an abelian group and $k$ a field. Show that a representation $V$ of $A$ over $k$ is absolute irreducible if and only if it is one-dimensional.

2.12. Show that $K_0(C_n;C) = \mathbb{Z}[\eta]$ where $\eta$ is a primitive $n$-root of unity.

2.13. Let $A$ be an abelian group that decomposes as $A \cong \prod_i C_{n_i}$ in a product of cyclic groups. Show that $K_0(A;C) = \mathbb{Z}[\eta_1,\ldots,\eta_r]$ where $\eta_i^{n_i} = 1$.

2.14. Let $A$ be a non-cyclic abelian group and $k$ a field whose characteristic is prime to the order $|A|$ and $V$ a representation of $A$ over $k$. Show that there is a non-zero element $v \in V$ and a non-trivial element $a \in A$ such that $a \cdot v = v$ (equivalently that $t - 1$ divides the characteristic polynomial of $a|_V$). **Hint:** Let $K$ be the field obtained by adjoining the appropriate roots of unity to $k$. Establish that there is an element $a \in A$ that solves the problem for $V_K = K \otimes_k V$. Check that $a$ solves the problem for $k$ as well by using that $a|_V$ and $a|_{V_k}$ have the same characteristic polynomial.

*
2.3 Examples in positive characteristic

As usual there are two dramatically different situations according to the being friendly or not for the group $A$, which still is supposed to be abelian; that is according to the characteristic $k$ being zero or prime to $|A|$ or not. In the former case irreducibles and indecomposables coincide, and we saw that the irreducibles all are one dimensional (since $A$ is abelian). In the latter case, when the field is not friendly, the representation theory becomes very complicated, and except for a rather restrictive class of groups (those having cyclic Sylow $p$-subgroups) there are many more indecomposable than irreducibles, for most groups even infinitely many. This part of the world is hardly understood, and the realistic group theorist might even say the terrain is inaccessible. To give a taste of what tribulations one encounter in this wilderness of representations of $p$-groups in characteristic $p$ we give two examples: The cyclic group $C_{p^m}$ in characteristic $p$ and the Klein four-group $C_2 \times C_2$ in characteristic 2.

The cyclic group $C_{p^m}$

We begin with representations of the cyclic group $C_{p^m}$ over a field $k$ of characteristic $p$, and we shall see that $k$ endowed with the trivial action is the only irreducible $C_{p^m}$-module (this is a feature sheared by all $p$-groups in characteristic $p$) but there will be $p^m$ non-zero indecomposable modules, one of each dimension between 1 and $p^m$.

The choice of a generator $g$ for $C_{p^m}$ induces an isomorphic between the group algebra $k[C_{p^m}]$ and the algebra $R = k[t]/(t^{p^m} - 1)$ with $g$ corresponding to $t$, so $g$ acts on elements $P(t)$ in $R$ by $g \cdot P(t) = tP(t)$.

In characteristic $p$ it holds true that $(t^{p^m} - 1) = (t - 1)^{p^m}$. The algebra $R$ is therefore a local algebra whose maximal ideal equals $(t - 1)^{p^m}R$, and all other ideals are powers of this ideal. For each integer $i$, with $0 \leq i \leq p^m$, we pose $V_i = (t - 1)^{p^m-i}R$; that is, $V_i$ is the ideal in $R$ generated by $(t - 1)^{p^m-i}$. One has $V_0 = 0$ and $V_{p^m} = R$. The subspaces $V_i$ being ideals are all invariant under the action of $C_{p^m}$ (since $g$ acts as multiplication by $t$), and they form an ascending chain whose subquotients all equal $k$ with trivial action; hence the spaces $V_i$ live in short exact sequences

$$0 \longrightarrow V_{i-1} \longrightarrow V_i \longrightarrow k \longrightarrow 0.$$ 

One deduces by induction that each $V_i$ is a representation of the group $C_{p^m}$ with $\dim V_i = i$.

The representations $V_i$ are not irreducible when $i \geq 2$ (they contain $V_{i-1}$), but they are all indecomposable. Indeed, any invariant subspace of $V_i$ is an
ideal in \( R \) since \( g \) acts as multiplication by \( t \), and the ideals form, as we saw, a linearly ordered chain so two cannot be complementary. In fact, the \( V_i \)'s are all the indecomposable representations of \( C_{p^m} \). We have

**Proposition 2.3** Let \( k \) be a field of characteristic \( p \). The \( V_i \)'s defined above are the only indecomposable \( C_{p^m} \)-modules over \( k \), so that any finite \( C_{p^m} \)-module \( V \) over \( k \) is isomorphic to a direct sum of the \( V_i \)'s; that is, one has an isomorphism

\[
V \cong \bigoplus_{1 \leq i \leq p^m} n_i V_i.
\]

**Proof:** As \( V \) is killed by \((t - 1)^{p^m}\), one deduces by the fundamental theorem for finitely generated modules over \( k[t] \), that \( V \) is a direct sum of modules of the form \( k[t]/(t - 1)^i \). But sending 1 to \((t - 1)^{p^m - i}\) gives an isomorphism from \( k[t]/(t - 1)^i \) to \( V_i \).

**The Klein four group**

We now come to the Klein four group \( G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) over a field \( k \) of characteristic 2. Its representations are in fact fully classified,\(^6\) but we content ourselves to show there are infinitely many of arbitrary high dimension. For a detailed exposition and further references one may consult the book by Beson.\(^7\)

Letting \( x \) and \( y \) correspond to two generators of \( G \) one finds

\[
k[G] = k[x, y]/(x^2 - 1, y^2 - 1) = k[s, t]/(s^2, t^2),
\]

where \( s = x - 1 \) and \( t = y - 1 \). Pose \( R = k[s, t]/(t^2, s^2, st) \). It is a quotient of \( k[G] \) and clearly any indecomposable \( R \) module is an indecomposable \( k[G] \)-module as well.

It is not very difficult to give infinitely many examples of representations of the Klein four-group, but checking they are indecomposable can appear a little tricky. The following is a devise to do that checking. For an \( R \)-module \( V \) denote by \( I(V) \) the subspace of \( V \) generated by the images of \( s|_V \) and \( t|_V \), that is \( I(V) = s \cdot V + t \cdot V \), and let \( C(V) \) denote the quotient \( V/I(V) \). This yields the short exact sequence

\[
0 \rightarrow I(V) \rightarrow V \rightarrow C(V) \rightarrow 0.
\]

Since \( s^2 = t^2 = st = 0 \) in \( R \) the two multiplication maps \( s: V \rightarrow V \) and \( t: V \rightarrow V \) both kill \( I(V) \), and hence they factor through \( C(V) \) and induce maps

---

\(^6\) This is contrary to what happens for \( \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \), with \( p > 2 \), whose indecomposable seems totally out of reach.

\(^7\) See Beson for further details.
$s'$ and $t'$ from $C(V)$ to $I(V)$. If $V$ decomposes as a direct sum of $G$-modules, both $I(V)$ and $C(V)$ decompose accordingly, and the two induced maps $s'$ and $t'$ respect these decompositions. So, a representation for which this is not the case, is an indecomposable representation.

To construct the infinitely many examples, one goes the other way around and starts by giving the maps $s'$ and $t'$ that do not decompose as direct sums.

Let $U$ be a vector space of dimension $n$ and $\tau: U \to U$ an endomorphism without invariant subspaces. For example, any nilpotent endomorphism with a one-dimensional kernel will do; indeed, any invariant subspace must contain the kernel and therefore two invariant subspaces cannot be complementary. We put $V = U \oplus U$ (the first summand corresponds to $I(V)$ and the second to $C(V)$) and let $s$ and $t$ be given as

$$s = \begin{pmatrix} 0 & \text{id}_U \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad t = \begin{pmatrix} 0 & \tau \\ 0 & 0 \end{pmatrix}.$$  

An easy verification shows that $s^2 = t^2 = st = 0$. The image of $s$ equals the first summand in $U \oplus U$ where also the image of $t$ lies. We deduce that $C(V)$ can be identified with the second summand and that $s' = \text{id}_U$ and $t' = \tau$. It follows that $V$ is irreducible because $\tau$, and hence $t'$, has no invariant subspace. The dimension of $V$ is $2n$ so we certainly get infinitely many non-isomorphic representations.

**Problems**

2.15. Let $n$ be a number that factors like $n = p^m p'$ with $p$ a prime and $p'$ prime to $p$, and let $k$ be field of characteristic $p$ containing all $p'$-roots of unity. Let $C_n$ be a cyclic group of order $n$, so that $C_n = C_{p'} \times C_{p^m}$. Show that the indecomposable representations of $C_n$ are the representations $L(\chi) \otimes_k V_i$ where $1 \leq i \leq p^m$ and $\chi \in \text{Hom}_{\text{Ab}}(C_{p'}, k^*)$.

2.16. Let $p$ be a prime and $C_n$ a cyclic group of order $n$. Show that $K_0(C_n, \mathbb{F}_p) = K_0(C_{n'}, C)$ where $n'$ is the $p'$-part of $n$.

2.17. Assume that $G$ is a $p$-group and that $k$ is a field of characteristic $p$. Show that $k$ is the only irreducible representation of $G$ over $k$. Hint: Let $V$ be a representation and show by induction on the order $|G|$ that $G$ has a non-zero fixed vector in $V$; i.e., a $v \in V$ with $g \cdot v = v$ for all $g \in G$. A useful fact is that the centre $Z(G)$ is non-trivial.

2.18. With notations as in the previous paragraphs, show that two representations of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ are isomorphic if and only if the corresponding $s'$-maps
and $t'$-maps are simultaneously conjugate. Show that if $k$ is an infinite field of characteristic two, there are infinitely many non-isomorphic irreducible representations of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ of each dimension.

2.19. Show that $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ has irreducible representations of any dimension; in fact infinitely many. HINT: Check that the above argument for the Klein group goes through mutatis mutandis.
3

Complete reducibilty— Schur, Wedderburn and Maschke

Very preliminary version 0.4 as of 14th November, 2017
Klokken: 09:24:36

Changes: 23/8: Tidied up here and there; added exercises 3.2 to 3.5.
27&28/8: Many changes; extensive reorganization and tiding up. Corrected some errors. 28/8: Added a few words about the Jacobson ideal
30/8: Rewritten WedderburnII + proof theorem 3.7 on page 62. Written some more about Jacobson radical and added some exercises. Added two exercises about the centre, 3.18 and 3.19
31/8: Added a corollary to Schur’s lemma about absolute irreducible reps (prop 3.4). Added an exercise about quaternions (problem 3.1)
4/9: The last section with examples is rewritten. Minor cosmetic changes elsewhere.
18/9: Corrected errors in the last section about dihedral groups. Added an exercise about $A_4$
(problem 3.27). Corrected several misspellings.

The ultimate aim of the theory, or at least one of them, is to describe all finite dimensional representations of a finite group $G$ over a field $k$. In the case the order $|G|$ is prime to the characteristic $p$ of the ground field $k$, this feasible, but, in contrast, when $p$ divides $|G|$ it seems to be an utterly difficult, if not hopeless, task in general.

When $p$ and $|G|$ are relatively prime, the situation is satisfactory. There is a certain number of simple representations that serve as building blocks in the sense that every other finite dimensional representation is isomorphic to a direct sum of these simple ones—this is the principal content of Maschke’s theorem. Hence the principle task is to describe these simple representations—in terms of the properties of the given group, of course—as well as the $G$-equivariant maps between them, and for this latter task Schur’s lemma is the main tool. Over algebraically closed fields, Schur’s lemma suffices to describe all maps well, but in general certain division algebras, that depends on $G$ and $k$, intervene and must be determined by other means.

Recall that a representation $V$ of the group $G$ is said to be $\textit{irreducible}$ if it contains no
non-trivial, proper \( G \)-invariant subspace. It is said to \textit{if} has no non-trivial, proper and \( G \)-invariant direct summand. In the good case that the order \( |G| \) of \( G \) is prime to the characteristic these two notion coincide.

For instance if \( G = C_p \) and \( k \) is of characteristic \( p \) a two dimensional space \( V \) with basis \( v \) and \( w \) and and a generator \( g \) acting as \( g \cdot v = v + w \) and \( g \cdot w = w \), is a simple example of a indecomposable space that is not irreducible.

3.1 \textit{Schur’s lemma}

In his article “Neue Begründungen der Theori der Gruppencharaktere“, which appeared in 1905, the German mathematician Issai Schur proved a famous result that nowadays is called “Schur’s lemma”. It seems that Burnside had obtained a similar result some years before, but under the stronger assumption that the ground field is the field \( \mathbb{C} \) of complex numbers. Schur’s proof hits the nail on the head and works in extreme generally (it is really about simple objects in abelian categories). We begin with formulating Schur’s lemma for groups, and afterwards we give the general statement for modules over a ring. The proofs are \textit{mutatis mutandis} identical.

\textbf{Proposition 3.1 (Schur’s lemma)} Let \( V \) and \( V' \) be two irreducible representations of the group \( G \). Then any \( G \)-equivariant map \( \phi: V \to V' \) is either zero or an isomorphism.

\textbf{Proof:} Assume that \( \phi \) is not the zero map. The representation \( V \) being irreducible the kernel \( \ker \phi \) is not the entire space \( V \); hence it is zero and \( \phi \) is injective. Neither is the image \( \text{im} \phi \) zero, and since \( V' \) is irreducible, it equals the entire space \( V' \), and \( \phi \) is surjective as well.

\textbf{Proposition 3.2} Let \( V \) be an irreducible representation of the group \( G \). Then \( \text{End}_G(V) \) is a division algebra over \( k \).

\textbf{Proof:} Any endomorphism \( \phi \in \text{End}_G(V) \) that is not zero, is invertible by Schur’s lemma.

\textbf{Proposition 3.3} If \( V \) is an irreducible representation of \( G \) over the algebraically closed field \( k \), it holds that \( \text{End}_G(V) = k \); that is, any endomorphism of \( V \) is a homothety.

\textbf{Proof:} Let \( \phi \) be an element in \( \text{End}_G(V) \). Since \( k \) is algebraically closed, the endomorphism \( \phi \) has an eigenvalue \( \lambda \) and \( \phi - \lambda \cdot \text{id}_V \) is an endomorphism of
V that is not injective. Hence \( \phi - \lambda \cdot \text{id}_V \) vanishes identically by Schur’s lemma, and \( \phi \) is a homothety.

(3.1) This last corollary can be strengthened substantially. The natural hypothesis not being about the field but about \( V \), and it is that \( V \) be absolute irreducible.

**Proposition 3.4** Assume that \( V \) is a representation of \( G \) over a field \( k \), and assume that \( V \) is absolutely irreducible. Then \( \text{End}_G(V) = k \)

**Proof:** Let \( \phi: V \to V \) be an \( G \)-endomorphism. The characteristic polynomial of \( \phi \) has a root on a finite extension \( K \) of \( k \). Hence the \( G \)-endomorphism \( \phi_K = 1 \otimes \phi \) of \( V_K = K \otimes_k V \) has an eigenvalue \( \lambda \in K \). so that \( \phi_K - \lambda \cdot \text{id}_{V_K} \) has a non-trivial kernel. The representation \( V \) being absolutely irreducible by assumption, the extended representation \( V_K \) is irreducible, and Schur’s lemma entails that \( \phi_K = \lambda \cdot \text{id}_{V_K} \). Now, if \( \{ v_i \} \) is a basis for \( V \) then \( \{ 1 \otimes v_i \} \) is a basis for \( V_K \), in which the matrix for \( \phi_K \) is the same as the matrix for \( \phi \) in \( \{ v_i \} \). Hence \( \phi_K \) being scalar multiplication by \( \lambda \), the same holds for \( \phi \); that is, \( \lambda \in k \) and \( \phi = \lambda \cdot \text{id}_V \).

**Examples**

In general the division ring \( D = \text{End}_G(V) \) is different from the ground field. The following three examples of groups \( G \) and irreducible representations \( V \) are meant to illustrate this. In two instances the ground field will be \( \mathbb{R} \) and the division algebras \( D \) will be the complex field \( \mathbb{C} \) and the quaternionic algebra \( \mathbb{H} \), and in the third example the ground field is \( \mathbb{Q} \) and the division algebra the cyclotomic field \( \mathbb{Q}(n) \).

3.1. The ground field is \( \mathbb{R} \) and the group is the cyclic group \( \mu_4 \) of fourth roots of unity. It acts on the complex field \( \mathbb{C} \) through multiplication. As a real representation this is irreducible (no line through the origin is invariant) and the ring of endomorphisms is equal to \( \mathbb{C} \) (since for an \( \mathbb{R} \)-linear map commuting with multiplication by \( i \) is the same as being complex linear).

3.2. In this example the ground field is the field \( \mathbb{Q} \) of rational numbers, and group is the cyclic group \( \mu_n \) of \( n \)-th roots of unity for an integer \( n \). The group \( \mu_n \) acts on the cyclotomic field \( \mathbb{Q}(n) \) through multiplication, and this makes \( \mathbb{Q}(n) \) into an irreducible \( \mu_n \)-module over \( \mathbb{Q} \). Indeed, a proper, invariant and non-zero \( \mathbb{Q} \)-vector subspace \( V \subseteq \mathbb{Q}(n) \) would be closed under multiplication by all powers of a primitive root of unity. Hence it would be a \( \mathbb{Q}(n) \)-linear subspace, which is absurd.
One has \( \text{End}_{\mu^n}(\mathbb{Q}(n)) = \mathbb{Q}(n) \), since a \( \mathbb{Q} \)-linear endomorphism of \( \mathbb{Q}(n) \) is \( \mathbb{Q}(n) \)-linear if and only if it commutes with multiplication by a primitive \( n \)-th root of unity.

3.3. The third example is very much in the same flavour as the two preceding ones. In this case we let \( G \) be the quaternionic group. That is, the group consisting of the eight quaternions \( \pm i, \pm j, \pm k \). It acts by multiplication on \( \mathbb{H} \), and it easy to see (just adapt the arguments in the two preceding examples) that \( \mathbb{H} \) is irreducible and that \( \text{End}_{\mathbb{C}}(\mathbb{H}) = \mathbb{H} \) (again, adapt the previous arguments).

**Problem 3.1. (The quaternions).** Let \( \mathbb{H} \) be the subset of \( M_2(\mathbb{C}) \) of matrices shaped like

\[
\begin{pmatrix}
    z & w \\
    -\overline{w} & \overline{z}
\end{pmatrix}.
\]

Check that this is a division algebra *i.e.*, closed under addition and multiplication and every non-zero element is invertible. Identify anti-commuting elements \( i, j \) and \( k \) so that \( i^2 = j^2 = k^2 = -1 \) and \( ij = k \). (Notice, the \( i \) here is not the imaginary unit, but a \( 2 \times 2 \)-matrix).

**Schur’s lemma for modules over rings**

Now, we come to the general statement of Schur’s lemma, and we let \( A \) be a ring (with unit as usual) and \( V \) and \( W \) two irreducible (or \textit{simple} as they are often called) \( A \)-modules. In this context Schur’s lemma takes the form:

**Theorem 3.1 (Schur’s lemma for rings)** Assume that \( V \) and \( V' \) are two irreducible modules over a ring \( A \). Then any \( A \)-module homomorphism \( V \to V' \) is either zero or an isomorphism. The space \( \text{End}_A(V) \) is a division ring.

**Proof:** Mutatis mutandis the same as for the group version 3.1. \( \blacksquare \)

(3.2) Notice that the division ring \( \text{End}_A(V) \) is generally not an algebra over \( A \) since \( a \phi \) is not necessarily \( A \)-linear; indeed, one has \( a \phi(a'v) = a^2 \phi(v) \) and there no reason this be equal to \( a' a \phi(v) \) without supplementary hypothesis on \( a \). For instance, if \( a \) is a central element in \( A \) this holds, and \( \text{End}_A(V) \) is an algebra over the centre \( Z(A) \) of \( A \).

In the case that \( A \) is an algebra of a field \( k \), the endomorphism space \( \text{End}_A(V) \) is contained in \( \text{End}_k(V) \) and \( A \) maps into \( \text{End}_A(V) \), and \( \text{End}_A(V) \) equals the set of \( k \)-linear endomorphisms \( \phi : V \to V \) that commute with those induced from \( A \). This motivates the frequently used name \textit{the commutant} of \( V \) for

\[ \text{The commutant} \]
the endomorphism ring $\text{End}_A(V)$. Clearly $V$ carries a natural structure as an $\text{End}_A(V)$-module ($\phi$ acts on $v$ as $\phi \cdot v = \phi(v)$).

(3.3) If $W$ is another $A$-module, the set $\text{Hom}_A(V, W)$ is a left module over $\text{End}_A(V)$ and a right module over $\text{End}_A(W)$; both module structures being induced by composition. The action of endomorphisms $\phi$ of $W$ and $\psi$ of $V$ on a map $\alpha : V \to W$ is the composition of the three maps

$$V \xrightarrow{\psi} V \xrightarrow{\alpha} W \xrightarrow{\phi} W,$$

that is $\psi \circ \alpha \circ \phi$.

**Extension of Schur’s lemma to direct sums $nV$**

We continue with $A$ being a ring and $V$ an irreducible $A$-module. There is almost an immediate extension of Schur’s lemma to linear maps between direct sums of copies of $V$, that is, a description of the space $\text{Hom}_A(nV, mV)$ of $A$-maps between the direct sums $nV$ and $mV$.

Schur’s lemma tells us that the endomorphisms ring $D = \text{End}_A(V)$ is a division ring, and the obvious guess for $\text{Hom}_A(nV, mV)$ would be the space of matrices $M_{n \times m}(D)$—each summand of $nV$ mapping into each summand of $mV$ with the help of $D$—and indeed, this turns out to be correct.

The result is not deep at all—the situation is close to the situation with linear maps between vector spaces over fields—and the main obstacle to understand what happens, is (like with a soap opera) to keep track of who commutes with whom! Or more seriously phrased: which hom-sets are modules over which rings. One source of confusion is that if $E$ and $F$ are say right modules over $D$, scalar multiplication does not make $\text{Hom}_D(E, F)$ a $D$-module, but of course it is a vector space over the center of $D$.

(3.4) The simplistic approach is to start with the natural map

$$\Phi : M_{n \times m}(D) \to \text{Hom}_A(nV, mV)$$

sending an $m \times n$-matrix $M = (m_{ij})$ to the map $v = (v_i) \mapsto Mv = (\sum_j m_{ij}v_i)$. Since the entries $m_{ij}$ belong to $D$, they commute with elements from $A$, and therefore $\Phi$ is an $A$-linear map (indeed, we have $\sum_j m_{ij}av_i = a \sum_j m_{ij}v_i$). One easily verifies by a classical matrix-product computation that the product of two composable matrices gives the composition of the two maps.

(3.5) Preferring a slightly more functorial viewpoint, we let $E$ and $F$ be two finite right modules over $D$ (or vector spaces over $D$ if you prefer), the case above being $E = nD$ and $F = mD$. In this setting, the above map is nothing but

*We need $E$ and $F$ to be right modules to be sure that $E \otimes_D V$ and $F \otimes_D V$ are well defined.*
the canonical map
\[ \Phi : \text{Hom}_D(E,F) \to \text{Hom}_A(E \otimes_D V, F \otimes_D V) \]
given by \( \phi \mapsto \phi \otimes \text{id}_V \) and it is \( A \)-linear because \( D \) commutes with \( A \). Moreover \( \Phi \) is functorial in both \( E \) and \( F \) as both the hom-sets and the tensor products are, and it is linear over the center of \( D \).

**Theorem 3.2 (Schur's extended lemma)** The canonical map
\[ \Phi : \text{Hom}_D(E,F) \to \text{Hom}_A(E \otimes_D V, F \otimes_D V) \]
is an isomorphism of modules over the center of \( D \).

**Proof:** Clearly \( \Phi \) is additive in \( E \) and \( F \) since both hom-sets and tensor products are, so by induction on ranks we are reduced to case \( E = F = D \). But then the left side reduces to \( \text{Hom}_D(D,D) = D \) and the right to \( \text{Hom}_A(V,V) = D \), and \( d \otimes \text{id}_V \) is just multiplication by \( d \).

(3.6)—**AN EQUIVALENCE OF CATEGORIES.** The map \( \Phi \) being functorial in \( E \) and \( F \) implies that all valid statements of "categorical nature" about right vector spaces over \( D \) have valid counterparts about modules shaped like \( nV \). In other words, the category \( \text{Vec}_{D^{op}} \) is equivalent to the full subcategory of the category of \( A \)-modules whose objects are isomorphic to \( nV \) for some non-negative integer \( n \).

For instance, we can mention the following easy "cancellation" result. If there is a decomposition \( nV \cong mV \oplus U \), then \( U \cong (n-m)V \). In fact, the inclusion of \( mV \) into \( nV \) corresponds to an inclusion of \( nD \) into \( mD \), whose image has a complement \( E \) isomorphic to \( (n-m)D \). The corresponding inclusion of \( (n-m)V \) in \( nV \) has an image which is a complement to \( mV \), and it is isomorphic to \( U \) (since both are isomorphic with \( nV/mV \)).

This property can be generalization in that any submodule of \( nV \) has a complement and is isomorphic to \( mV \) for some \( m \leq n \):

**Lemma 3.1** Assume that \( V \) is an irreducible. Let \( W \cong nV \) and let \( W' \) be a submodule of \( W \). Then \( W' \cong mV \) for some \( m \) and \( W' \) lies split in \( W \); that is, \( W = W' \oplus W'' \) for some submodule \( W'' \).

**Proof:** The proof goes by induction on \( n \). The \( A \)-module \( W' \) is of finite length over \( A \) and hence possesses a minimal non-zero submodule \( L \), which being minimal must be irreducible.

By assumption \( W \cong nV \), and we may consider the corresponding projections from \( W \) to \( V \). At least one of them must be non-zero on \( L \) and therefore restricts to an isomorphism from \( L \) to \( V \) by Schur’s lemma.
The inclusion $\iota: L \to W = nV$ corresponds to an inclusion $D \to nD$, which has a section $\pi_0$. It follows that $\pi = \pi_0 \otimes \text{id}_V$ is a section of $\iota$. Hence $W = L \oplus U$ where $U = \ker(\text{id}_V - \pi)$ and $W' = L \oplus U'$ with $U' = \ker(\text{id}_U - \pi|_U)$. Clearly $U' \subseteq U$ and by the cancellation property above it holds true that $U \cong (n - 1)V$. Induction gives then that $U' \cong m'V$ and that $U'$ lies split in $U$. Hence the lemma follows.

3.2 Jacobson’s and Wedderburn’s theorems

The observation that the modules shaped like $nV$ behave just like vector spaces over $D$, has some important implications. The first one that we present, is a famous result by the Polish-American mathematician Nathan Jacobson’s from 1945, called the density theorem. The second, is equally famous, and characterize simple rings as matrix algebras over division rings.

**Theorem 3.3 (Jacobson’s density theorem)** Let $V$ be a simple $A$-module, and let $v_1, \ldots, v_n$ be vectors in $V$ which are linearly independent over $D$. For any vectors $w_1, \ldots, w_n$ in $V$ there exists an $a \in A$ with $w_i = av_i$

**Proof:** The image $U$ of the map $A \to nV$ that sends $a$ to $(av_i)$ is a submodule of $nV$, and the theorem is equivalent to $U$ being equal to $nV$. Assume that that is not the case. By lemma 3.1 there is a projection $\pi': nV \to nV$ whose image equals $U$. The map $\pi = \text{id}_{nV} - \pi'$ vanishes on $U$, and it is not the zero map as $U$ is supposed to be a proper submodule. Moreover, $\pi$ is given by a non-zero matrix $(d_{ij})$ with entries in $D$; whence $\sum_j d_{ij}v_i = 0$ for all $j$, and at least one $d_{ij}$ does not vanish. Absurd, since the $v_i$’s are linearly independent!

**Footnote:**

Multiplication in $V$ by any element $a$ from $A$ is not always $A$-linear as in general $a(a'v) \neq a'(av)$, but by definition of $D = \text{End}_A(V)$ the operations of $D$ and $A$ on $V$ commute and multiplication by $a$ is $D$-linear. Thus sending $a$ to the multiplication-by-$a$-map we obtain a ring homomorphism $A \to \text{End}_D(V)$.

One of the important consequences of the the density theorem is that this map is surjective when $V$ is irreducible, at least if $A$ is of finite dimension over a field:

**Theorem 3.4 (Burnside)** Let $A$ be a finite dimensional algebra over a field $k$ and let $V$ be an irreducible module over $A$. Then the map $A \to \text{End}_D(V)$ is surjective.

**Proof:** The module $V$ is a finite module over $A$ by assumption, hence it is a finite dimensional vector space over $k$ and a fortiori over the larger $D$. Pick a
basis \( v_1, \ldots, v_n \) for \( V \) over \( D \). For every \( D \)-linear map \( \phi: V \to V \) applying the density theorem to the vectors \( \phi(v_1), \ldots, \phi(v_n) \) one sees that there exists an element \( a \) from \( A \) so that \( av_i = \phi(v_i) \) for \( 1 \leq i \leq n \). Thus the two \( D \)-linear maps \( \phi \) and multiplication-by-\( a \) agree on a basis and therefore \( \phi(v) = av \) for all \( v \).

Recall that a ring \( A \) is said to be simple if the only two-sided ideals in \( A \) are the zero ideal and \( A \) itself. Kernels of ring homomorphisms are always two-sided ideals, and hence we immediately achieve the following corollary.

**Theorem 3.5 (Wedderburn)** Assume that \( A \) is a simple algebra of finite dimension over a field \( k \), and that \( V \) is a simple \( A \)-module. Then \( A \cong \operatorname{End}_D(V) \).

This celebrated theorem was found by Wedderburn in 1908, and had a vast influence on the science of algebra; to cite Emil Artin: This extraordinary result has excited the fantasy of every algebraist and still does so in our day.

The hypothesis that \( A \) be finite dimensional over a field, can be replaced by the weaker finiteness hypothesis that \( A \) be of finite length which was proved by Emil Artin in 1926, and in that form the theorem is known as the Wedderburn-Artin theorem. The theorem will later on be strengthened to also cover the so called semi-simple modules; that is, direct sums of finitely many irreducible modules (theorem 3.7 on page 62).

**(3.2)** Every ring \( A \) possesses at least one simple module (maximal ideals always exist by Zorn’s lemma) and it is elementary that endomorphism rings of finite dimensional vector spaces are matrix-rings; so the choice of a basis for \( V \) over \( D \) gives an isomorphism \( \operatorname{End}_D(V) \cong M_n(D^{op}) \) (notice the \( D^{op} \)). In this manner one obtains a full description of simple finite \( k \)-algebras. They are the matrix-algebras over division algebras of finite dimension over \( k \). (As \( D = \operatorname{End}_A(V) \) it is contained in \( \operatorname{End}_k(V) \) and therefore of finite dimension)

**Corollary 3.1** if \( A \) is a simple algebra of finite dimension over a field \( k \), then \( A \cong M_{n \times n}(D^{op}) \) where \( D \) is a finite dimensional division algebra over \( k \).

The world is however not always as simple as it might seem. One can surely handle matrices, but describing division algebras of finite dimension over fields is in general a complicated matter. They are fully classified just for a few classes of fields. If \( k \) is algebraically closed, however, it is known that their are no other than \( k \) itself:

**Corollary 3.2** Every simple algebra of finite dimension over an algebraically closed field \( k \), is isomorphic to an algebra of matrices with entries in \( k \).
Problem 3.2. Show that if $k$ is algebraically closed and $D$ is a division algebra of finite dimension over $k$, then $D = K$. Hint: If $a \in D$, the field $k(a)$ is contained in $D$.

Problems

3.3. Show that matrix algebras over division rings are simple rings.

3.4. Let $D$ be a division algebra (or a field, if you want). Show that $\text{End}_D(V)$ up to isomorphism has only one irreducible (left) module, namely the vector space $V$ with the obvious action.

3.5. Show the Skolem-Noether theorem: Any automorphism of a matrix algebra is inner. Or in clear text: If $\theta : \text{M}_{n\times n}(k) \to \text{M}_{n\times n}(k)$ is an automorphism, then there exists a matrix $a$ such that $\theta(x) = axa^{-1}$ for all $x \in \text{M}_{n\times n}(k)$. Hint: Letting $b \in \text{M}_{n\times n}(k)$ act on vectors $v \in k^n$ via $b \cdot v = \theta(b)v$ gives a $\text{M}_{n\times n}(k)$-module structure on $k^n$.

3.3 Semi-simple modules—Wedderburn’s second

We continue for a while working with modules over a ring $A$. A What we just did, has a natural extension to modules that are finite direct sums of irreducible modules. Such modules are called semi-simple and they are shaped like

$$V = W_1 \oplus W_2 \oplus \ldots \oplus W_r,$$

where the $W_i$’s are irreducible submodules.

There is another concept complete reducible that requires every submodule to have a complement; i.e., if $V' \subseteq V$ there is an $V''$ such that $V = V' \oplus V''$. These two concept turn out to be equivalent; one has

**Proposition 3.5** Let $A$ a ring and let $V$ be an $A$-module of finite length. Then the following three conditions are equivalent
1. $V$ is complete reducible;

2. $V = \sum_i V_i$ with the $V_i$’s being irreducible submodules;

3. $V = \bigoplus_i V_i$ with the $V_i$’s being irreducible submodules.

The condition that $V$ be of finite length is not necessary, but it renders the proof slightly easier, and of course, it is satisfied whenever $A$ is of finite dimension over a field $k$ and $V$ is a finitely generated $A$-module.

**Proof:**

3 $\Rightarrow$ 2: Trivial.

2 $\Rightarrow$ 1: Assume that $V' \subseteq V$ is a submodule. Let $V''$ be a maximal submodule intersecting $V'$ trivially. Such a module exists trivially since $V$ is noetherian (and because of Zorn’s lemma in general). We claim that $V' + V'' = V$, and this will finish the argument as $V' \cap V'' = 0$ by construction. Assume that $V' + V'' \neq V$. For at least one $j$ it would then hold that $V_j$ was not contained in $V' + V''$, and as $V_j$ is simple, the intersection $V_j \cap V' = 0$. But then $V'' + V_j$ would properly contain $V''$ and meet $V'$ trivially which contradicts the maximality of $V''$.

1 $\Rightarrow$ 3: This is a straightforward induction on the length of $V$. Let $V'$ be a simple non-zero submodule. One has $V = V' \oplus V''$ by the assumption that $V$ be complete reducible, but $V'$ and $V''$ are both of length less that $V$ and the induction hypothesis applies to both.

An immediate and important corollary is that submodules and quotients of semi-simple modules are semi-simple:

**Corollary 3.3** Assume that $V$ is a semi-simple $A$-module. If $W$ is a submodule or a quotient of $V$, then $W$ is semi-simple.

**Proof:** Assume $W$ is a quotient of $V$ and let $\pi: V \to W$ be the quotient map. Since $V$ is semi-simple there is a decomposition $V = \bigoplus_i V_i$ with the $V_i$’s irreducible. Clearly $W = \sum \pi(V_i)$, and each $\pi(V_i)$ is irreducible (or zero). Therefore $W$ is semi-simple by the proposition. Any submodule $W$ of $V$ is also a quotient since by the proposition $V$ complete reducible, and hence $W$ is semi-simple.

The isotypic components

A decomposition of a semi-simple module into its irreducible constituents, like the one in (3.1) above, is not unique. There will be several different such when two or more of the irreducible summands $W_i$ are isomorphic; but of
course, the Jordan-Hölder theorem guarantees that the involved summands are determined up to order and isomorphism. For instance, if $A = k[C_n]$ is the group algebra of a cyclic group $C_n$ over a big and friendly field $k$ (the complex field for example), and $V$ is a finite $k[C_n]$-module, the decomposition

$$V \simeq \bigoplus_{\chi \in \hat{G}} n_{\chi} L(\chi)$$

involves the choice of bases\(^1\) for those eigenspaces $V_\chi$ whose dimension exceeds two.

One may, however, group together those summands $W_i$ in the decomposition (3.1) that are isomorphic, and thus one arrives at a decomposition

$$V = U_1 \oplus \ldots \oplus U_s$$

where each summand $U_j$ is a direct sum of isomorphic, irreducible modules; that is, $U_j \simeq n_j W$ with $W$ one of the $W_i$’s from (3.1). And, of course, the irreducibles that occur for different $j$’s are not isomorphic. We need the following little lemma:

**Lemma 3.2** If $U \subseteq V$ is an irreducible submodule, then $U$ is contained in one of the $U_j$’s.

**Proof:** Let $U_j \simeq nW_j$ with $W_j$ irreducible, and let $\pi_j$ denote the projection from $V$ onto $U_j$. By Schur’s lemma $\pi_j$ vanishes on $U$ unless $U \simeq W_j$, and this happens for only one index $j_0$ since the $W_i$’s are not isomorphic for different $j$’s. Hence $U \subseteq \bigcap_{j \neq j_0} \ker \pi_j$, and this intersection equals $U_{j_0}$.

The reason for this lemma is it shows that the $U_j$ appearing in (3.2) above, is the sum (non necessarily direct) of all sub-modules $V' \subseteq V$ that are isomorphic to $W_j$. Consequently $U_j$ is canonically defined and unique; it is the maximal submodule isomorphic to a module of shape $nW_j$.

The summands $U_j$ in (3.2) are called the **isotypic components** of $V$; and we say that $U_j$ is associated with the irreducible module $W$ if $U_j \simeq nW$ for some $n$, and we introduce\(^3\) the notation $U_W(V)$ for the isotypic component of $V$ associated with $W$. Thus there is a canonical decomposition of a semi-simple module $V$ as a sum of the isotypic submodules, expressible as

$$V = \bigoplus_{W \in \text{Irr } A} U_W(V),$$

\(^1\) To be precise, the choice of a bases modulo scalar.

\(^3\) A more correct notion would be $U_{\omega}(V)$ where $\omega$ stands for the isomorphism type of $W$, but we find the notation $U_W(V)$ simpler and more suggestive.
where the summation takes place over a set of representatives of the isomorphism classes of irreducible $A$-modules, and where $U_W(V)$ is allowed to be zero.

**Example 3.4.** In our illustrative example of a cyclic group $C_n$ acting on $V$ (as usual with $n$ prime to the characteristic of $k$ and $k$ containing all $n$-th roots of unity), the decomposition (3.2) corresponds to the decomposition $V = \bigoplus V_k$ of $V$ into eigenspaces of the different multiplicative characters.

(3.2) When the irreducible module $W$ is fixed, Schur’s lemma entails that the isotypic component $U_W(V)$ depends functorially on $V$. Indeed, when $W$ and $W'$ are non-isomorphic irreducibles, it holds true that $\text{Hom}_A(nW, n'W') = 0$, and consequently any map $\phi : V \to V'$ must take $U_W(V)$ into $U_W(V')$ since $\phi$ composed with the projection onto $U_W(V')$ forcibly vanishes when $W' \not\cong W$.

We have established

**Theorem 3.6 (Isotypic decomposition)** Let $A$ be a ring and $V$ a semi-simple $A$-module. Then $V$ has a canonical decomposition

$$V = \bigoplus_{W \in \text{Irr } A} U_W(V),$$

where the sum is over a set of representatives of the irreducible $A$-modules. For each irreducible $W$, the isotypic component $U_W(V)$ depends functorially on $V$.

**Problem 3.6.** Let $V$ be a semi-simple $A$-module and $W$ an irreducible one. Show that the natural evaluation map $\text{Hom}_A(W, V) \otimes W \to V$ given by $\phi \otimes w = \phi(w)$ is an isomorphism onto $U_W(V)$. Giving $\text{Hom}_A(W, V) \otimes W$ the $A$-structure from the right factor (that is, $a \cdot \phi \otimes w = \phi \otimes aw$), show that the evaluation maps is an $A$-module homomorphism. **HINT:** Use that both sides are additive in $V$.

(3.3)—**Submodules of semi-simples.** The semi-simple modules have a very lucid structure. The maps between them and their submodules are readily understood in terms of the isotypic decomposition. For submodules one has:

**Proposition 3.6.** Assume that $V$ is a semi-simple $A$-module of finite length. Any submodule $U \subseteq V$ is semi-simple and has $U_W(U) = U \cap U_W(V)$ as the isotypic component associated to $W$. That is, the isotypic decomposition of $U$ equals:

$$U = \bigoplus_{W \in \text{Irr } A} U \cap U_W(V).$$

Moreover, $U_W(U)$ lies split in $U_W(V)$. 

IsoTypiskCanonisk
Proof: By corollary 3.3 on page 58, we know that \( U \) is semi-simple and of finite length. Hence it has an isotypic decomposition. By lemma 3.2 above, the isotypic components \( U_W(U) \) are contained in \( U_W(V) \), and lie split there because of lemma 3.1 on page 54.

In clear text, this means that if \( V = n_1W_1 \oplus \ldots \oplus n_rW_r \) is the isotypic decomposition of the semi-simple module \( V \), then its submodules are all of shape \( U = m_1W_1 \oplus \ldots \oplus m_rW_r \), and, naturally, the multiplicities \( m_i \) satisfy \( m_i \leq n_i \).

**Corollary 3.4**  Let \( \pi_W: V \to U_W(V) \) be the projection induced from the decomposition into isotypic components. Then \( \pi_W \) induces an isomorphism between \( U \cap U_W(V) \) and the image \( U_W(U) \) in \( U_W(V) \).

Proof: All the isotypic components components \( U \cap U_{W'}(V) \) of \( U \) with \( W' \not\cong W \) maps to zero in \( U_W(V) \) by Schur’s lemma. Hence \( \pi_W U = \pi_W(U \cap U_W(V)) \).

(3.4)—Homomorphisms between semi-simples. Combining the isotypic decomposition with Schur’s lemma, we readily obtain the following important description of the maps between semi-simple modules:

**Proposition 3.7**  Let \( U \) and \( V \) be two semi-simple \( A \)-modules. Then it holds true that

\[
\text{Hom}_A(U, V) = \bigoplus_{W \in \text{Irr} \ A} \text{Hom}_A(U_W(U), U_W(V)),
\]

where summation takes place over a set of representatives of the irreducible \( A \)-modules.

Pushing this further and combining this theorem with what we called the extended Schur’s lemma (which describes homomorphisms between \( nW \) and \( mW \) as the matrix algebra \( M_{n \times m}(D_W) \) over \( D_W = \text{End}_A(W) \)) we deduces that \( \text{Hom}_A(U, V) \) is just the direct product of such matrix algebra:

\[
\text{Hom}_A(U, V) \cong \prod_{W \in A} M_{n_W \times m_W}(D_W),
\]

where \( n_W \) and \( m_W \) are the multiplicities of \( W \) in respectively \( U \) and \( V \); that is, \( n_W = \dim_{D_W} U_W(U) \) and \( m_W = \dim_{D_W} U_W(V) \).

(3.5)—A categorical statement: In the end, we have described the category \( \text{SemSim}_A \) that is the full subcategory of \( \text{Mod}_A \) whose objects are the semi-simple \( A \)-modules. It is equivalent to a product of categories of vector spaces:

**Proposition 3.8**  Let \( A \) be an algebra of finite dimension over \( k \). Then there is a natural equivalence of \( k \)-linear categories

\[
\text{SemSim}_A \cong \bigotimes_{W \in \text{Irr} \ A} \text{Vect}_{D_W}.
\]
3.3.1 The final version of Wedderburn’s theorem

In paragraph (3.1) on page 55 we introduced, for any irreducible A-module W, the map \( A \to \text{End}_{D_W}(W) \) that sends element \( a \) to \( a|_W \), the “multiplication-by-a-on-W-map”. And we showed it to be surjective. (Remember that \( D_W = \text{End}_A(W) \), so by the very definition of \( D_W \), multiplication is \( D_W \)-linear).

It is very natural to recollect these maps for different \( W \)'s into a map

\[
A \to \prod_{W \in \text{Irr} A} \text{End}_{D_W}(W)
\]

sending \( a \) to the tuple with \( a|_W \) in the slot with index \( W \). It turns out that under appropriate finiteness conditions (like \( A \) being artinian or of finite dimension over \( k \)), this map is surjective. This is a generalization of the first Wedderburn theorem (theorem 3.5 on page 56), and it is a famous and important theorem which is fundamental for understanding “small” algebras; i.e., artinian algebras, including the objects that interest us the most, group algebras of finite groups over fields.

The endomorphism ring \( \text{End}_{D_W}(W) \) is also an \( A \)-module by way of left multiplication by \( a \); indeed, if \( \phi: W \to W \) is \( D_W \)-linear, \( a \in A \) and \( d \in D_W \), one has

\[
a \phi(dv) = a \cdot d \phi(v) = d \cdot a \phi(v),
\]

since \( a \) and \( d \) commute, and hence \( a \phi \) is \( D_W \)-linear. Moreover,

**Lemma 3.3** Let \( A \) be an algebra of finite dimension over \( k \) and \( W \) an irreducible \( A \)-module. Then as \( A \)-modules one has isomorphisms

\[
\text{End}_{D_W}(W) \cong nW
\]

where \( D_W = \text{End}_A(W) \) and \( n = \text{dim}_{D_W} W \).

**Proof:** If \( w_1, \ldots, w_n \) is a basis for \( W \) over \( D_W \), the map \( \text{End}_{D_W}(W) \to nW \) sending \( \phi \) to the \( n \)-tuple \( (\phi(w_i)) \) is easily checked to be an isomorphism (of \( A \)-modules). \( \square \)

**Theorem 3.7 (Wedderburn)** Let \( A \) be a \( k \)-algebra of finite dimension, then the natural map \( A \to \prod_{W \in \text{Irr} A} \text{End}_{D_W}(W) \) is surjective. In particular, \( A \) has up to isomorphism only finitely many irreducibles modules.

**Proof:** Firstly, as we just saw (lemma 3.3 above), each \( \text{End}_A(W) \) is semi-simple as an \( A \)-module being isomorphism to a direct sum of copies of \( W \). Hence
\[ \prod_{1 \leq i \leq r} \text{End}_{D_{W_i}}(W_i) \] is the isotypic decomposition of a semi-simple \( A \)-module for any finite collection of irreducibles \( W_1, \ldots, W_r \). Secondly, we know that for each irreducible \( W \) the projection \( A \to \text{End}_{D_{W}}(W) \) is surjective (this is the first version of Wedderburn, theorem 3.5 on page 3.5), but then applying corollary 3.4 on page 61 to the image of the map \( A \to \prod_{1 \leq i \leq r} \text{End}_{D_{W_i}}(W_i) \) we infer that this map is surjective. Hence there are can only be finitely many irreducible modules over \( A \) (obviously, \( r \) can at most be equal to \( \text{dim } A \)), and we are through.

(3.1)—The Jacobson radical. The kernel \( J(A) \) of the map in the Wedderburn’s theorem is for obvious reasons of interest. It is called the Jacobson radical of \( A \) and consists of the elements \( a \in A \) that kill all irreducible \( A \)-modules; that is they satisfy \( a|_W = 0 \) for all \( W \in \text{Irr } A \). In particular it is a two sided ideal being the kernel of a ring homomorphism.

**Proposition 3.9** Assume that \( A \) is of finite length (e.g., of finite dimension over a field \( k \)). The Jacobson radical \( J(A) \) is a maximal nilpotent ideal, i.e., it is nilpotent and contains any other nilpotent ideal.

**Proof:** Assume that \( I \) is a nilpotent ideal; say \( I^n = 0 \) and assume that \( I \nsubseteq J(A) \). Then there is an irreducible module \( W \) that is not killed by \( I \), and hence one may find a non-zero vector \( w \in W \) such that \( I \nsubseteq \text{ann } w \). But since \( \text{ann } w \) is a maximal ideal (since \( W \) is irreducible) this means that there is an element \( x \) in \( I \) that can be written as \( x = 1 + y \) with \( y \in \text{ann } w \) (if \( x \in I \) but \( x \notin \text{ann } w \), the ideal \( \text{ann } w + Ax \) contains \( \text{ann } w \) strictly; whence equals \( A \)). Rising this equality to the \( n \)-th power gives \( x^n = 1 + z \) with \( z \in \text{ann } w \), and since by assumption \( x^n = 0 \) for \( n \) sufficiently big, it follows that \( 0 = w + zw = w \), contradicting the fact that \( w \) is non-zero.

To see that \( J(A) \) is nilpotent, let \( \{ W_i \}_{0 \leq i \leq r} \) be a composition series for \( A \); that is, an ascending chain of submodules

\[ 0 = W_0 \subseteq W_1 \subseteq \ldots \subseteq W_r = A \]

such that \( W_{i+1}/W_i \) is an irreducible \( A \)-module. An element \( x \in J(A) \) kills each \( W_{i+1}/W_i \) and hence \( xW_{i+1} \subseteq W_i \). An easy induction then gives that \( x/A = x'/r \subseteq W_{r-j} \). Consequently \( x' \in W_0 = 0 \), and \( x \) is nilpotent.

**Problems**
3.7. Find examples of nilpotent elements that are not in $J(A)$. Hint: Already in matrix algebras one finds such.

3.8. Show that every nilpotent element of the centre of $A$ lies in the Jacobson radical $J(A)$.

3.9. Show that if $W$ is an irreducible $A$-module and $w \in W$ is a non-zero element, then $\text{ann } w = \{ x \in A \mid xw = 0 \}$ is a maximal (left) ideal.

3.10. Show that $J(A)$ is the intersection of all maximal left ideals in $A$.

*  

3.4 Maschke’s theorem

The proof of Maschke’s theorem relies on the technique of averaging over orbits of an acting group. This is a way of producing invariant elements, and naturally, the technique is valuable in a much broader context than the present one. Just like the centre of mass of a rigid body is invariant under any symmetry of the body, the average of a function over orbits is invariant under the action of the group—expressed in a fancy language, the average is just the push forward of the function to the orbit space.

For averages to make sense one must be able to do some sort of integration along the orbits. In our present setting this is a modest request; orbits are finite, and “integrals” are just finite sums. Computing averages requires as well the division by the “volume of the orbit”, which for us will be the number of points in the orbit, and this forces the order of the group to be invertible in field where the functions take their values, i.e., either the characteristic of $k$ is zero or prime to the order $|G|$—in short, $k$ is a friendly field, as we called it.

(3.1) The averaging operator $E$ is the element of the group algebra $k[G]$ defined by

$$E = |G|^{-1} \sum_{g \in G} g,$$

where dividing by $|G|$ is legitimate since $|G|$ is non-zero in $k$. The element $E$ is invariant in the sense that $hE = Eh = E$ for all $h \in G$. Indeed, on has

$$hE = |G|^{-1} \sum_{g \in G} hg = E,$$
since $hg$ runs through $G$ when $g$ does, and that $Eh = E$ follows similarly. Another important property of $E$ is that of being idempotent. This follows from the invariance:

$$E^2 = E(\sum_{g \in G} g) = |G|^{-1} \sum_{g \in G} Eg = |G|^{-1} \sum_{g \in G} E = E.$$  

These two properties entail that $E$ acts on any $G$-module $V$ as a projection operator onto the subspace $V^G$ of invariants vectors. Indeed, $g \cdot E(v) = E(v)$ by invariance and $E(v) = v$ since $E$ is idempotent. We have thus established the following lemma:

**Lemma 3.4**  Let $G$ be a group and let $V$ be a representation of $G$ over a field $k$ friendly for $G$. The operator $E|_V : V \to V$ is a $G$-equivariant projection onto $V^G$. That is, its image equals $V^G$ and it holds true that $E(g \cdot v) = g \cdot E(v)$ and $E^2 = E$.

Be aware, however, that the average $E(v)$ very well might be zero; in fact, it frequently holds true that $V^G = 0$. A stupidly simple instance is the action of the cyclic group $C_2$ with two elements on $k$ through multiplication by $-1$.

(3.2) To arrive at Maschke’s theorem we apply this averaging technique to the $G$-module $\text{Hom}_k(V,W)$ equipped with the action $g \cdot \alpha = g \circ \alpha \circ g^{-1}$. By lemma 1.1 on page 12 the set $\text{Hom}_G(V,W)$ of $G$-equivariant maps equals the set $\text{Hom}_k(V,W)^G$ of invariants in $\text{Hom}_k(V,W)$.

**Theorem 3.8 (Maschke—first version)**  Let $G$ be a finite group whose order is invertible in $k$. Let $V$ and $W$ be two $G$-modules over $k$ and $\phi : W \to V$ a $G$-equivariant map that has a section. Then $\phi$ has a $G$-equivariant section.

**Proof:** Let $q : V \to W$ be any section of $\phi$. It can either be a right section or a left section, but we shall merely treat the case of a left section, right sections being handled mutatis mutandis. So assume that $g \cdot q = q \circ g$. The average over the orbit of $q$ in $\text{Hom}_k(W,V)$ is the map $E(q) : V \to W$ defined by

$$E(q) = |G|^{-1} \sum_{g \in G} g \circ q \circ g^{-1},$$

and by what we said above, $E(q)$ is equivariant. Moreover, since $\phi$ is equivariant and $q$ a left section, it holds that $q \circ g^{-1} \circ \phi = q \circ \phi \circ g^{-1} = q$, hence

$$E(q) \circ \phi = |G|^{-1} \sum_{g \in G} g \circ g^{-1} = \text{id}_W.$$  

\[ \square \]
(3.3) There are two ways a linear map can have a section, either it can be injective and have a left section, or it can be surjective and which case it has a right section. The classical version of Maschke’s theorem is formulated in the former setting:

**Proposition 3.10 (Maschke)** Let $G$ be a finite group whose order is invertible in $k$, and let $V$ be a $G$-module over $k$. Then every $G$-invariant subspace $W$ of $V$ has a $G$-invariant complement; in other words, every $k[G]$-module of finite dimension over $k$ is semi-simple.

**Proof:** The inclusion map $ι: W \rightarrow V$ is equivariant and therefore has an equivariant section $E(ι)$ by the first version of Maschke’s theorem. This section is an equivariant projection onto $W$ having an invariant kernel $\ker E(ι)$ which by standard reasoning is a complement to $W$. For the last sentence, every finite dimensional and complete reducible module is semi-simple by proposition 3.5 on page 57.

(3.4) Notice that one way of phrasing Maschke’s theorem is that (in case $|G|$ is invertible in $k$) any indecomposable representation is irreducible; indeed, any invariant subspace would be a direct summand. So in this friendly case the two notions “irreducible” and “indecomposable” are equivalent.

### 3.4.1 Decomposing into sums of irreducibles

With Maschke’s theorem up our sleeve, we can draw on the general theorems we establish for semi-simple modules. So we have

**Theorem 3.9** Let $G$ be a group and $k$ a friendly field for $G$. Then any finite dimensional representation of $G$ over $k$ decomposes as a direct sum of irreducible representations:

$$V = W_1 \oplus \ldots \oplus W_r.$$  

And of course one may group isomorphic $W_i$’s together, to obtain

**Theorem 3.10** Let $G$ be a group and $k$ a friendly field for $G$. Then any finite dimensional representation of $G$ over $k$ decomposes as a direct sum of isotypic components:

$$V = \bigoplus_{W \in \text{Irr } G} U_W(V).$$

where the sum is over a set of representatives of the irreducible $G$-modules over $k$.

**The structure of $k[G]$**

Combining Maschke’s theorem with Wedderburn’s theorem on the structure of finite algebras over $k$, we obtain a rather complete description of the struc-
ture of the group algebra $k[G]$ in the good case that $k$ is friendly for $G$. The canonical map appearing in Wedderburn’s theorem turns out to be injective as well.

(3.1) We begin with a tiny lemma of interim interest—more informative versions will soon emerge:

**Lemma 3.5** Every irreducible $G$-module $W$ is isomorphic to a direct summand in $k[G]$. The left regular representation $k[G]$ is a direct sum of irreducibles.

**Proof:** Indeed, let $w \in W$ be a non-zero vector and consider the map $k[G] \to W$ sending $\alpha$ to $\alpha \cdot w$. It is clearly a non-zero $k[G]$-homomorphism, and since $W$ is assumed to be irreducible, it is surjective. The second statement comes directly from Maschke’s theorem.

(3.2) With that little lemma in place, we proceed with the following important description of the group algebra:

**Theorem 3.11** Let $G$ be a group and let $k$ be a field where the order $|G|$ of $G$ is invertible. The there is a canonical isomorphism

$$k[G] \simeq \prod_{W \in \text{Irr} G} \text{End}_{D_W}(W).$$

(3.3)

**Proof:** Recall that the map $k[G] \to \prod_{W \in \text{Irr} G} \text{End}_{D_W}(W)$ sends $\alpha$ to the tuple with $\alpha|_W$ in the slot corresponding to $W$. By Wedderburn’s theorem this map is surjective, and it remains to be seen that it is injective as well. So assume that it sends $\alpha$ to zero. This means that $\alpha|_W = 0$ for all irreducibles $W$, but as observed in the modest lemma above, $k[G]$ is a direct sum of such. Hence multiplication by $\alpha$ from the left in $k[G]$ is the zero-map. Consequently, $\alpha = 0$ since $\alpha = \alpha \cdot 1$.

By lemma 3.3 on page 62 we know that $\text{End}_{D_W}(W) \simeq nW$ with $n = \dim_{D_W} W$, so equating the dimensions over $k$ of the two sides in (3.4) gives the following relation between the order of the group $G$ and the dimensional invariants of its irreducibles representations, valid in the context that $k$ is friendly for $G$:

$$|G| = \sum_{W \in \text{Irr} G} (\dim_{D_W} W)^2 \dim_k D_W.$$ 

(3.3)—**The case when $k$ is algebraically closed.** As usual, there is more specific conclusion when the field $k$ is algebraically closed, since in that case all the division algebras $D_W$ reduce to the ground field $k$. We have
Theorem 3.12 Let $G$ be a group and let $k$ be an algebraically closed field where the order $|G|$ of $G$ is invertible. Then there is a canonical isomorphism

$$k[G] \simeq \prod_{W \in \text{Irr } G} \text{End}_k(W).$$

(3.4)

Once more resorting to lemma 3.3 which still is on page 62, we have $\text{End}_k(W) \simeq (\dim_k W)W$, so that the decomposition of the regular representation $k[G]$ takes the form

$$k[G] \simeq \sum_{W \in \text{Irr } G} (\dim_k W)W.$$  

(3.5)

In other words, the multiplicity of the irreducible $W$ in $k[G]$ equals $\dim_k W$.

Equating dimensions of the two sides in (3.5) we arrive at the equality

**Proposition 3.11** Let $G$ be a finite group and $k$ an algebraically closed friendly field for $G$. Then

$$|G| = \sum_{W \in \text{Irr } G} (\dim_k W)^2,$$

where the sum is over a set of representatives for the isomorphism classes of the irreducible representations of $G$.

An extension of Maschke’s theorem

One application of Maschke’s theorem one frequently meets in group theory is when a $p'$-group acts on an abelian $p$-group; for example when an abelian subgroup of a Sylow $p$-subgroup is normalized by a $p'$-group.

In case $A$ is an elementary $p$-group (i.e., a vector space over $\mathbb{F}_p$) a direct application of Maschke’s theorem tells us that any invariant subgroup $A'$ has an invariant complement $A''$; that is, one has $A = A' \oplus A''$ (or $A = A' \times A''$ is $A$ if written multiplicatively). With a careful reading of the proof of Maschke’s theorem, one realizes that it is still valid when the hypothesis that $A$ be elementary is dropped (but of course, it must be abelian and a $p$-group).

**Problems**

3.11. Assume that $G$ is $p'$-group acting on the abelian $p$-group $A$. Show that any invariant subgroup $A'$ has an invariant complement. HINT: If $n = |G|$, multiplication by $n$ in $A$ is invertible.
3.12. Show that if $S \subseteq G$ is a non-normal Sylow $p$-subgroup of $G$, then there is a non-trivial $p'$-subgroup acting on $S$.

3.13. Let $S$ a $p$-group. Show that $S$ has an non-trivial elementary abelian subgroup.

3.14. Assume that $k$ is a friendly field for $G$. Show that the centre of the group algebra $k[G]$ is a reduced ring (i.e., it has no non-zero nilpotent elements).

3.15. Let $e$ be the element of the group algebra $k[G]$ given as $\sum_{g \in G} g$. Show that $e \neq 0$ and that $e^2 = |G| e$. Conclude that $e^2 = 0$ whenever $p$ divides $|G|$. Conclude that the centre of $k[G]$ is not a reduced ring in that case.

3.16. Show that theorem 3.12 and proposition 3.11 still are true when we weaken the hypothesis and only assume that all irreducible $G$-modules over $k$ be absolutely irreducible.  Hint: Proposition 3.4 on page 51 could be useful.

*  

3.5  The number of irreducible representations

When searching for the irreducible representations of a group, it is of course important to know how many we are looking for. The number of irreducible representations depends on the field as well on the group. In the big and friendly case; that is, when $|G|$ is invertible in $k$ and e.g., $k$ is algebraically closed, it turns out to be equal to the number of conjugacy classes in $G$. However, in the opposite case when $k$ is of positive characteristic $p$ with $p$ dividing $|G|$, the number of so called $p'$-classes or $p$-regular classes appears. Those are the conjugacy classes of elements of order prime to $p$, and a theorem of Brauer’s tells us there is as many such classes as there are irreducible representations of $G$.

These results follow from the simple observation that the number of irreducible representations is the same as the number of matrix algebras appearing as factors in the Wedderburn decomposition of $k[G]/J(k[G])$, combined with devices to detect that number.

For instance, in the simple, but important case, when $|G|$ is invertible in $k$ and all the division algebras $D_W$ reduce to $k$—this happens e.g., when $k$ is algebraically closed—the group algebra $k[G]$ is the product of matrix algebras over $k$. As each one of these has a centre of dimension one over $k$, we can conclude that the number of irreducible representations equals the dimension of the centre of $k[G]$. 
The case that \( p \) divides \(|G|\) is more subtle, and one must resort to another one-dimensional space associated with a matrix algebra. The linear subspace \([M : M]\) of a matrix algebra \( M = M_{n \times n}(k)\) generated by the commutators \( \alpha \beta - \beta \alpha\), is of codimension one (indeed, it coincides with the space of matrices having trace zero) and hence \( M/[M : M]\) is a one dimensional quotient of \( M\), and it will serve as the “counting device” in that case.

**The centre of \( k[G] \) and conjugacy classes**

Recall that two elements \( g \) and \( g' \) from the group \( G \) are said to be *conjugate* if \( g' = xgx^{-1} \) for some element \( x \in G\). This is an equivalence relation on \( G\), and correspondingly \( G \) is partitioned into equivalence classes, which are called *conjugacy classes*. The conjugacy classes of \( G \) and the centre of the group algebra \( k[G] \) are closely related. With every conjugacy class \( C \) one may associate the element \( s_C = \sum_{g \in C} g \) of the group algebra which lies in the centre of \( k[G] \).

Indeed, since \( xgx^{-1} \) runs through \( C \) when \( g \) does, one finds that

\[
xs_Cx^{-1} = \sum_{g \in C} xgx^{-1} = \sum_{g \in G} g = s_C. 
\]

The main property of these elements is that they form a basis for the centre of \( k[G] \). The shape of the field \( k \) is not important ; the \( s_C \)'s form in fact a basis for the group algebra \( R[G] \) for any commutative ring \( R \).

**Lemma 3.6** Let \( R \) be any commutative ring. The elements \( s_C \) when \( C \) run through the different conjugacy classes \( C \) form a basis for the center of \( R[G] \).

**Proof:** The elements \( s_C \) are linearly independent, being sums of different elements from a basis for \( R[G] \).

Assume then that \( \alpha \) belongs to the centre of \( R[G] \) and write \( \alpha = \sum a_g \cdot g \). Let \( x \in G \) and consider \( x\alpha x^{-1} \). On one hand \( \alpha = x\alpha x^{-1} \), the element \( \alpha \) being central. On the other hand, after changing the dummy variable from \( g \) to \( x^{-1}gx \), one has

\[
x\alpha x^{-1} = \sum_{g \in G} a_g \cdot xgx^{-1} = \sum_{g \in G} a_{x^{-1}gx} \cdot g.
\]

Hence \( \sum_{g \in G} a_{x^{-1}gx}g = \sum g \) for all \( g \) and all \( x \). One deduces that as a function of \( g \) the coefficient \( a_g \) is constant on conjugacy classes, and denoting the constant value on \( C \) by \( a_C \), one arrives at the equality

\[
\alpha = \sum_C (a_C \sum_{g \in C} g) = \sum_C a_C s_C.
\]
And $\alpha$ is a linear combination of the $s_C$'s.

**Problem 3.17.** In the identification of the group algebra $k[G]$ with the space of $k$-valued functions $L_k(G)$ show that the element $s_C$ associated to the conjugacy class $C$ corresponds to the *characteristic function* of $C$ (i.e., the one that takes the value 1 on elements in $C$ and vanishes elsewhere).

**Problem 3.18.** Show that a subgroup $H \subseteq G$ is normal if and only it is the union of conjugacy classes.

**Problem 3.19.** Let $C_1, \ldots, C_r$ be the conjugacy classes of $G$, and let $a_{ij}^k$ be the number of ordered pairs $(g, h)$ with $g \in C_i$ and $h \in C_j$ such for a given $t \in C_k$ it holds that $gh = t$. Show that this number is independent of $t$ (as long as $t$ belongs to $C_k$) and that $s_{C_i}s_{C_j} = \sum_k a_{ij}^k s_{C_k}$.

**The friendly case**

Assume that the ground field $k$ is algebraically closed and friendly for $G$, so that $k[G]$ is a product of matrix algebras over $k$ with as many factors as there are irreducible representations. The center of $k[G]$ will equal the product of the centers of these matrix algebras (multiplication in the direct product takes place componentwise), and the center of each of the matrix algebras $M_{n \times n}(k)$ is one-dimensional, consisting of the diagonal matrices. Hence we have

**Proposition 3.12** Assume that $k$ is algebraically closed and that $|G|$ is invertible in $k$. The number of irreducible representations of $G$ equals the dimension of the center of $k[G]$.

(3.1) Combining proposition 3.12 and lemma 3.6, we immediately arrive at the fundamental result:

**Theorem 3.13** Assume that $k$ is algebraically closed and that the order of $G$ is invertible in $k$. Then the number of irreducible representations of $G$ equals the number of conjugacy classes in $G$.

**Class functions and class functionals**

The functions on $G$ that are constant on the conjugacy classes are called *class functions* and play an extremely important role. They are at the centre stage of
all treatments of group representations, and we shall come back to them in the next chapter. They enjoy the property that
\[ a(xgx^{-1}) = a(g) \]
for all \( x \) and all \( g \), and substituting \( g = xy \), one sees it is equivalent to
\[ a(xy) = a(yx) \]
for all \( x, y \in G \). We shall denote by \( \text{Cfu}_k G \) the set of class functions with values in \( k \). It is a vector space over \( k \) whose dimension equals the number of conjugacy classes of \( G \).

(3.2) The counterpart of a class function in the realm of \( k \)-algebras is what we shall call a class functional. They also bear the name trace functions, and are linear functionals on \( A \)—that is, linear maps \( a: A \to k \)—satisfying the property
\[ a(\alpha \beta) = a(\beta \alpha), \quad (3.6) \]
for all elements \( \alpha \) and \( \beta \) from the algebra \( A \). They form a vector space over \( K \).

The commutator space of \( A \) is the linear subspace spanned by all commutators (recall that a commutator is an element of the shape \( [\alpha, \beta] = \alpha \beta - \beta \alpha \)). In view of the defining relation (3.6) , a functional is a class functional if and only if it vanishes on the commutator subspace \( [A : A] \). Whence the space of class functionals is naturally identified with \( \text{Hom}_k (A / [A : A], k) \).

(3.3)—The case of group algebras. When \( A \) is a group algebra \( A = k[G] \) of \( G \), the class functionals are naturally tightly linked to the class functions. Any class functional on \( k[G] \) restricts evidently to a class function on the group \( G \), but the converse is also true:

**Lemma 3.7** A functional \( a \) on \( k[G] \) satisfies \( a(\alpha \beta) = a(\beta \alpha) \) for all \( \alpha \) and \( \beta \) if and only if it extends a class function \( G \).

**Proof:** Notice that extensions of class functions vanish on commutators of the form \( gh - hg \). The following computation shows that \( [A : A] \) in fact is generated by such commutators, and consequently the extension of a class function is a class functional:
\[
a \beta - \beta \alpha = \sum_{g} \sum_{h} \alpha_g \beta_h gh - \sum_{g} \sum_{h} \alpha_g \beta_h hg = \sum_{g,h} \beta_h \alpha_g (gh - hg).
\]

\[ \square \]
Corollary 3.5 Regardless of the field $k$, the number of conjugacy classes in $k[G]$ equals $\dim_k k[G]/[k[G] : k[G]]$. The images of any set of representatives $\{g_C\}$ of the conjugacy classes of $G$ form a basis for $\dim_k k[G]/[k[G] : k[G]]$.

Proof: The first part is just a restatement of the lemma. To prove the second, it will suffice to show that the images of the $g_C$'s are linearly independent. For each conjugacy class $D$ let $\delta_D$ be the class functional taking the value one on $D$ and vanishing on all the others. Then $\delta_D(g_D) = 1$, whereas $\delta_D(g_C) = 0$ when $C \neq D$, and it ensues that the $g_C$'s are linearly independent.

(3.4)—The Case of Matrix-Algebras. The arch-example of a class functional would be the good old ordinary trace $tr: M_{n \times n}(k) \to k$, sending a matrix to the sum of the eigenvalues (or the sum of the elements along the diagonal), and with Wedderburn’s theorem in the back of our mind, we are of course largely interested in algebras that are product of matrix algebras. For such we have the following lemma

Lemma 3.8 Assume that $A$ is a product of $r$ matrix algebras $\prod_{1 \leq i \leq r} M_{n_i}(k)$ over a field $k$. Then $\dim_k A/[A : A] = r$. Moreover $[A : A]$ coincides with the space of elements whose trace on every irreducible $A$-module vanishes.

Proof: We treat the case when there is merely one factor, the general statement follows easily from this; so assume that $A = M_n(k)$. The trace is a nontrivial linear function on $A$ vanishing on $[A : A]$, so $\dim_k A/[A : A] \geq 1$. Our task reduces hence to showing that $\dim_k [A : A] \geq n^2 - 1$, and we shall do that by exhibiting that many linearly independent elements in $[A : A]$.

For each pair $(i, j)$ of numbers between $1$ and $n$, let $a_{ij}$ be the $n \times n$-matrix all whose entries vanish except one that resides in place $(i, j)$. Then $a_{ij}$ is a commutator when $i \neq j$ since letting $d_i = a_{ii}$ (which is diagonal) one has

$$d_i a_{ij} - a_{ij} d_i = a_{ij}.$$

This gives $n^2 - n$ linearly independent commutators. For the remaining $n - 1$ commutators we need, notice that the matrix

$$b_i = a_{i1} a_{11} - a_{11} a_{i1}$$

has a one on the first diagonal place, a minus one on the $i$-th and zeros everywhere else. The zealous student should check that the $n^2 - 1$ commutators so obtained are linearly independent.

Coming back to a product with several factors, we have shown that the trace-functions that vanish on all factors except one where they coincide with the traditional trace-function, constitute a basis for $\text{Hom}_k(A/[A : A], k)$. Hence the second statement in the lemma holds. ☐
**Problem 3.20.** If \( k \) is of positive characteristic \( p \), show that all the scalar \( p \times p \) matrices \( \lambda \cdot I \) with \( \lambda \in k \) are of trace 0 and hence are sums of commutators. Exhibit and explicit representation of the identity matrix as a sum of commutator. **HINT:** The matrices \( b \) above can be useful.

**The modular case**

When \( k \) is a field of positive characteristic \( p \) (but still algebraically closed) the above count of the number of irreducible representations is not valid anymore—e.g., cyclic groups \( C_p^m \) of order a power of \( p \) have, as we saw, just one irreducible representations namely the trivial one, but of course, they have \( p^m \) conjugacy classes.

What counts, as was proved by Brauer, are the \( p \)-regular classes, or the \( p' \)-classes as they also are called. Recall that a group element \( g \) is said to be a \( p' \)-element (or a \( p \)-regular element) if its order does not have \( p \) as divisor, and the conjugacy class where it belongs is accordingly called a \( p' \)-class (or a \( p \)-regular class).

**Problem 3.21.** Verify Brauer’s theorem for abelian groups using that all irreducible representations over an algebraically closed field are one-dimensional.

In establishing Brauer’s theorem we shall apply a non-commutative version of the classical Frobenius relation in characteristic \( p \), which says that if \( A \) is a commutative \( k \) algebra, one has \( (a+b)^p = a^p + b^p \). This hinges on the binomial theorem in addition to the binomial coefficients involved all being divisible by \( p \). In the non-commutative case, the binomial theorem is no longer true, but still the Frobenius relation can be salvaged but in a weaker form. The equality is replaced by the congruence \( (a+b)^p \equiv a^p + b^p \mod [A : A] \). This is quite suggestive (\( A/[A : A] \) has a commutative look!), but slightly subtle (\( A/[A : A] \) is not an algebra!), and we postpone the proof to the end of this section in order not to interrupt the “flow of ideas”.

**Theorem 3.14 (Brauer)** Let \( G \) be a group and \( p \) a prime factor of the order \( |G| \). Assume that \( k \) is a field of characteristic \( p \) over which all irreducible \( g \)-modules are absolutely irreducible. Then the number of irreducible representations of \( G \) over \( k \) coincides with the number of \( p \)-regular conjugacy classes.

**Proof:** For typographical reason we put \( A = k[G] \) and \( A_0 = A/J(A) \). We are to show that \( \dim_k A_0/[A_0 : A_0] \) coincides with the number of \( p \)-regular con-
jugacy classes, and we know that a set of representatives \( \{ g_i \} \) of the conjugacy classes in \( G \) forms a basis for \( A/[A:A] \).

Our first observation is that the commutator space \( [A:A] \) is closed under \( p \)-th powers; indeed, with the aid of lemma 3.9 below one achieves the equality

\[
(ab - ba)^p \equiv (ab)^p - (ba)^p = a \cdot bab \ldots ab - bab \ldots ab \cdot a \in [A:A],
\]

where the congruence is taken modulo \( [A:A] \) and the monomial \( bab \ldots ab \) has \( 2p - 1 \) factors.

Now, let \( g \) be any group element. It can be factored as \( g = su \) with \( s \) a \( p' \)-element (that is semi-simple on any module) and \( u \) a \( p \)-element (that is unipotent on any module), and \( s \) and \( u \) commute. The difference \( g - s = s(u - 1) \) is nilpotent hence it acts as an operator of trace zero on any \( G \)-module, in particular on the irreducible ones, and we can deduce that \( g - s \) maps to zero in \( A_0/[A_0:A_0] \). Hence \( A_0/[A_0:A_0] \) is generated by the images of those representatives \( g_i \) that are \( p \)-regular.

Finally, we let \( g_1, \ldots, g_r \) be the representatives of the \( p \)-regular conjugacy classes and suppose that

\[
\sum_i a_i g_i \equiv 0 \quad \text{in} \quad A_0/[A_0:A_0]
\]

which means that \( \sum_i a_i g_i \in J(A) + [A:A] \). Write \( \sum_i a_i g_i = x + y \) with \( x \in J(A) \) and \( y \in [A:A] \) and chose \( r \) big enough that \( x^{pr} = 0 \) and \( g_i^{pr} = g_i \) (which can be done, since the radical \( J(A) \) is nilpotent by proposition 3.9 on page 63 and the \( p \) is prime to the order of \( g \)).

Hence one one hand we have

\[
(\sum_i a_i g_i)^{pr} \equiv \sum_i a_i^{pr} g_i^{pr} = \sum_i a_i^{pr} g_i,
\]

and on the other

\[
(\sum_i a_i g_i)^{pr} = (x + y)^{pr} \equiv y^{pr} + x^{pr} = y^{pr} \in [A:A].
\]

Consequently \( \sum_i a_i^{pr} g_i \) maps to zero in \( A/[A:A] \) and since the \( g_i \)'s are linearly independent there, we deduce that \( a_i^{pr} = 0 \); that is, \( a_i = 0 \) and we are done.

(3.5)—Proof of the “Frobenius-type” lemma.

Lemma 3.9 Let \( A \) be an algebra over a field \( k \) of characteristic \( p \). Then \( (a + b)^p \equiv a^p + b^p \) modulo the commutator space \( [A:A] \).

Proof: Writing out the product \( (a + b)^p \) one arrives at a formula

\[
(a + b)^p = \sum m_i,
\]
where \( m \) runs over all monomials in \( a \) and \( b \) of degree \( p^r \). The cyclic group \( C_{p^r} \) acts on the set of monomials in \( a \) and \( b \) by cyclic permutation of the factors. If \( \sigma \) generates \( C_{p^r} \) and \( m = a^r \cdots x_{p^r} \) is a monomial, the effect of \( \sigma \) acting on \( m \) is

\[
\sigma(m) = x_{p^r} \cdot a \cdot \cdots \cdot x_{p^r-1}.
\]

The only monomials fixed under this action are \( a^{p^r} \) and \( b^{p^r} \), whence any other orbit has \( p^s \) elements with \( 0 < s \leq r \) since in general the number of elements in an orbit divides the order of the acting group.

For any monomial \( m = a^r \cdots x_{p^r} \) the difference

\[
m - \sigma m = x_1 \cdots x_{p^r-1} \cdot x_{p^r} - x_1 \cdots x_{p^r-1}
\]

is a commutator, and it holds that \( m \equiv \sigma m \mod \left[ A : A \right] \); and hence \( m \equiv \sigma^i m \mod \left[ A : A \right] \) for all \( i \). Adding all elements in the orbit of a monomial \( m_0 \) different from \( a^{p^r} \) and \( b^{p^r} \) results in

\[
\sum_{0 \leq i \leq p^r-1} \sigma^i m_0 \equiv \sum_{0 \leq i \leq p^r-1} m_0 = p^s m_0 = 0
\]

the congruence being modulo the commutator space \( \left[ A : A \right] \). Consequently, grouping terms in \( \sum_{m \neq a^{p^r}, b^{p^r}} m \) belonging to the same orbit, we achieve the congruence \( \sum_{m \neq a^{p^r}, b^{p^r}} m \mod \left[ A : A \right] \), and the claim is proven.

3.6 Examples: The dihedral groups and some symmetric groups

After some general observations on symmetric groups we take a closer look at the smaller cases; that is, the symmetric groups \( S_3 \) and \( S_4 \) and give a complete description of their irreducible representations regardless of the characteristic of \( k \). We then turn to the dihedral groups, and determine their irreducible representations in the friendly case, and in some other cases.

The symmetric groups \( S_3 \) and \( S_4 \)

Every permutation can be assigned a sign, and this gives a homomorphism \( S_n \) to \( \mu_2 = \{ \pm 1 \} \). The kernel is the alternating group \( A_n \), which hence is as a normal subgroup of index two, and there is an exact sequence

\[
1 \longrightarrow A_n \longrightarrow S_n \xrightarrow{\text{sign}} \mu_2 \longrightarrow 1.
\]

This shows that in case the ground field is not of characteristic two, there are two multiplicative characters, trivial one and the sign. Hence there are two
one-dimensional representations, the trivial one \( k \) and the alternating one \( L_{\text{sign}} \).
If the characteristic happens to be two, these two coincide. Moreover, as \([S_n : S_n] = A_n\) they are the only one-dimensional representations.

Recall the standard representation \( V_n \) of \( S_n \). It this the permutation representation on the the set \( \{1, \ldots, n\} \) and has a basis \( e_1, \ldots, e_n \), and \( S_n \) is acting on \( V_n \) by permuting the basis elements; that is, \( \sigma(e_i) = e_{\sigma(i)} \). The subspace consisting of vectors \( \sum_i a_i e_i \) with \( \sum_i a_i = 0 \) is an invariant subspace, and the elements \( e_i - e_n \) with \( 1 \leq i \leq n - 1 \) form a basis for it. Indeed, subjected to the condition \( \sum_i a_i = 0 \) one has

\[
\sum_{i \leq n} a_i e_i = \sum_{i \leq n} a_i e_i + a_n e_n = \sum_{i \leq n} a_i e_i - (\sum_{i \leq n} a_i) e_n = \sum_{i \leq n} a_i (e_i - e_n),
\]

and it is clear that the \( (e_i - e_n) \) are linearly independent. We shall denote this subspace by \( U_{n-1} \), and it turns out to be irreducible in the friendly case that \( n! \) invertible in \( k \) (exercise 3.24 below). For \( n = 2 \) it is not difficult to give an ad hoc argument for this, and in general it follows by induction on \( n \).

**Problems**

3.22. Assume that \( k \) is not of characteristic three; the aim of the exercise is to show that \( U_2 \) is irreducible. Show that the matrices of maps induced by the action of permutations \((1,2)\) and \((1,3)\) on \( U_2 \) in the basis above are respectively

\[
M_{(1,2)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad M_{(1,3)} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}
\]

If \( U_2 \) is not irreducible, it must have an invariant one-dimensional subspace, generated by \((a,b)\) say, that is either trivial or alternating. Use \( M_{(1,2)} \) to see that \( a = \pm b \) and conclude by using \( M_{(2,3)} \) that \( a = b = 0 \).

3.23. In the same vein as the previous exercise, this exercise is about the representation \( U_3 \) of the symmetric group \( S_4 \). We assume that the ground field \( k \) is different from two, and the aim is to show that \( U_3 \) is irreducible.

a) Show that \( U_3 \) has no one-dimensional, invariant subspace. \( \text{Hint:} \) Use the transpositions \((1,2)\), \((1,3)\), \((2,3)\) and \((1,4)\).

b) Show that \( U_3^* \) does not have any one-dimensional invariant subspace.

c) Show that \( U_3 \) is irreducible (if the characteristic of \( k \) is not two). \( \text{Hint:} \) If not, either \( U_3 \) or \( U_3^* \) has an invariant subspace of dimension one.
3.24. Assume that \( n \) is invertible in the field \( k \). Show by induction on \( n \) that \( U_{n-1} \) is irreducible. **HINT:** Observe that restricting \( U_{n-1} \) to the subgroup \( S_{n-1} \) that fixes \( e_n \) is isomorphic to \( V_{n-1} \), and hence decomposes at \( k_{S_{n-1}} \oplus U_{n-1} \) with \( U_{n-1} \) irreducible. Conclude that if \( U_{n-1} = A \oplus B \) with both \( A \) and \( B \) non-zero subrepresentations, then either \( A \) or \( B \) is the trivial representation. Deduce a contradiction from this.

(3.1)—**The group \( S_3 \).** This group has six elements, three two-cycles and two three-cycles; correspondingly there are three conjugacy classes. In characteristic different from two and three we have found three irreducibles, the two one-dimensional ones \( k \) and \( L_{\text{sign}} \) and the standard \( U_2 \) of dimension two.

In characteristic two there are two 2-classes, the trivial one and the one containing the three-cycles. The two one-dimensional representations coincide, but \( U_2 \) is irreducible.

Finally, in characteristic three, the two one-dimensional representations are different, but \( U_2 \) is not irreducible; it contains the invariant element \( e_1 + e_2 + e_3 \). The two one-dimensional ones are all irreducible, as there are just two 3-classes, the trivial one and the one containing the two-cycles.

(3.2)—**The group \( S_4 \).** The symmetric group \( S_4 \) has five conjugacy classes the corresponding cycle decompositions schemes are 1, \( (a, b) \), \( (a, b)(c, d) \), \( (a, b, c) \) and \( (a, b, c, d) \), so in characteristic different from 2 and 3, there are five irreducible modules.

We know the standard module \( U_3 \) and the two one dimensional \( k \) and \( L_{\text{sign}} \). One easily checks that \( U_3 \otimes L_{\text{sign}} \) is irreducible as well (if \( V \) was an invariant subspace, \( V \otimes L_{\text{sign}}^{-1} \) would be an invariant subspace in \( U_3 \)), and not isomorphic to \( U_3 \) (one has \( \det(U_3 \otimes L_{\text{sign}}) = \det(U_3) \otimes L_{\text{sign}}^3 = \det(U_3) \otimes L_{\text{sign}} \) which is different from \( \det(U_3) \)). The missing fifth irreducible, comes from the fact that \( S_4 \) has a quotient group isomorphic to \( S_3 \), hence the representation \( U_2 \) of \( S_3 \) gives a representation of \( S_4 \) via “pull back”. That is, its representation map is the composition of the projection \( S_4 \rightarrow S_3 \) with the representation map \( \rho_{U_2} : S_3 \rightarrow \text{GL}(2, k) \).

A good check that we are not completely astray, is to see that the sum of the squares of the dimensions of the representations we have found, equals 24; the order of \( S_4 \):

\[
1^2 + 1^2 + 3^2 + 3^2 + 2^2 = 1 + 1 + 9 + 9 + 4 = 24.
\]

There are just two 2-regular classes, and there are only two irreducible representations: The trivial one and the two dimensional one \( U_2 \) coming from \( S_3 \).
There are four 3-regular classes, and hence four irreducible representations over a field of characteristic three. The two one-dimensional ones, and $U_3$ and $U_3 \otimes L_{\text{sign}}$.

**Problem 3.25.** Show that the permutations in $S_4$ that are the product of two disjoint two-cycles (i.e., those shaped like $(a,b)(c,d)$ with $\{a,b\} \cap \{c,d\} = \emptyset$) together with the unity form a normal subgroup $N$. Show that $N$ is isomorphic to the Klein four group. Show that the quotient $S_4/N$ is isomorphic to the $S_3$. Hint: $S_4/N$ acts by conjugation on $N \setminus \{1\}$.

### 3.6.1 The dihedral groups $D_n$

The dihedral group $D_n$ is of order $2n$ and is generated by two elements $r$ and $s$ that satisfy the relations

$$r^n = s^2 = 1 \text{ and } srs = r^{-1}.$$ 

The elements of $D_n$ are either on the form $r^i$ for $0 \leq i < n$ or $s^i r^j$ with $0 \leq i < n$. It holds true that $s^i r^j = sr^{j-i}$ which easily follows from the relation $srs = r^{-1}$.

**Geometric Construction.** The dihedral group $D_n$ has a geometric incarnation as the isometry group of a regular plane $n$-gon, and is most easily realized in the complex plane. The generator $r$ corresponds to the rotation $z \mapsto \eta z$ with $\eta = \exp 2\pi i/n$, whereas the involution $s$ corresponds to complex conjugation $z \mapsto \bar{z}$. The relation $srs = r^{-1}$ is fulfilled as a $srs$ acts on $z$ as $(\eta z)^{-1} = \eta^{-1}z$, which is in concordance with the action of $r^{-1}$.

In addition to the rotational symmetries a $n$-gon has reflectional symmetries—the reflections through lines dividing the $n$-gon into two equal parts. In case $n$ is odd, these lines are the normals from a vertex to the opposite side, and there are $n$-of those. In case $n$ is even, say $n = 2m$, the bisecting lines come in two flavours. Either they joint two opposite vertices, or they joint the midpoints of two opposite sides. There are $m$ of each of these type of bisectors.

**Conjugacy Classes.** One has $\sigma \tau \sigma = \tau^{-1}$ which shows that the set $A_i = \{r^i, r^{-i}\}$ is a conjugacy class for each natural number $i$. Indeed, the conjugacy class containing $r^i$ cannot be any bigger since its cardinality equals the index $[D_n : C_{D_n}(r^i)]$ which is at most $2n/n = 2$ the whole subgroup $R_n = \langle r \rangle$.

The set $A_i$ has just one element only when $r^i = r^{-i}$; that is, when $2i = 1$. In this case the integer $n$ must be even and $i \equiv n/2 \mod n$, and $r^{n/2} = r^i$ is a central element of $D_n$. In the geometric model $r^{n/2}$ corresponds to inversion through the origin (or multiplication by $-1$ if you prefer). In all other cases $A_i = \{r^i, r^{-i}\}$ is a conjugacy class having two elements.
All the elements $r^i$ are involutions, i.e., elements of order two. One finds $r^i r^j = r^i r^{-j} s$ = 1. In the geometric model they correspond to the reflections through the bisecting lines.

If $n$ is odd, all the involutions are conjugate; indeed, one has $r s r^{-1} = r^2 s$, and as 2 is invertible mod the odd number $n$, any $i$ is on the form $6^{2j}$. Hence in that case there are three types of conjugacy classes. The trivial one $\{1\}$, those shaped like shaped $\{r^i, r^{-i}\}$, of which there are $(n - 1)/2$, or finally, the “big one” consisting of all the involutions $2a = \{s, rs, .., r^{n-1}s\}$.

For later reference we state it as a proposition. The name-giving of the classes follow the frequently used convention (coming from a computer programme called GAP) that the names are composed of a number equal to the order of elements in the class followed by a letter numbering the different classes with elements of the same order.

**Proposition 3.13** Assume that $n$ is an odd number. Then the conjugacy classes of the dihedral group $D_n$ are

- For each $1 \leq i \leq (n - 1)/2$ the class $na_i = \{r^i, r^{-i}\}$,
- The “big one” consisting of all the involutions $2a = \{s, rs, .., r^{n-1}s\}$,
- The trivial one $1a = \{1\}$.

If $n$ is even, the classes $na_i = \{r^i, r^{-i}\}$ are still there, but the one with $2i = n$ reduces to a singleton $2c = \{r^{n/2}\}$. The set of involutions, however, disintegrates into two classes; $2a = \{r^{2i+1}s \mid 0 \leq i < n/2\}$ and $2b = \{r^{2i}s \mid 0 \leq i < n/2\}$, each with $n/2$ elements, and of course there is the trivial class $1a = \{1\}$.

**Proposition 3.14** Assume that $n$ is even. Then the conjugacy classes of the dihedral group $D_n$ are

- For each $1 \leq i < n/2$ the class $A_i = \{r^i, r^{-i}\}$,
- The three classes containing involutions, $2a = \{r^{2i+1}s \mid 0 \leq i < n/2\}$, $2b = \{r^{2i}s \mid 0 \leq i < n/2\}$ and $2c = \{1\}$,
- The trivial class $1a = \{1\}$.

(3.3)—Representations. To every $n$-th root of unity $\eta$ from the field $k$, there is a representation of $D_{2n}$ on $k^2$. The representation map $\rho_\eta$ is given on the generators $r$ and $s$ of $D_{2n}$ by the formulas

$$\rho_\eta(r) = \begin{pmatrix} \eta & 0 \\ 0 & \eta^{-1} \end{pmatrix} \quad \text{and} \quad \rho_\eta(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$
and it is an easy exercise in matrix multiplication (left to the zealous student) to check that the relations \( r^n = s^2 = 1 \) and \( srs = r^{-1} \) are respected. Moreover, replacing \( \eta \) by \( \eta^{-1} \) gives isomorphic representations since \( \rho_{\eta}(s) \) in fact gives an isomorphism between the two, but if \( \zeta \notin \{ \eta, \eta^{-1} \} \) one checks that \( W_{\eta} \) and \( W_{\zeta} \) are not isomorphic.

Moreover, it is not difficult to verify that \( W_{\eta} \) is irreducible if \( \eta \neq \eta^{-1} \). Indeed, if the vector \( v = (a, b) \) generated an invariant subspace of dimension one, it would follow that \( a = b \) since \( v \) is invariant under \( s \), and that \( (\eta a, \eta^{-1} b) \) was a multiple of \( (a, b) \) since it is invariant under \( r \). But \( a = b \neq 0 \) would then imply that \( \eta = \eta^{-1} \). We conclude that in case \( k \) contains \( n \) different \( n \)-th roots of unity, we obtain, according to the parity of \( n \), either \( (n - 1)/2 \) or \( (n - 2)/2 \) non-isomorphic irreducible representations \( W_{\eta} \) of dimension two.

When \( \eta = \eta^{-1} \) obviously either \( \eta = 1 \) or \( \eta = -1 \) and in the latter case \( n \) must be even. In both cases, \( W_{\eta} \) decomposes into a sum of two one-dimensional representations: The two eigenvectors \( (1, 1) \) and \( (1, -1) \) for \( \rho(s) \) (with eigenvalues 1 and \(-1\)) will be both be invariant under \( \rho(r) \). In this way we get up to four one-dimensional representations of shape \( L(\chi) \) with \( \chi \) one of the multiplicative characters given by the table below

<table>
<thead>
<tr>
<th>( \chi(r) )</th>
<th>( \chi(s) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi_0 )</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_a )</td>
<td>1</td>
</tr>
<tr>
<td>( \chi^+ )</td>
<td>-1</td>
</tr>
<tr>
<td>( \chi^- )</td>
<td>-1</td>
</tr>
</tbody>
</table>

When \( n \) is odd, only the two first \( \chi_0 \) and \( \chi_a \) apply. To check we have found all the irreducible representations in the big and friendly case (i.e., \( 2n \) is invertible in \( k \) and \( n \)-th roots lie in \( k \)), we compare with the number of conjugacy classes, there are \((n - 1)/2 + 2\) conjugacy classes if \( n \) is odd, and \((n - 2)/2 + 4\) if \( n \) is even, which is a perfect match!

(3.4) **The case of \( n \) odd and the characteristic of \( k \) two.** All the conjugacy classes \( \{r^i + r^{-i}\} \) are 2-regular, but the one containing the reflections is not, so all except one are 2-regular. When \( k \) contains the \( n \)-th roots of unity, all the two-dimensional representations \( W_{\eta} \) persist, only one one-dimensional representation is lost, as \( \chi_a \) becomes equal to \( \chi_0 \).

The kernel of \( k[G] \to k[G]/J(k[G]) \) is therefore of dimension 1 and generated by the nilpotent \( \sum_{g \in D_{2n}} g \).

(3.5) **The case of \( D_p \) with \( p \) an odd prime and \( k \) of characteristic \( p \).** In this case the conjugacy classes \( \{r^i, r^{-i}\} \) are all irregular and the only two \( p \)-regular ones are the trivial class and the big one consisting of the reflections. The only two irreducible representations are the trivial one \( L(\chi_0) \) and \( L(\chi_a) \).
Problem 3.26. Show that in the case of (3.5) the kernel of \( k[D_p] \to k[D_p] / J(D_p) \) is of dimension \( 2p - 2 \), with the elements \( s - sr^i \) and \( 1 - r^i \) where \( 1 \leq i < p \) forming a basis. Show that \((s - sr^i)^{2p} = 0\) and \((1 - r^i)^p = 0\).

Problem 3.27. Determine all the irreducible representations of the alternating group \( A_4 \) in all characteristics assume the ground field is sufficiently large.

Hint: There is an exact sequence

\[
1 \longrightarrow N \longrightarrow A_4 \longrightarrow C_3 \longrightarrow 1
\]

where \( N \) is as in problem 3.25 above.
4

Characters

Very preliminary version 0.4 as of 14th November, 2017
Klokken: 09:24:36
Just a sketch and will change.

18/9: Substantial changes
19/9: Brushed up chapter 4.1 “Definitions and first properties”
20/9: Added several exercises about permutation representations, exercise 4.4 and 4.5 and 4.9 to 4.12. Added a section about the direct product page 93.
23/9: Has added a section about Burnside’s $p^aq^b$-theorem. Added some exercises on algebraic integers on page 108
2/10: Added a section on some Galois actions; under work!!
5/10: Added a minor observation and an interesting exercise on page 92.

In the years from 1895 to 1898 a well known exchange of letters between Richard Dedekind and Georg Frobenius took place, a correspondence that initiated the representation theory of finite groups. At the time Dedekind was working on the so called group determinant, trying to find its factorization into irreducible polynomials. In the abelian case he could, but he did not succeed for a general finite group. So Dedekind passed the problem to Frobenius, who quickly solved the problem. Doing so, Frobenius made use of the regular characters of the group, albeit not in the guise we know. This was the start of the representation theory for general (non-abelian) groups. Characters of abelian groups, however, had been in use for some time, we find them notably in Dirichlet work on primes in arithmetic progressions.

This chapter is concerned with the representations of finite groups defined over the complex numbers, but the results remain valid over any algebraically closed field of characteristic zero; the field $\mathbb{Q}$ of algebraic numbers being an-
other important example. Eventually we shall prove a theorem of Burnside’s
that, loosely speaking, says the results hold true over a “sufficiently large” field
of characteristic zero, i.e., a field containing all the m’s roots of unity, m being
the exponent of G (the least common multiple of the orders of elements in G).

4.1 Definition and first properties

The heros of the chapter are the so called characters. Given a representation G
afforded by the vector space V over the complex field C, let \( \rho_V : G \to \text{Aut}_C(V) \)
be the representation map. We define the character \( \chi_V \) of the representation to
be the function on G that takes the value \( \text{tr}(\rho_V(g)) \) at the element g; that is,

\[
\chi_V(g) = \text{tr}(\rho_V(g)).
\]

The trace is invariant under conjugation, and \( \chi_V \) is therefore a class function
on G, it is constant on the conjugacy classes of G. Moreover if V and V’ are
isomorphic representations, say \( \theta : V \to V’ \) is an isomorphism, then \( \chi_V = \chi_{V’} \).
Indeed, if \( \{v_i\} \) is a basis for V it holds that \( \{\theta(v_i)\} \) is a basis for V’ and since
\( g_{V'} = \theta \circ g_V \circ \theta^{-1} \) it hold true that \( g_V \) has the same matrix in the basis \( \{v_i\} \) as
\( g_{V'} \) has in the basis \( \{\theta(v_i)\} \) and a fortiori their traces are equal.

**Proposition 4.1** The character of a representation V is a class function. Isomorphic
representations have equal characters.

This property is of course fundamental, but even more fundamental is that
the converse holds—and this is the clue to understand the importance of the
characters—so two complex representation are isomorphic if and only if their
characters are equal. A proof would for the moment would be premature,
some more machinery is needed.

(4.1) One says that the character \( \chi_V \) is irreducible if the representation V is. The
value \( \chi_V(1) \) is the trace of the identity map id\(_V\) and equals the dimension of
V. In the literature it is frequently called the degree of the character \( \chi_V \).

**Example 4.1.** If V is a one-dimensional representation of G, the character \( \chi_V \)
coincides with multiplicative character we introduced on page 39.

**Example 4.2.** Assume that G is the dihedral group = \( D_n \) and that V is one of
the two-dimensional representations \( W_\eta \) as in the paragraph on page 79 with
\( \eta = \exp(2\pi i k/n) \). Then \( \chi_V(r^l) = 2 \cos kj\pi/n \) and \( \chi_V(r^l s) = 0 \).

These characters carry an astonishingly lot of information, and are an unsur-
passed tool for studying groups and their representations.
Problem 4.1. Let $V$ be a complex vector space of dimension $n$, and let $\sigma$ be a semi-simple endomorphism of $V$. Show that $\sigma$ is determined up to conjugacy by the numbers $\text{tr}(\sigma^i)$ for $0 \leq i \leq n$. Hint: Use Newton’s relations between power sums and elementary symmetric functions to deduce that the numbers $\text{tr}(\sigma^i)$ determine the eigenvalues of $\sigma$.

The basic properties

Some of the basic properties of the characters are summarized in the following proposition. With one exception they all follow immediately from corresponding formulas for the trace of linear endomorphisms. For the benefit of students that are not fluent in linear algebra, we have included a quick and dirty recap of these as an appendix to this chapter.

Proposition 4.2 (Basic properties) Given two complex representations $V$ and $W$ of $G$. Their characters satisfy the following properties:

- $\chi_V(1) = \dim V$,
- $\chi_{V\oplus W} = \chi_V + \chi_W$,
- $\chi_{V\otimes W} = \chi_V \chi_W$,
- $\chi_{V^*}(g) = \chi_V(g^{-1})$,
- $\chi_V(g^{-1}) = \overline{\chi_V(g)}$.

Proof: The exception that needs a proof is the very last statement, so let $\lambda_1, \ldots, \lambda_r$ denote the eigenvalues of the endomorphism $\rho(g)$. They are all roots of unity since $g$ is of finite order, and hence $\lambda_i^{-1} = \overline{\lambda_i}$. With this in mind, we find

$$\chi_V(g^{-1}) = \text{tr}(\rho(g^{-1})) = \sum_i \lambda_i^{-1} = \sum_i \overline{\lambda_i} = \overline{\text{tr}(\rho(g))} = \overline{\chi_V(g)}$$

(4.2) We let $\text{Ch}_C(G)$ be the linear subspace of the space of complex class functions $C_fu_C$ $G$ generated by the characters of $G$. The elements are of the form $\chi = a_1 \chi_1 + \ldots + a_r \chi_r$, where $a_i$ are complex constants and the $\chi_i$ are irreducible characters. Such an expression is a genuine character if and only if it has a representation with the $a_i$ being non-negative integers. This follows from the second property above since if $V = a_1 W_1 + \ldots + a_r W_r$, one has $\chi_V = a_1 \chi_{W_1} + \ldots + a_r \chi_{W_r}$. When the $a_i$’s are merely integers—that is, one allows some of them to be negative—one says that $\chi$ is a virtual character. The
virtual characters form a finitely generated subgroup \( \text{Ch}(G) \) of the additive group of \( \text{Ch}_C(G) \) which spans \( \text{Ch}_C(G) \) over the complex numbers.

By the second property (the one concerning direct sums) the character construction gives a map from the representation ring \( K_0(G, C) \) to the ring of complex class functions \( \text{Cfu}_C G \), and the third statement in the proposition (the one concerning tensor products) tells us that this is a ring homomorphism. We shall soon see that this induces a ring isomorphism \( K_0(G, C) \otimes \mathbb{Z} C \simeq \text{Cfu}_C G \).

Examples

4.3. —The trivial character. If \( V \) is a one-dimensional representation, the value \( \chi_V(g) \) is just the eigenvalue of \( g \) on \( V \). The trivial character \( 1_G \) is the constant function on \( G \) with value 1. It equals the character of the trivial representation; that is, a one-dimensional vector space with each \( g \) acting trivially.

4.4. —Permutation representations. Recall the permutation representation from example 1.5 on page 10 associated to the action of \( G \) on a finite set \( X \). There it was denoted by \( L_k(X) \), but when \( k = C \) we shall simply write \( L(X) \) for it. It consists of complex functions on \( X \) with the action \( g \cdot \phi(x) = \phi(g^{-1}x) \). We let \( \chi_X \) denote the character of \( L(X) \).

There is another interpretation (in exercise 4.4 below you are asked to show the two are equivalent, see also the paragraph on page 26 where the case \( X = G \) is treated), namely as the \( C \)-vector space \( C[X] \), with the elements of \( X \) as a basis. The elements of which are of the shape \( \xi = \sum_{x \in X} a_x x \). A group element \( g \) acts on \( C[X] \) by permuting the basis elements in \( X \) according to its action on \( X \). The matrix of \( g \) is therefore a permutation matrix: It has only one non-zero entry in every column and this entry is a 1. Now, this non-vanishing entry resides on the diagonal if and only if the corresponding basis element \( x \in X \) is fixed by \( g \). Hence the trace being the sum of the entries along the diagonal, the character \( \chi_X(g) \) equals the number of fixed points \( g \) has; or expressed with a formula:

\[
\chi_X(g) = \# \{ x \in X \mid gx = x \}.
\]

4.5. One particular permutation representation is \( \text{on} \ k[G] \). It is induced by the action of \( G \) on itself by left multiplication and its character will be denoted by
\( \chi_{\text{reg}} \). One has
\[
\chi_{\text{reg}}(g) = \begin{cases} 
|G| & \text{when } g = 1, \\
0 & \text{when } g \neq 1.
\end{cases}
\]
Indeed, multiplication in \( G \) by a group element \( g \) different from the unity, is fixed point free: \( gh = h \) implies \( g = 1 \).

**Problems**

4.2. Assume that \( H \subseteq G \) is a normal subgroup. Let \( X = G/H \) endowed with the action of \( G \) induced by multiplication. Show that for every coset \( x \in X \) the isotropy group \( G(x) \) equals \( H \). Conclude that
\[
\chi_X(g) = \begin{cases} 
0 & \text{when } g \notin H, \\
[H:G] & \text{when } g \in H.
\end{cases}
\]

4.3. Assume that \( H \subseteq G \) is a subgroup enjoying the property that \( H^g \cap H = \{1\} \) whenever \( g \notin H \), and let \( X = G/H \) be the set of left cosets endowed with the action of \( G \) induced by multiplication. Show that an element \( g \in G \) different from 1 has at most one fixed point. Conclude that \( \chi_X(g) = \begin{cases} 
0 & \text{if } g \notin H, \\
1 & \text{if } g \in H \text{, but } g \neq 1, \\
[H:G] & \text{if } g = 1.
\end{cases} \)
Such groups are called Frobenius groups and the subgroup \( H \) is called a Frobenius complement.

4.4. We refer to the notation in example 4.4 above (except that \( k \) can be any field). Let \( x \) be an element from \( X \) and let \( \delta_x \) be the indicator function for the set \( \{x\} \); that is, \( \delta_x \) is the function on \( X \) with \( \delta_x(x) = 1 \) and \( \delta_x(y) = 0 \) for all other \( y \in X \). Show that \( g \cdot \delta_x = \delta_{gx} \). Show that the map sending \( x \) to \( \delta_x \) is an isomorphism between \( k[X] \) and \( L_k(X) \) as \( G \)-modules.

4.5. *(Burnside’s formula).* Let \( G \) act on the finite set \( X \). Show\(^1\) that the equality
\[
\sum_{g \in G} \# \{ x \mid gx = x \} = m |G|
\]
holds true where \( m \) denotes the number of orbits

\(^1\) This was well known by both Cauchy and Frobenius, but is usually called Burnside’s formula. usually
$G$ has in $X$. **Hint**: Consider the subset $A = \{(g,x) \mid gx = g\}$ of $G \times X$ and compute the cardinality $|A|$ in two ways by analyzing the two projections.

### 4.1.1 Scalar products on the space of functions

On the space $L(G)$ of complex functions on $G$ there is a hermitian product mimicking the $L^2$-product we know from analysis; in fact, it is an $L^2$-product when sums over group elements are interpreted as integrals with respect to the counting measure. In fact, $L(G)$ has another product as well, that is not hermitian but symmetric. It has the virtue of being defined on $L_k(G)$ what so ever the field $k$ is as longs as it is friendly for $G$. In this chapter we exclusively deal with complex representations and shall stick with the hermitian product.

(4.1)—**The hermitian product.** The hermitian product is defined as

$$\langle \alpha, \beta \rangle = |G|^{-1} \sum_{g \in G} \bar{\alpha}(g)\beta(g). \quad (4.1)$$

Linearity in the first variable and symmetry in the sense that $\langle \alpha, \beta \rangle = \langle \beta, \alpha \rangle$, are obvious properties which follow directly from the definition. Moreover, the product is positive definite since

$$\langle \alpha, \alpha \rangle = |G|^{-1} \sum_{g \in G} |\alpha(g)|^2 = \sum_{g \in G} |\alpha(g)|^2 \geq 0,$$

where equality holds if and only if $\alpha = 0$. Whence $\langle \alpha, \beta \rangle$ is a hermitian product.

(4.2)—**The symmetric product.** There is another natural product on $L_k(G)$ (valid for any field $k$ friendly for $G$) which is not hermitian (which has no meaning over a general field $k$), but symmetric. It is given by the formula

$$\langle \alpha, \beta \rangle = |G|^{-1} \sum_{g \in G} \alpha(g)\bar{\beta(g^{-1})}. \quad (4.2)$$

The product is obviously linear in both $\alpha$ and $\beta$ and, exchanging $g$ with $g^{-1}$ we infer that it is symmetric (in the usual sense that $\langle \alpha, \beta \rangle = \langle \beta, \alpha \rangle$) since $g^{-1}$ runs through $G$ when $g$ does. If either $\alpha$ or $\beta$ is a character, the two products coincide. Indeed, say if $\beta = \chi_V$, one has $\beta(g^{-1}) = \overline{\beta(g)}$ by proposition 4.2 on page 85.

The product $\langle \alpha, \beta \rangle$ is *non-degenerate*, meaning that $\langle \alpha, \beta \rangle = 0$ for all $\alpha \in L(G)$ implies that $\beta = 0$. To see this, just take $\beta$ to be the indicator function $\delta_X$
of an arbitrary element $g$ in $G$. Then $\langle \alpha, \delta_g \rangle = |G|^{-1} \alpha(g)$, and we deduce that $\alpha = 0$.

In the same vein one checks that $\langle \alpha, \beta \rangle$ it is non-degenerate on the subspace $Cf_k G$ of $L(G)$ consisting of class function; the indicator functions $\delta_C$ of the conjugacy classes do the trick.

(4.3)—The Hermitian Product and Invariants. A most useful property of the hermitian product is that gives us a means to determine the multiplicity of an irreducible representation in a given representation. Of particular importance, which also will be our starting point, is the case of the trivial representation $1_G$, the general statement follows suit in the next section.

Lemma 4.1 Let $V$ be a complex representation of $G$. One has

$$\text{dim}_C V^G = (\chi_V, 1_G).$$

Proof: It is a primary property of the trace of a projection operator $e$—that is, one satisfying $e^2 = e$—that it equals the dimension of the operators image (this is specific for operators over fields of characteristic zero; in characteristic $p$ one only gets a congruence mod $p$). The averaging operator $E = |G|^{-1} \sum_{g \in G} g$ defined in (3.1) on page 64 is a projection onto $V^G$, whence we find

$$\text{dim} V^G = \text{tr}(E|_V) = \text{tr}(|G|^{-1} \sum_{g \in G} g|_V) = |G|^{-1} \sum_{g \in G} \chi_V(g),$$

which in its turn equals $(\chi_V, 1_G)$. \hfill \Box

(4.4)—Equivariant Maps and the Hermitian Product. The next result connects the hermitian product to “the realities of representations”; that is, it shows we in a certain sense can compare representations by comparing their characters.

Proposition 4.3 If $V$ and $W$ are two complex representations of $G$, one has

$$\text{dim} \text{Hom}_G(V, W) = (\chi_V, \chi_W).$$

Proof: There are two ingredients. Firstly, one has the canonical $G$-equivariant isomorphism $V^* \otimes W = \text{Hom}_k(V, W)$, and from the third and last equality in proposition 4.2 above, one deduces

$$\chi_{\text{Hom}_k(V, W)}(g) = \chi_W(g)\chi_V(g^{-1}) = \chi_W(g)\overline{\chi_V(g)}.$$ 

The second ingredient is the equality $\text{Hom}_G(V, W) = \text{Hom}_k(V, W)^G$, which combined with the pervious lemma and what we just did, gives

$$\text{dim}_k \text{Hom}_G(V, W) = |G|^{-1} \sum_{g \in G} \chi_W(g)\overline{\chi_V(g)}.$$ 

\hfill \Box
4.2 The first orthogonality and the basis theorems

A nice property of the irreducible characters, which is used over and over again, is that they form an orthonormal set with respect to the hermitian product introduced above. This is just Schur’s lemma expressed in the language of characters.

The orthogonality theorem has several corollaries of fundamental importance for the theory. In the forefront is the basis theorem, telling us that the irreducible characters form a orthonormal basis for the space of class functions. The basis theorem is obtained by combining the orthogonality with what we established in the previous chapter, that there are as many irreducible characters as there are conjugacy classes.

The decomposition of a representation into irreducibles can hence be determined from its character by a standard coordinate calculation; one consequence of this being that that a representation is determined up to isomorphism by its character. We finish of the section with a useful irreducibility criterion.

The first orthogonality theorem

As said, expressing Schur’s lemma in the language of characters with the help of the hermitian product gives us the following:

**Theorem 4.1 (First orthogonality theorem)** Let $\chi_V$ and $\chi_W$ be the characters of two complex irreducible representations. Then $\langle \chi_V, \chi_W \rangle = 0$ when $V$ and $W$ are not isomorphic, and $\langle \chi_V, \chi_V \rangle = 1$.

**Proof:** From proposition 4.3 above and Schur’s lemma it follows that

\[
\langle \chi_V, \chi_W \rangle = \dim \text{Hom}_G(V, W) = \begin{cases} 
0 & \text{when } V \simeq W \\
1 & \text{when } V \not\simeq W
\end{cases}
\]

where we use that $C$ is algebraically closed so that $\text{End}_C(W) = C$.

The basis theorem

The immediate—and may be the most important—consequence of the orthogonality is what one calls the basis theorem.

**Theorem 4.2 (The basis theorem)** The complex irreducible characters of $G$ form an orthonormal basis for the space $\text{Cfuc}_G G$ of complex class functions on $G$. 
Proof: The number of irreducible representations equals the dimension of the space of class functions (theorem 3.13 on page 71). By the first orthogonality theorem the different irreducible characters are orthogonal, and hence they are linearly independent (any orthogonal set is) and form a basis for $C_{f u C} G$, which $a \text{ priori}$ is orthonormal.

(4.1) Characters are class functions and are constant on the conjugacy classes in $G$. The basis theorem implies that the converse is true as well.

Corollary 4.1 Two elements from $G$ are conjugate if and only if every character of $G$ takes the same value on the two.

Proof: Let $g$ and $g'$ be two elements in $G$. The indicator function $\delta_C$ of a conjugacy class $C$ can by the basis theorem (theorem 4.2 above) be expressed as a linear combination of characters, and consequently $\delta_C$ takes the same value at $g$ and $g'$ whenever all the characters do. Hence in that case $g$ and $g'$ belong to the same conjugacy class. The other implication is obvious characters being class functions.

(4.2)—Determining multiplicities. It is customary to introduce an exhaustive list $\chi_1, \ldots, \chi_r$ of mutually non-equal irreducible characters of $G$ (which is unique up to order). The first orthogonality theorem then takes the form

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

where $\delta_{ij}$ is the ubiquitous Kronecker-delta. After Maschke’s theorem any finite $G$-module $V$ can be decomposed as a direct sum

$$V \cong n_1 W_1 \oplus \ldots \oplus n_r W_r$$

where the $W_i$’s are irreducibles, and indexing the $W_i$’s in a manner that $\chi_{W_i} = \chi_i$, we deduce from this decomposition the formula

$$\chi_V = \sum_i n_i \chi_i,$$

which expresses the character of $V$ as a linear combination of irreducible characters with non-negative integral coefficients. The coefficients $n_i$ can be found by the usual technic to determine coordinates relative to an orthonormal basis:

$$(\chi_V, \chi_j) = \sum_i n_i (\chi_i, \chi_j) = \sum_i n_i \delta_{ij} = n_j.$$

We have established the promised formula for multiplicities:

Proposition 4.4 The multiplicity of the irreducible representation $W$ in $V$ equals $(\chi_V, \chi_W)$. 

The isomorphism theorem. One of the important consequences of the basis theorem is that the complex representations of $G$ are determined up to isomorphism by their characters. Formulated in a fancy way, this says that the ring homomorphism $\chi$ sending an element in the $K$-group $K_0(G,\mathbb{C})$ to its character is an isomorphism of rings $K_0(G,\mathbb{C}) \simeq \text{Ch}_Z(G)$. Most aspects of representations are hence caught by their characters, but characters have additional prospects not seen by the representations. Their values, for instance are algebraic integers with—as we shall see—strong “divisibility properties”.

**Corollary 4.2** Two complex representations of $G$ having the same character are isomorphic. The character-map is an isomorphism of rings $K_0(G,\mathbb{C}) \simeq \text{Ch}_Z(G)$.

**Proof**: The multiplicity of any irreducible representation $W$ in a representation $V$ is determined by the character $i_W$; it equals $(\chi_V, \chi_W)$. Whence any irreducible representation occurs with the same multiplicity in two representations with coinciding characters, and the two are isomorphic having identical decompositions into irreducibles.

A natural and sometimes useful consequence of the isomorphism theorem is the following observation

**Proposition 4.5** A representation $V$ of $G$ is isomorphic to a multiple $n\mathbb{C}[G]$ of the regular representation $\mathbb{C}[G]$ if and only if the character $\chi_V$ vanishes on all non-trivial elements of $G$.

**Proof**: By example 4.5 on page 86 the regular character $\chi_{\text{reg}}$ satisfies

$$\chi_{\text{reg}}(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1 \end{cases}$$

so that our hypothesis implies the equality $n\chi_{\text{reg}} = \chi_V$ for $n = (\chi_V, 1_G)$. Hence $V \simeq n\mathbb{C}[G]$.

**Problem 4.6.** Let $W$ be a faithful and irreducible representation of $G$ and assume that the character $\chi_W$ assumes exactly $t$ different values. Show that any irreducible $V$ occurs as summand in $W^{\otimes i}$ for some $i$ with $0 \leq i \leq t - 1$. Hint: Let $\{a_1, \ldots, a_t\}$ be the values that assumes. Consider the class function $\psi = \prod_{1 \leq i \leq t} (\chi_W - a_i) = \sum_{0 \leq i \leq t} b_i \chi^i_W$ and show it is a non-zero multiple of the regular character. Conclude that $(\chi_V, \chi^i_W) \neq 0$ for at least one $i$ in the actual range.

**Two irreducibility criteria.** Among the characters, the irreducible characters are recognized as those of norm one with respect to the hermitian
product. A corresponding and slightly stronger statement applies to virtual characters (recall that a virtual character is a linear combination \( \sum_i n_i \chi_i \) of the irreducible ones with integral coefficients). In addition to being of norm one, they must be of “positive degree”, that is \( \chi(1) \geq 0 \).

**Proposition 4.6** A complex representation \( V \) of \( G \) is irreducible if and only if \( (\chi_V, \chi_V) = 1 \).

**Proof:** If \( V \cong \bigoplus_i n_i W_i \), one has \( (\chi_V, \chi_V) = \sum_i n_i^2 \). The \( n_i \) being non-negative integers, the sum equals one if and only all the \( n_i \)'s vanish except for one which must be equal to one.

**Proposition 4.7** A virtual character \( \chi \) is a character if and only if \( (\chi, \chi_i) \geq 0 \) for all irreducible characters \( \chi_i \). A virtual character \( \chi \) is an irreducible character if and only if \( (\chi, \chi) = 1 \) and \( \chi(1) \geq 0 \).

**Proof:** By definition a virtual character is an integral linear combination of irreducible characters; i.e., \( \chi = \sum_i n_i \chi_i \) with \( n_i \in \mathbb{Z} \). Since \( n_i = (\chi, \chi_i) \) it holds that \( n_i \geq 0 \), so that \( V = \bigoplus_i n_i W_i \) is a representation whose characters equals \( \chi \). In case \( (\chi, \chi) = 1 \), it holds that \( \chi = \pm \chi_i \) for one \( i \) since \( (\chi, \chi) \) is sum of squares of integers. But since \( \chi(1) \geq 0 \), the plus sign must be used, and \( \chi = \chi_i \).

**Direct products**

Let \( G \) and \( H \) be two finite groups. We intend to describe all irreducible representations of the direct product \( G \times H \) in terms of the irreducible representation of the two groups, and the relation turns out to be one that comes first to the mind (the irreducibles are tensor products of one coming from \( G \) and one coming from \( H \)). This will a nice example of the efficiency of the irreducibility criterion 4.6, although it can be done without.

(4.5)—**The external tensor product**. We let \( p_G \) and \( p_H \) denote the two projections from \( G \times H \) onto \( G \) and \( H \) respectively. Representation can be “pulled back” along this, just by composing with the representation map. If for instance, \( V \) is a representation of \( G \) by a representation map \( \rho_V \circ p_G : G \times H \to \text{End}_k(V) \), or in terms of actions, a couple \((g, h)\) acts on \( V \) as \( g \cdot v \). In the same vein, any \( H \)-module \( W \) has a pullback \( p_H^* W \).

We shall follow the common usage and call the tensor product \( p_G^* V \otimes p_H^* W \) for the external tensor product of \( V \) and \( W \), and we shall denote it by \( V \boxtimes W \). Its
underlying vector space is just the ordinary tensor product $V \otimes_k W$ of the two vector spaces, and the action of a pair $(g, h)$ on decomposable tensors is given as $(g, h) \cdot v \otimes w = gv \otimes hw$.

The subgroup $G \times \{1\}$ of $G \times H$—which obviously is isomorphic to $G$—maps to 1 by $p_H$, so when restricted to that subgroup the external tensor product $V \boxtimes W$ becomes isomorphic to the $G$-module $(\dim W) V$, that is, the direct sum of $\dim W$ copies of $V$.

\textbf{(4.6)—MULTIPLICATIVITY OF THE HERMITIAN PRODUCT.} The hermitian product behave as expected when it comes to external tensor products—it is multiplicative:

\begin{lemma}
Let $V$ and $V'$ be two complex representations of $G$ and $W$ and $W'$ two of $H$. Then

$$(\chi_V \boxtimes \chi_W, \chi_{V'} \boxtimes \chi_{W'}) = (\chi_V, \chi_{V'}) (\chi_W, \chi_{W'}).$$

\end{lemma}

\begin{proof}
One has $\chi_{V \boxtimes W}(g, h) = \chi_V(g) \chi_W(h)$ by the multiplicativity of the trace, hence the lemma ensues from the little computation below:

$$(\chi_V \boxtimes \chi_W, \chi_{V'} \boxtimes \chi_{W'}) = |G|^{-1} |H|^{-1} \sum_{g, h} \chi_V(g) \chi_{V'}(g) \chi_W(h) \chi_{W'}(h) =$$

$$= (|G|^{-1} \sum_g \chi_V(g) \chi_{V'}(g)) (|H|^{-1} \sum_h \chi_W(h) \chi_{W'}(h)) = (\chi_V, \chi_{V'}) (\chi_W, \chi_{W'}).$$

\end{proof}

\textbf{(4.7)} Here comes the announced result. We formulate it over the complex numbers, but it holds over big and friendly fields. In more general situations it breaks down, confront the examples given after the proof.

\begin{theorem}
Assume that $V$ and $W$ are irreducible complex representations of $G$ and $H$ respectively. Then the exterior tensor product $V \boxtimes W$ is irreducible and all irreducible $G \times H$-modules are of this form. Moreover, if $V'$ and $W'$ are irreducible representation of $G$ and $H$ as well, then $V \boxtimes W$ and $V' \boxtimes W'$ are isomorphic if and only if $V \simeq V'$ and $W \simeq W'$.

The short way to formulate this theorem is to say that the map from $\text{Irr} \ G \times \text{Irr} \ H$ to $\text{Irr} \ (G \times H)$ sending $(V, W)$ to the external tensor product $V \boxtimes W$ is bijective.

\textbf{Proof:} When combining the criterion 4.6 above with the lemma, we get this for free. Indeed, when $V$ and $W$ are irreducible representations of $G$ and $h$, it holds that $(\chi_V, \chi_V) = (\chi_V, \chi_V) = 1$. The lemma then yields

$$(\chi_V \boxtimes \chi_W, \chi_V \boxtimes \chi_W) = (\chi_V, \chi_V)(\chi_W, \chi_W) = 1.$$
and by the criterion (proposition 4.6) the boxed product $V \boxtimes W$ is irreducible. For the last statement in the proposition, one has by the lemma

$$(\chi_{V\boxtimes W}, \chi_{V'\boxtimes W'}) = (\chi_V, \chi_V')(\chi_W, \chi_W')$$

so if either $V$ and $V'$ or $W$ and $W'$ are not isomorphic, the right side vanishes. Hence the left side does as well, and we infer that $V \boxtimes W$ and $V' \boxtimes W'$ can not be isomorphic.

Denoting by $r$ and $s$ the number irreducible representations of $G$ and $h$ respectively, the external products give rise to exactly $rs$ isomorphism classes of irreducible representations of the product. Knowing that in general (over big and friendly fields) the number of conjugacy classes in a group and the number of irreducible representations of the group coincide, the lemma just below finishes the proof.

Lemma 4.3 Two pairs $(g, h)$ and $(g', h')$ from $G \times H$ are conjugate in $G \times H$ if and only if $g$ and $g'$ are conjugate in $G$ and $h$ and $h'$ are conjugate in $H$. Hence the conjugacy classes are precisely the products $C \times D$ where $C$ runs through the conjugacy classes of $G$ and $D$ those of $H$.

Proof: When $(s, t) \in G \times H$ it holds true that $(s, t)(g, h)(s, t)^{-1} = (sgs^{-1}, tht^{-1})$ from which one deduces the lemma with a minimum of mental effort.

Example 4.6. This examples is to show that theorem 4.3 above is not valid over small fields; the ground field will be the field $\mathbb{Q}$ of rationals.

We start out with the algebra $\mathbb{H}$ of rational quaternions; that is, the algebra $\mathbb{H} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ in which the elements $i, j$ and $k$ are multiplied together in the usual quaternionic way (confront example 3.3 and exercise 3.1 on page 52). One of the involved groups will be the quaternionic group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. It acts on $\mathbb{H}$ by left multiplication, thus making $\mathbb{H}$ an irreducible $\mathbb{Q}$-module.

Is is straightforward to check that the quaternion $q = -(1 + i + j + k)/2$ is order three; i.e., $q^3 = 1$. So the cyclic group $C_3$ acts on $\mathbb{H}$ through multiplication by $q$ from the right. As right multiplication always commutes with left multiplication, this action commutes with the action of $Q$.

Hence the two actions combine to an action of $Q \times C_3$ on $\mathbb{H}$, and this $Q \times C_3$-module we name $W$. The module $W$ is a simple $Q \times C_3$-module, since it is simple considered as $Q$-module (as such, it equals $\mathbb{H}$), and we shall see that it is not isomorphic to an external tensor product. Indeed, if $W$ were, it would have been of the form $W = V \otimes QL$ where $L$ is a one-dimensional representation of $C_3$ over $\mathbb{Q}$ (as $W$ restricts to $Q$ as a simple $Q$-module, the a priori possibility
that dim \( V = \dim L = 2 \) does not materialize), but there is merely one such \( L \), namely the trivial one. Hence \( C_3 \) would have acted trivially on \( W \), which obviously is not the case. 

**Problems**

4.7. Let \( x_1, \ldots, x_r \) be elements in \( G \) one from each of the \( r \) different conjugacy classes. Show that the first orthogonality theorem may be phrased

\[
\sum_k |C_G(x_k)|^{-1} \chi_i(x_k) \chi_j(x_k) = \delta_{ij},
\]

where \( C_G(x) \) denotes the centralizer of \( x \); that is, the subgroup of elements commuting with \( x \). **HINT:** The number of elements in the conjugacy class where \( x \) belongs equals the index \([G : C_G(x)] = |G|/|C_G(x)|^{-1}\) of the centralizer.

4.8. Let \( \chi \) be a complex character of \( G \). Show that if \((\chi, \chi) = 2\) and \( \chi(1) \geq 0 \), then \( \chi \) is either the sum or the difference of two irreducible characters.

4.9. Assume that \( G \) acts transitively on \( X \). Show that \((1_G, \chi_X) = 1\); that is, the trivial representation occurs with multiplicity one in \( L_k(X) \). In general, if \( X_1, \ldots, X_m \) are the orbits of \( G \), show that \( L(X) = \bigoplus_j L_k(X_j) \). Show that \((1_G, \chi_X) = m\).

4.10. Let \( X \) and \( Y \) be two finite sets upon which \( G \) acts. Then \( G \) acts on the product \( X \times Y \) by acting on the “coordinates” the two projections \( p_X \) and \( p_Y \) are then \( G \)-maps. Define a map \( \Theta: L_k(X \times Y) \to \text{Hom}_k(L_k(X), L_k(Y)) \) by the formula \( \Theta(\xi)(\phi) = p_{Y*}(\xi \cdot p_X^*(\phi)) \), or equivalently

\[
\Theta(\xi)(\phi)(y) = \sum_{x \in X} \xi(x, y)\phi(x)
\]

for \( y \in Y \).

a) Show that \( \Theta \) is \( G \)-equivariant.

b) Argue that the spaces \( L(X \times Y) \) and \( \text{Hom}_k(L(X), L(Y)) \) both are of dimension \( |X| \cdot |Y| \).

c) Show that if \( \delta_{x_0} \) is the indicator function of the point \( x_0 \in X \), then \( \Theta(\xi)(\delta_{x_0})(y) = \xi(x_0, y) \). Conclude that \( \Theta \) is an isomorphism.

4.11. (Wieland’s lemma). Let \( G \) be a finite group acting on the finite set \( X \). Let \( L_C(X) = \bigoplus_i n_i V_i \) be the decomposition of \( L_C(X) \) into irreducibles. Show that the number of orbits \( G \) has on \( X \times X \) equals \( \sum_i n_i^2 \).
4.12. Show that $G$ acts double transitively on $X$ if and only if $\chi_X - 1_G$ is an irreducible character.

4.13. We refer to example 4.6 for notation in this exercise. Let $\eta$ be a primitive third root of unity, so that the field $\mathbb{Q}(\eta)$ is a $C_3$-module of dimension two over $\mathbb{Q}$ when we let a generator of $C_3$ act as multiplication by $\eta$. Show that the $\mathbb{Q} \times C_3$-module $H \otimes \mathbb{Q}(\eta)$ decomposes as $W \oplus W$.

* 

4.3  The second orthogonality theorem

We have seen that the irreducible characters form a basis for the space of class functions, but there are of course other interesting basis as well. A very natural one is formed by the indicator functions of the conjugacy classes. If $C$ is a conjugacy class the indicator function $\delta_C$ is given as

$$\delta_C(g) = \begin{cases} 1 & \text{when } g \in C \\ 0 & \text{when } g \notin C. \end{cases}$$

A natural question that arises is what is the transition matrix between the two bases? Obviously it holds true for any character (or class function for that matter) that

$$\chi = \sum_C \chi(C) \delta_C,$$

where the sum is taken over all conjugacy classes, and where we have adopted the convention that $\chi(C)$ denotes the common value of $\chi$ on the elements from $C$.

So what happens the other way around? To examine this, we fix a conjugacy class $C$ in $G$, and consider the development of $\delta_C$ in terms of the irreducible characters. It has the shape

$$\delta_C = \sum_i a_i(C) \chi_i,$$

and as the $\chi_i$’s form an orthonormal basis, the coefficients are given as $a_i(C) = (\delta_C, \chi_i)$. This gives

$$a_i(C) = |G|^{-1} \sum_{g \in G} \delta_C(g) \overline{\chi_i(g)} = |G|^{-1} \sum_{g \in C} \overline{\chi_i(g)} = |C| |G|^{-1} \overline{\chi_i(C)},$$

where $|C|$ denotes the cardinality of $C$ and $\chi_i(C)$ the common value a character $\chi_i$ takes on the members of $C$. When $G$ acts by conjugation on $G$, the isotropy group of an element $g \in G$ equals the centralizer $C_G(g)$—that is the subgroup
of elements commuting with \( g \)—and the orbit of \( g \) is the conjugacy class \( C \) containing \( g \). Hence \(|C| = |G : C_G(g)|\). Introducing this in formula above, we obtain

**Proposition 4.8** If \( \delta_C \) denotes the indicator function of the conjugacy class \( C \) and \( g \) is any element in \( C \), one has

\[
\delta_C = |C_G(g)|^{-1} \sum_i \chi_i(g) \chi_i.
\] (4.2)

(4.1) When evaluated at another group element \( h \), this in turn leads to the following orthogonal theorem—called the second orthogonality theorem—where one sums over the different irreducible characters not over group elements.

**Theorem 4.4 (The second orthogonality theorem)** Let \( g \) and \( h \) be two elements from \( G \). Then

\[
\sum_i \chi_i(g) \chi_i(h) = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugate}, \\ 0 & \text{if } g \text{ and } h \text{ are not conjugate}. \end{cases}
\]  

**Proof:** By the relation (4.2) above one finds letting \( C \) be the conjugacy class of \( g \) that

\[
\delta_C(h) = |C_G(g)|^{-1} \sum_i \chi_i(g) \chi_i(h),
\]

from which the statement follows readily.

Putting \( h = 1 \), one has the special case, where the second formula is well known.

**Corollary 4.3** Let \( n_i = \dim V_i = \chi_i(1) \) be the dimensions of the irreducible representations. Then \( \sum_i n_i^2 = |G| \) and if \( g \neq 1 \) it holds true that

\[
\sum_i n_i \chi_i(g) = 0.
\]

(4.2) It is worth while remarking that the second orthogonality theorem could also have been obtain by considering the \( r \times r \) matrix \( A = (a_{ij}) \) with entries \( a_{ij} = \chi_i(x_j) \sqrt{c_j} \) where the \( x_j \)’s are elements from the \( r \) different conjugacy classes of \( G \) and where \( c_j = |C_G(x_j)| \). The first orthogonality theorem (theorem 4.1 on page 90) is equivalent to \( A \) being a unitary matrix; that is \( AA^* = I \), whence \( A^* A = I \) by a general property of matrices. Making this relation explicit one arrives at the second orthogonality theorem.
Problem 4.14. Let $|C|$ denote the cardinality of a conjugacy class $C$. Show that

$$(\delta_C, \delta_D) = \begin{cases} 0 & \text{when } C, \\ |C| & \text{when } C = D. \end{cases}$$

Hence the class functions $e_C = \sqrt{|C|^{-1}} \delta_C$ when $C$ runs through the different conjugacy classes in $G$ form an orthonormal basis for $\text{Cf}_C G$.

4.4 More orthogonality

There are several interesting functions on $G$ other than the characters. For instance, the entries in the irreducible representation matrices. Let $\rho: G \to \text{Aut}_C(V)$ be an irreducible representation of $G$ of dimension $d$, and choose a basis for $V$. In that basis $\rho$ is represented by an $d \times d$-matrix say $R_V$. Let $r_{ij}$ be the entries of $R$. They are functions on $G$, one has $R(g) = (r_{ij}(g))$. These functions also enjoy an orthogonality relation, in general with respect to the symmetric product on $L_C(G)$.

(4.1) We start out applying the common technic of averaging an arbitrary linear map to get:

**Lemma 4.4** Let $V$ and $W$ be two irreducible representations of $G$ and let $a: V \to W$ be any linear map. Then $E(a) = |G|^{-1} \sum_{g \in G} g | W \circ a \circ g^{-1} |_V$ is $G$-equivariant from $V$ to $W$.

- If $V \not\cong W$ one has $E(a) = 0$,
- if $V = W$ it holds that $E(a) = \lambda \text{id}_V$ with $\lambda = \text{tr}(a)/\text{dim } V$.

**Proof:** We already know that $E(a)$ is $G$-equivariant. If $V$ and $W$ are not isomorphic $E(a)$ vanishes by Schur’s lemma, and in case $V = W$ Schur’s lemma tells us that $E(a)$ is a homothety by some $\lambda$. Taking traces yields

$$\lambda \dim V = \text{tr}(E)(a) = |G|^{-1} \sum_{g} \text{tr}((g) \circ a \circ g^{-1}) = \text{tr}(a).$$

(4.2)---Matrices. Now, we choose a basis for each irreducible module $V \in \text{Irr } G$, and consider the corresponding matrices of all the maps involved. That is $(a_{ij})$ is the matrix of $a$, $(E_{ij})$ of $E(a)$ and the representation maps of the $V$’s have the matrices $(r_{ij}^V)$.

Expressing the equalities in the lemma in terms of matrices we arrive (after a trivial and boring calculation of matrix products) at the following

$$E_{ij} = \sum_{g} \sum_{k,l} r_{jk}^W (g)a_{kl}r_{lj}^V (g^{-1}) = \begin{cases} 0 & \text{when } V \not\cong W \\ \delta_{ij} |G| \text{tr}(a)/\text{dim } V & \text{when } V = W. \end{cases}$$
This holds true for all matrices \((a_{ij})\), so we may chose \((a_{ij})\) to be elementary; that is, a matrix with only one non-zero entry, and that entry equals one. This gives
\[
< r^W_{ik}, r^V_{lj} > = 0
\]
when \(V \not\cong W\). In case \(V = W\) we observe that \(\text{tr}(a) = 0\) unless the sole one is situated on the diagonal, hence
\[
< r^V_{ij}, r^V_{kl} > = \delta_{ij}\delta_{kl}/ \dim V.
\]

**Theorem 4.5** Let entries \(r^V_{ij}\) of matrices of the representation maps of the different \(V\) from \(\text{Irr} G\) form an orthogonal basis with respect to the symmetric product for the space \(L_C(G)\) of complex functions on \(G\).

**Proof:** What is left to prove is that the number of entries equals the dimension of \(L_C(G)\). But for each irreducible \(V\), there are \((\dim V)^2\) entries, and we know e.g., by Wedderburn that \(\sum_{V \in \text{Irr} G} (\dim V)^2 = |G|\). 

**(4.3)—Unitary representations.** Recall that complex \(d \times d\)-matrix is said to be **unitary** if \(RR^* = I\) where \(R^*\) is the conjugate transposed of \(R\). Another way of phrasing this is that the columns of \(R\) are orthonormal (in the standard hermitian product on \(C^d\)). If \(V\) is a complex vector space endowed with a hermitian product \((v, w)\), an operator \(A: V \to V\) is unitary if it conserves the hermitian product; that is, \((Av, Aw) = (v, w)\) for all vectors \(v\) and \(w\). This is the case if and only if the matrix of \(A\) in any orthonormal basis is unitary. The unitary operators form a group \(U(V)\) called the unitary group.

Now, let \(V\) be a complex representation on \(V\) with representation map \(\rho: G \to \text{Aut}_C(V)\), and assume that \(V\) is equipped with a hermitian product \((v, w)\). There is a corresponding unitary subgroup \(U(V)\) of \(\text{Aut}_C(V)\). The representation is said to be **unitary** if \(\rho\) takes values in the unitary group \(U(V)\). Equivalently, the hermitian product is invariant under \(G\); that is, \((g v, g w) = (v, w)\) for all group elements \(g\) and all vectors \(v\) and \(w\). Or another phrasing differently, for any orthonormal basis of \(V\) the matrices of \(\rho(g)\) are all unitary.

**Proposition 4.9** Let \(V\) be a complex representation of \(G\). Then there is a hermitian product on \(V\) that is invariant under \(G\); in other words, all complex representations are unitary.

**Proof:** The proof is a by now standard averaging process. Let \((v, w)\) be any hermitian product on \(V\) and define \((v, w)_G\) by
\[
(v, w)_G = \sum_{g \in G} (g \cdot v, g \cdot w).
\]
The product \((v, w)_G\) is obviously sesquilinear, and conjugate symmetric. As \(gh\) runs through \(G\) when \(g\) does, one has
\[
(h \cdot v, h \cdot w)_G = \sum_{g \in G} (gh \cdot v, gh \cdot w) = (v, w)_G
\]
so that the new product is \(G\)-invariant. It remains to be seen that it is positive definite, but
\[
(v, v)_G = \sum_{g \in G} (g \cdot v, g \cdot v) > 0
\]
unless \(gv = 0\) for all \(g\) and this happens only when \(v = 0\).

4.5 Values of characters

A character \(\chi\) of the group \(G\) assumes not only in the complex field \(\mathbb{C}\), but in the subring \(A\) of algebraic integers. This has several serious and strong implications, and one might be tented to say this one flavour added to the theory. (4.1) The trace of any endomorphism equals the sum of its eigenvalues. In particular if \(V\) is a complex representation of \(G\), the value \(\chi_V(g)\) is the sum of the eigenvalues of the endomorphism \(g|_V\):
\[
\chi_V(g) = \lambda_1 + \ldots + \lambda_d
\]
where \(d = \dim_C V\). Belonging to a finite group, the group element \(g\) is of finite order, and therefore all the eigenvalues \(\lambda_i\) are roots of unity. Consequently \(\chi_V(g)\) is an algebraic integers as any root of unity is. This yields:

**Proposition 4.10** The values of any character \(\chi\) are algebraic integers.

(4.2)—Cyclotomic relations. Recall that the exponent of the group \(G\) is the least common multiple of the orders of its elements. In general the exponent differs from the order of \(G\), but it will always be a divisor in |\(G|\|. If a group element \(g\) satisfies \(g^l = 1\) and \(\lambda\) is an eigenvalue of \(g|_V\), clearly \(\lambda^l = 1\). Hence values of characters of \(G\) will be sums of \(m\)-th roots of unity, and we can make the previous proposition more precise:

**Proposition 4.11** Let \(m\) be the exponent of the finite group \(G\). Then the values of the characters belong to the cyclotomic field \(Q(m)\).

The cyclotomic field \(Q(m)\) is the smallest field containing all the \(m\)-th roots of unity \(\mu_m\). The Galois groups \(\text{Gal}(Q(m)/Q)\) acts on the roots of unity by rising to powers; that is \(\sigma \in \text{Gal}(Q(m)/Q)\) there is an \(l\) with \(\sigma(\eta) = \eta^l\) for all \(\eta \in \mu_m\). This is no more mysterious than the fact that \(\mu_m\) being cyclic, any
Lemma 4.5 Let \( V \) be a representation of a group \( G \) with exponent \( m \). For any element \( g \in G \) and any \( \sigma \in \text{Gal}(\mathbb{Q}(m)/\mathbb{Q}) \) it holds true that
\[
\sigma(\chi_V(g)) = \chi_V(g^l).
\]

PROOF: The value \( \chi_V(g) \) is the sum
\[
\chi_V(g) = \lambda_1 + \ldots + \lambda_r
\]
of the eigenvalues \( \lambda_i \) of \( g|_V \) and they are \( m \)-th roots of unity, \( m \) being the exponent of \( G \). Hence \( \sigma_i(\lambda_i) = \lambda_i^l \), and we arrive at
\[
\sigma_i(\chi_V(g)) = \sigma_i(\lambda_1) + \ldots + \sigma_i(\lambda_r) = \lambda_1^l + \ldots + \lambda_r^l = \chi_V(g^l).
\]

Problem 4.15. Let \( A = (a_{ij}) \) be an invertible square matrix whose rows are indexed by a set \( I \) and the columns by a set \( J \). Assume that the group \( G \) acts on both \( I \) and \( J \) (independently) such that \( a_{gi}g_j = a_{ij} \) for all \( i \in I, j \in J \) and \( g \in G \). Then \( G \) has as many fixed points in \( I \) as in \( J \). HINT: Let \( C_I \) (resp. \( C_J \)) be the permutation matrix of the action on \( I \) (resp. \( J \)). Show that \( C_I A = A C_J \), conclude that \( \text{tr}(C_I) = \text{tr}(C_J) \).

Problem 4.16. Show that a group \( G \) has as many characters with real values as there are conjugacy classes with \( C = C^{-1} \).

(4.3)—An Illustration. To illustrate the usefulness of this description of the cyclotomic Galois action, let us show that \( \sum_{g \in G} \chi_V(g) \) is an integer. It hinges on the fact that when \( l \) is invertible mod the exponent \( m \) of \( g \), the power map \( G \to G \) given as \( g \mapsto g^l \) is bijective. Indeed, if \( ll' \equiv 1 \mod m \) one has \( g = (g^{l'})^l \) so that the power map is surjective. Therefore it is bijective, \( G \) being finite.

From this it follows that
\[
\sigma_i(\sum_{g \in G} \chi_V(g)) = \sum_{g \in G} \chi_V(g^l) = \sum_{g \in G} \chi_V(g)
\]
since \( g^l \) runs through \( G \) when \( g \) does. Consequently the sum \( \sum_{g \in G} \chi_V(g) \) is invariant under the Galois group \( \text{Gal}(\mathbb{Q}(m)/\mathbb{Q}) \) and is a rational number. However, \( \text{a priori} \) it is an algebraic integer, hence it is a rational integer.
(4.4)—Som e useful congruences. Let $\mathbb{A}_m$ be the ring of integers in $\mathbb{Q}(m)$; that is, $\mathbb{A}_m = \mathbb{A} \cap \mathbb{Q}(m)$. It is a finite algebra over $\mathbb{Z}$. One has

**Proposition 4.12** Let $V$ be a representation of $G$, and let $p$ be a prime. Then for all $g \in G$ it holds true that

$$\chi_V(g^p) \equiv \chi_V(g)^p \pmod{p\mathbb{A}_m}.$$  

If $\chi_V(g) \in \mathbb{Z}$ on even has

$$\chi_V(g^p) \equiv \chi_V(g) \pmod{p}.$$  

**Proof:** Computing in the algebra $\mathbb{A}_m/p\mathbb{A}_m$ which is a commutative algebra in characteristic $p$, one finds

$$\chi_V(g)^p = (\lambda_1 + \ldots + \lambda_r)^p \equiv \lambda_1^p + \ldots + \lambda_r^p = \chi_V(g^p).$$  

The second statement follows from the first in view of Fermat’s little theorem.

Action of the huge Galois group Gal($\mathbb{C}/\mathbb{Q}$)

Let $\sigma$ be any automorphism of $\mathbb{C}$ over $\mathbb{Q}$; that is, an element in the Galois group Gal($\mathbb{C}/\mathbb{Q}$). It acts on the set of complex functions on $G$ by the rule $a^\sigma(g) = \sigma(a(g))$, and obviously it sends class functions to class functions. In fact, it also sends characters to characters. Indeed, let $\rho : G \to \text{Aut}_\mathbb{C}(V)$ be a representation of $G$ and choose a basis for $V$. In that basis each $\rho(g)$ is represented by a matrix $R(g) = (r_{ij})$. We let $R^\sigma(g) = \sigma(R(g)) = (\sigma(r_{ij}))$. As $\sigma$ is an algebra homomorphism, $\sigma(R(g)R(h)) = \sigma(R(g))\sigma(R(h))$, so we have constructed a new representation $V^\sigma$ of $G$. Clearly $\text{tr}(R^\sigma(g)) = \sigma(\text{tr}(R(g)))$, and the character of the new representation equals $\chi^\sigma$. The following lemma shows that $G(\mathbb{C}/\mathbb{Q})$ acts on the set Irr $G$.

**Lemma 4.6** If $\chi_V$ is irreducibl, then $\chi_V^\sigma$ is as well.

**Proof:** One finds

$$(\chi^\sigma, \chi^\sigma) = |G|^{-1} \sum_g \sigma(\chi(g))\sigma(\chi(g^{-1})) = |G|^{-1} \sum_g \sigma(\chi(g)\chi(g^{-1})) = \sigma(\chi, \chi) = 1.$$  

(4.5)—Another illustration. Again, we give an illustration of the usefulness of the Galois action, or in fact, we shall give two. First let us show that $\sum_{V \in \text{Irr} G} \chi(g)$ is an integer. Indeed, as $V^\sigma$ runs through $\text{Irr} G$ when $V$ does, the
sum is invariant under the Galois group $\mathbb{C}/\mathbb{Q}$). Hence it is a rational number, and consequently an integer, since it lies in $\mathbb{A}$.

Secondly, we prove a multiplicative version. Let $V_1, \ldots, V_s$ be the orbit of $\text{Gal}(\mathbb{C}/\mathbb{Q})$ in $\text{Irr} G$ containing $V$, and let $V_1 = V$. Then the product $\prod_i \chi_{V_i}(g)$ is an integer for all $g \in G$. The argument is *mutatis mutandis* the same, the product is invariant under the Galois action, hence lies in $\mathbb{Q}$, and it is an algebraic integer being the product of such.

**Proposition 4.13** Let $V$ be an irreducible representation of $G$ and assume that $\dim V \geq 2$. Then $\chi_V(g)$ vanishes for some $g \in G$.

**Proof:** One has $|G| = \sum_{g \in G} |\chi_V(g)|^2$.

---

**The kernel of a character**

Being the sum of roots of unity is a very special property of algebraic integers, and there is the potential to squeeze a lot more out of the expression 4.3. By a simple application the triangle inequality, one obtains the following easy but important lemma.

**Lemma 4.7** Assume that $V$ is complex representation of the finite group $G$ and let $g \in G$. Then $|\chi_V(g)| \leq \chi(1)$ and equality holds if and only if $g|_V$ is a homothety; that is, one has $g|_V = \lambda \text{id}_V$ for a root of unity $\lambda$.

**Proof:** The inequality is a direct consequence of (4.3) and the triangle inequality, and the second statement follows from the subsequent elementary lemma. From that lemma we infer that all the eigenvalues of $\chi_V(g)$ are equal, hence being semi-simple, $\chi_V(g)$ is a homothety.

---

**Lemma 4.8** Let $z_1, \ldots, z_d$ be $d$ points on the unit circle. Assume that $|z_1 + \ldots + z_d| = d$. Then all the $z_i$ are equal.

**Proof:** Let $\eta = (z_1 + \ldots + z_d)d^{-1}$. Replacing each $z_i$ by $z_i \eta^{-1}$ we may well assume that $z_1 + \ldots + z_d = d$. Let $\phi_i$ be the argument of $z_i$. The real parts of the $z_i$’s being $\cos \phi_i$ we obtain the relation

$$d = \sum_{1 \leq i \leq d} \cos \phi_i.$$ 

Since $|\cos x| \leq 1$, and since there are $d$ terms in the sum, we infer that $\cos \phi_i = 1$ for each $i$; that is $\phi_i = 0$ and hence $z_i = 1$ for every $i$. 

---
(4.6)—The kernel of a character. An important observation is that the collection of elements $g$ such that $\chi_V(g) = \chi_V(1)$ coincides with the kernel of the representation map $\rho_V$; that is

$$\{ g \mid \chi_V(g) = \chi_V(1) \} = \ker \rho_V.$$ 

Indeed, if $g|_V = \text{id}_V$ it holds true that $\chi_V(g) = \text{tr}(g|_V) = \dim V = \chi_V(1)$, and this takes care of one of the inclusions. The other one follows since lemma 4.7 above tells us that $g|_V = \lambda \text{id}_V$ in case $\chi_V(g) = \dim V$, and we may deduce that $\dim V = \text{tr}(g)|_V = \lambda \dim V$. Hence $\lambda = 1$. This observation motivates the name kernel of $\chi_V$ for the collection of group elements $g$ with $\chi_V(g) = \chi_V(1)$.

It is a normal subgroup of $G$. To sum up, we have shown:

**Proposition 4.14** Given a character $\chi$ of the finite group $G$. The kernel of $\chi$, that is, the set $\{ g \mid \chi_V(g) = \chi_V(1) \}$ is a normal subgroup of $G$.

This is a key tool when applying character theory to the study groups; it provides a means to produce non-trivial normal subgroups. In two instances we shall see this tool in action; the proofs of Burnside’s $p^aq^b$ theorem and the theorem about Frobenius groups both rely heavily on it.

**Problem 4.17.** Show that $\{ g \in G \mid |\chi_V(g)| = \chi_V(1) \}$ is a normal subgroup. 

HINT: Use lemma 4.7 to see that the set closed under multiplication.

---

**Weighted averages**

The averaging operator $E$ that we introduced in 3.1 on page 64, can be generalized in a natural way by giving each summand a weight. That is, if $a$ is a function on $G$ with values in $k$, we define the weighted average operator $E_a$ to be the element in the group algebra $k[G]$ given by the formula

$$E_a = \sum_{g \in G} a(g^{-1}) \cdot g.$$ 

Amid the results one may use these operators to prove, we mention two: The basis theorem—the characters form a basis for the class functions—and the division theorem—the dimension of any irreducible $G$-module divides the order $|G|$ of $G$.

(4.7) We now specialize to the case when the weight function $a$ is a class function. The averaging operator $E_a$ then becomes , a central element in the group algebra $k[G]$: 

---
Lemma 4.9 Let $k$ be any field. Assume that $a$ is a class function, then the averaging operator $E_a$ is a central element in $k[G]$.

Proof: The following little calculation shows this:

$$E_a \cdot h = \sum_{g \in G} a(g^{-1})g h = \sum_{s \in G} a(hs^{-1})s = \sum_{s \in G} a(s^{-1}h)s = \sum_{g \in G} a(g^{-1})hg = h \cdot E_a.$$ 

The second equality above comes from the substitution $s = gh$, the third holds because $a$ is assumed to be a class function, and in the forth we have performed the substitution $s = hg$. 

As a consequence, when $a$ is a class function, all the operators $E_a|_V$ that $E_a$ induces on $G$-modules $V$, are $G$-equivariant.

Example 4.7. Already in chapter 3 we met some of this averaging operators. If $C$ is a conjugacy class the set $C^{-1}$ consisting of all inverse elements $g^{-1}$ of the elements $g \in G$ is another conjugacy class (it can happen they are equal).

Letting $a$ be the indicator function of a conjugacy class $C^{-1}$, one finds $E_a = \sum_{g \in C} \delta_{C^{-1}}(g^{-1})g = \sum_{g \in C} g$. These are nothing but the elements $s_C$ that appeared in lemma 3.6 on page 70 as a basis for the centre of the group ring.

(4.8) When $W$ is an irreducible $G$-module—and $a$ still being a class function—the operator $E_a|_W$ will because of Schur’s lemma be a homothety. Letting $\lambda$ be the scalar such that $E_a|_W = \lambda \text{id}_W$ we find

$$\lambda \text{id}_W = \sum_{g \in G} a(g^{-1})g|_W.$$ 

Taking traces we arrive at the formula

$$\lambda \dim_k W = \sum_{g} a(g^{-1})\chi_W(g) = \sum_{g \in G} \chi_W(g)\chi_W(g) = |G| \cdot (a, \chi_W),$$

where in the middle equality $g$ has been replaced by $g^{-1}$ and where the equality $\chi_W(g^{-1}) = \overline{\chi_W(g)}$ is used. This establishes the lemma.

Lemma 4.10 Let $a$ be a class function on $G$ and let $W$ be an irreducible $G$-module. Suppose that the averaging operator $E_a$ acts on $W$ as multiplication by the scalar $\lambda$. Then the following formula holds true

$$\lambda \dim_C W = |G| \cdot (a, \chi_W).$$
Divisibility

Our second application of the averaging operators is a divisibility result that goes back to Frobenius in 1896 (Über die Primfaktoren der Gruppendeterminante, Sitzungsber. Akad. Berlin (1896) 1343-1382), and which says that the dimension \( \dim_k W \) of every irreducible \( G \)-module \( W \) is a factor of the order \( |G| \). We follow Eltinghof and call it the “Frobenius divisibility theorem”.

This theorem can be substantially strengthened; in fact, the dimension \( \dim_k W \) divides the index \([A : G]\) of any normal abelian subgroup \( A \) of \( G \), but we postpone that result to a later occasion. Now we content ourselves with showing that \( \dim_k W \) divides the index of centre of \( G \).

(4.9) Our ground field \( k \) is in this chapter assumed to algebraically closed and of characteristic zero. Therefore \( k \) contains the field \( \mathbb{Q} \) of algebraic numbers (or more precisely a copy of \( \mathbb{Q} \)). Inside \( \mathbb{Q} \) we find the ring \( \mathbb{A} \) of algebraic integers. This is the subring whose elements satisfy relations shaped like

\[
x^r + \sum_{i < r} a_i x^i = 0, \tag{4.5}
\]

where the coefficients \( a_i \) are confined to \( \mathbb{Z} \). The ring \( \mathbb{A} \) is integrally closed in \( k \); that is, any element in \( k \) satisfying a relation like (4.5) but with coefficients \( a_i \) allowed to lie in \( \mathbb{A} \), must lie in \( \mathbb{A} \).

(4.10) Let \( e \) be an endomorphism of the vector space \( V \) over \( k \) and assume that \( e \) satisfies an equation \( P(e) = 0 \), where \( P(t) \) is a monic polynomial whose coefficients lie in some subring \( R \) of \( k \). Any eigenvalue of \( e \) must satisfies the same equation; indeed, since if \( v \) is an eigenvector so that \( e \cdot v = \lambda v \), one has \( e^i \cdot v = \lambda^i v \) for all natural numbers \( i \). Whence \( P(e) \cdot v = P(\lambda)v \). By assumption \( P(e) = 0 \), and as \( v \) is non-zero being an eigenvector, we may conclude that \( P(\lambda) = 0 \). This leads to

**Lemma 4.11**: Let \( V \) be a \( G \)-module and let \( e \in \mathbb{A}[G] \). Any eigenvalue of \( e|_V \) is an algebraic integer.

**Proof**: The element \( e \) is of the form \( e = \sum g a_g g \) with \( a_g \)'s all lying in \( \mathbb{A} \), as they are finite in number, hence the element \( e \) belongs to \( \mathbb{A}'[G] \) for some subring \( \mathbb{A}' \) of \( \mathbb{A} \) which is finite over \( \mathbb{Z} \). The algebra \( \mathbb{A}'[G] \) is a noetherian \( \mathbb{A}' \)-module. Hence the ascending chain \( M_l = \langle 1, e, e^2, \ldots, e^l \rangle \) of submodules stabilizes, and there is a relation \( e^r = \sum_{i < r} \alpha_i e^i \) with the coefficients \( \alpha_i \) being algebraic integers. The observation above shows that the eigenvalues of \( e \) satisfy the same relation, and therefore they are integral over \( \mathbb{A} \), but \( \mathbb{A} \) is integrally closed, so they are algebraic integers. \( \square \)
Corollary 4.4 (The divisibility theorem) For any complex irreducible representation $W$ of $G$, an any class function $a$ on $G$ whose values are algebraic integer, the number

$$\lambda = \frac{|G| (a, \chi_W)}{\dim W}$$

is an algebraic integer.

**Proof:** By lemma 4.11 above, $\lambda$ is the eigenvalue of the averaging operator $E_a$ operating on $W$ and $E_a = \sum_{g \in G} a(g^{-1}) g$ lies in $\mathbb{A}[G]$ since by hypothesis all the $a(g^{-1})$ lie there. \qed

**Problems**

4.18. Show that $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. 

4.19. Show that a complex number is an algebraic integer if and only if it is the eigenvalue of a matrix with integral coefficients. **Hint:** One implication is clear, for the other use the so called companion matrix of polynomial.

4.20. Show that if $a$ and $b$ are eigenvalues of the $n \times n$-matrix $A$ and the $m \times m$-matrix $B$ respectively, then $ab$ and $a + b$ are eigenvalues of respectively $A \otimes B$ and $A \otimes I_m + I_n \otimes B$. Conclude that the set of algebraic integers $\mathbb{A}$ is closed under addition and multiplication.

4.21. Show that if $a$ belongs to a subring $R$ of $\mathbb{C}$ that is finitely generated over $\mathbb{Z}$, then $a$ is an algebraic integer. **Hint:** The ring $R$ is a finitely generated abelian group and the ascending chain of subgroups $\langle 1, a, a^2, \ldots, a^i \rangle$ must be stationary.

4.22. Show that $\mathbb{A}$ is integrally closed; that is, if $a$ is integral over $\mathbb{A}$, it is contained in $\mathbb{A}$. 

(4.11)—**Frobenius divisibility.**

**Theorem 4.6** For any irreducible $G$-module $W$, the dimension $\dim_k W$ divides the order $|G|$ of the group $G$. 

---

*Footnotes and references are not included in the natural text.*
Proof: Since $(\chi_W, \chi_W) = 1$ lemma 4.10 on page 106 with $a$ equal to $\chi_W$ gives that the averaging operator acts on $W$ as a homothety with

$$\lambda = \frac{|G|}{\dim_k W},$$

which obviously is a rational number.

The eigenvalues of the endomorphisms $g|_W$ are all roots of unity, and being sums of such, all values $\chi_W(g)$ are algebraic integers. It follows that the averaging operator $E_{\chi_W}$ belongs to in $A[G]$, and by lemma 4.11 the number $\lambda$ is an algebraic integer. A well known fact from elementary number theory tells us that an algebraic integer which is rational, is an integer, and we can conclude that $\lambda$ is an integer.

Theorem 4.7 For any irreducible $G$-module $W$, the dimension $\dim_k W$ divides the index $[G : Z]$ of the the centre $Z$ of $G$.

Proof: Let $W$ be an irreducible $G$-module and let $m$ be a natural number. Have in mind that the centre $Z$ acts on $W$ through multiplication by scalars, say by the multiplicative character $\psi$.

We know that the $G^m$-module $W^G_m = W \boxtimes \cdots \boxtimes W$ is irreducible (theorem 4.3 on page 94). Let $H \subseteq Z^m$ be the kernel of the multiplication map $Z^m \to Z$, which is a group homomorphism as $Z$ is abelian. That is, $H$ is the subgroup consisting of the $m$-tuples $(x_1, \ldots, x_m)$ such that $x_1 \cdot \ldots \cdot x_m = 1$, and one easily verifies that $H \simeq Z^{m-1}$.

Since the centre $Z$ acts on $W$ through multiplication by the scalar character $\psi$, an element $(x_1, \ldots, x_m) \in Z^m$ acts on $W^G_m$ through multiplication by $\psi(x_1) \cdot \ldots \cdot \psi(x_m) = \psi(x_1 \cdot \ldots \cdot x_m)$. Consequently $H$ acts trivially on $W^G_m$, and $W^G_m$ is an irreducible $G^m/H$-module. Now, $|G^m/H| = |G : Z|^{m-1}G$, and $\dim_k W^G_m = (\dim_k W)^m$. It follows that $(\dim_k W)^m$ divides $[G : Z]^{m-1}$ and the conclusion follows (if $p$ is a prime with $p^a$ the power of $p$ occurring in $\dim W$ and $p^b$ the one occurring in $[G : Z]$, one has $ma \leq (m-1)b + c$ for a constat $c$. Hence $a \leq b$.)

(4.12)—Central characters. Another important divisibility property comes by applying lemma to the indicator function $\delta_C$ of a conjugacy class. Obviously it takes values in $A$ (the values are either 0 or 1). The hermitian product of $\delta_C$ against an irreducible character $\chi_W$ is

$$|G| (\chi_W, \delta_C) = \sum_{g \in G} \chi_W(g) \delta_C(g) = \sum_{g \in C} \chi_W(g) = |C| \chi_W(g),$$

where $|C|$ denotes the number of elements in $C$, and in the rigimost expression $g$ is any element in the conjugacy class $C$. Feeding this into corollary 4.4 above yields without further effort the following.
Proposition 4.15 Let \( C \) be one of the conjugacy classes of \( G \) and let \( W \) be a complex representation of \( G \). Let \( g \in C \) be any element. Then the number

\[
\frac{|C| \chi_W(g)}{\dim W}
\]

is an algebraic integer.

In the litterature one frequently meets this number in sloighty guise. Writing \( h_C \) for the number og elements in \( C \) and remembering that \( \dim W = \chi_W(1) \), the number in the corollary assumes the shape

\[
\frac{h_C \chi_W(g)}{\chi_W(1)}.
\]

Problem 4.23. Let \( \rho: G \to \text{End}_C(W) \) be the representation map of an irreducible complex representation \( W \) of \( G \). Let \( \alpha \in C[G] \) be a central element. Show that \( \rho(\alpha): W \to W \) is \( G \)-equivariant and conclude by Schur’s lemma that \( \rho(\alpha) \) is a homothety, say by the scalar \( \omega_W(\alpha) \). Show that \( \omega_W \) is a multiplicative function on the centre of \( C[G] \). Show that value \( \omega_W \) assumes on the class sum \( s_C \) is given as \( \omega_W(s_C) = |C| \chi(g) / \dim W \) where \( g \) is any element in \( C \).

4.6 Character tables

The character table of a group is a table whose columns are indexed by the conjugacy classes and the rows by the irreducible characters. There is common way of naming the conjugacy classes (defined in the computer program GAP), the names being composed of a number and a letter. The number indicates the order of the elements in the class and the letter is a running indexing of the classes with elements of the given order (this limits the number to 27 which is more than sufficient for us).

For example the group \( S_3 \) has three conjugacy classes \( \{1\} \), \( \{(1,2),(1,3),(2,3)\} \), \( \{(1,2,3),(1,3,2)\} \), whose names are 1a, 2a and 3a. There are three irreducible characters, the trivial one \( \chi_{1S_3} \), the alternating one \( \chi_a \), and the one of dimension two we met on page 76 and there baptized \( U_2 \). We shall denote its character by \( \chi_2 \). Recall that the representation \( U_2 \) has a basis of the form \( e_1 - e_3, e_2 - e_3 \) with \( S_3 \) permuting the \( e_i \)’s.

So the table looks like

<table>
<thead>
<tr>
<th></th>
<th>1a</th>
<th>2a</th>
<th>3a</th>
</tr>
</thead>
<tbody>
<tr>
<td>1S_3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>\chi_a</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>\chi_2</td>
<td>2</td>
<td>0</td>
<td>-1</td>
</tr>
</tbody>
</table>
The trivial character assumes the value 1 on all classes, and the alternating one is the sign of the permutations in the class, one for even permutations and −1 for odd. This takes care of the first two rows. The second orthogonality theorem says that the columns are orthogonal, and knowing the two first, one easily determines the last row. Alternatively, we perfectly know the representation \( U_2 \) and can calculate the character by counting fixed points.

Of course there is a certain arbitrariness in the order of the rows and the columns, but the uppermost row will always be the trivial character so there will only be 1’s there, and the first column will always correspond to the trivial conjugacy class \( \{1\} \). That column will contain the degrees of the irreducible characters i.e., the dimensions of the corresponding representations.

**Problem 4.24.** Refering to the characters of \( S_3 \), show that \( \chi_2^3 = \chi_2 + \chi_n + 1 \). Show that \( \chi_n^{n+1} = \chi_n^n + 2\chi_n^{n-1} \) and finde a closed formula for \( \chi_2^n \).

*The Klein four group*

This is the group \( K = C_2 \times C_2 \) with commuting generators \( \sigma \) and \( \rho \) both being of order two. All its irreducible representations are one dimensional and there are four of them up to isomorphism. The four characters assume all different combinations of \( \pm 1 \) on the two generators, so that the character table looks like

<table>
<thead>
<tr>
<th></th>
<th>1a</th>
<th>2a</th>
<th>2b</th>
<th>2c</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1_K )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_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>
</tr>
<tr>
<td>( \chi_3 )</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
</tr>
</tbody>
</table>

where \( 2a = \{\sigma\} \), \( 2b = \{\sigma \rho\} \) and \( 2c = \{\rho\} \).

*Groups of order eight*

The aim of this paragraph is, in addition to elucidate aspects of character tables, to give an example that non-isomorphic groups can have identical character tables (up to permutation of rows and columns). This happens for the two non-abelian groups of order eight, the dihedral group \( D_4 \) and the quaternion group \( Q_8 \). We shall find their common character table.

So groups in general are not determined by their character table—because of the arbitrariness of the ordering of rows and columns, two tables must be considered to be the same if they coincide after a permutation of the rows and the columns. This is a frequent phenomenon among 2-groups; for instance there are 14 non-isomorphic groups of order 16 and 11 different character
tables, and if one goes up to order 256 there will be 56092 groups, but only 9501 different tables. Hence many groups share character tables. However, in the opposite corner of the group universe things are different. Simple groups are determined by their character table. If the irreducible representations of a finite group $H$ has the same dimensions as the irreducible representations of the simple group $G$ (counted with multiplicities; that is, $H$ has as many irreducible representations of a given dimension as $G$), then $G$ and $H$ are isomorphic. (4.1) Of course, it is not coincidental that $D_4$ and $Q_8$ have the same character table, the two groups are close cousins! Both sit in the middle of an exact sequence shaped like

$$1 \longrightarrow C_2 \longrightarrow G \overset{\pi}{\longrightarrow} C_2 \times C_2 \longrightarrow 1$$

(4.6)

where $C_2$ is the centre of $G$. In technical terms, they are central extensions of $C_2 \times C_2$ by $C_2$. The difference is that for $D_4$ the sequence has a section; that is, $D_4$ has subgroups isomorphic to $C_2 \times C_2$, whereas $Q_8$ has no such groups (all non-central elements are of order four). And in fact, sitting in the sequence (4.6) a group has its character table determined, irrespectively of there being a section or not.

(4.2)—The dihedral group $D_4$. We begin with the dihedral group $D_4$ (we did a detailed study of $D_n$ in 3.6.1 on page 79). Recall that $D_4$ has generators are $r$ and $s$ with the relations $r^4 = s^2 = 1$ and $srs = r^{-1}$, and its conjugacy classes are the following with names with GAP-style names: $1a = \{1\}$, $2a = \{r^2\}$, $2b = \{s, rs\}$, $2c = \{rs, r^{-1}s\}$, $4a = \{r, r^{-1}\}$.

Now, any representation $L$ of $C_2 \times C_2$ pulls back to a representation $\pi^* L$ of the dihedral group, and the character are related by $\chi_{\pi^* L}(x) = \chi_L(\pi(x))$. As $\pi(s) = \sigma$, $\pi(r) = \rho$ and $\pi(rs) = \rho \sigma$ we obtain immediately the upper part of the character table below by just inserting the character table of the Klein group appropriately placed (coloured blue), and the bottom row then is found by successively applying the second orthogonality theorem to the first and the four other columns.

<table>
<thead>
<tr>
<th></th>
<th>$1a$</th>
<th>$2a$</th>
<th>$2b$</th>
<th>$2c$</th>
<th>$4a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1_{D_4}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<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>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>2</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
The quaternion group $Q_8$. Recall that $Q_8$ has two generators $r$ and $s$ subjected to the relations $r^2 = s^2$ and $r^4 = s^4 = 1$ and $sr^{-1} = r^{-1}$. One readily checks that the elements of $Q_8$ are $\{1, r^2, r, r^{-1}, s, s^{-1}, sr, rs\}$, with $r^{-1} = r^3$, $s^{-1} = s^3$ and $(sr)^{-1} = rs$.

The element $r^2$ is central, and $Q_8$ fits in as the middle term of the exact sequence (4.6). However in this there is no section, as all elements except the generator $r^2$ of the centre and the unit element are of order four.

The map $\pi$ is defined by $\pi(s) = \sigma$ and $\pi(r) = \rho$, and then $\pi(rs) = \sigma \rho$ and $\pi(r^2) = 1$. The five conjugacy classes are $1 = \{1\}$, $2a = \{r^2\}$, $4a = \{s, s^{-1}\}$, $4b = \{sr, rs\}$ and $4c = \{r, r^{-1}\}$.

Proceeding exactly as in the case of $D_4$ we arrive at the character table. The two tables are not only equal, they originate from the same source, namely the extension (4.6).

$$
\begin{array}{c|ccccc}
\text{1}_{Q_8} & 1a & 2a & 4a & 4b & 4c \\
\chi_1 & 1 & 1 & 1 & 1 & 1 \\
\chi_2 & 1 & 1 & -1 & -1 & 1 \\
\chi_3 & 1 & -1 & 1 & 1 & 1 \\
\chi_4 & 2 & -2 & 0 & 0 & 0 \\
\end{array}
$$

About normal subgroups. It is noteworthy that one can read off all the normal subgroups of a group $G$ from the character table of $G$. One can even find all inclusions among the normal subgroups, and the full character tables of the quotients of $G$ modulo by the different normal subgroups. However, the isomorphism type of the subgroups are out of reach. The point is the proposition 4.14 on page 105 which describes the kernel of a representation as the elements $g$ with $\chi(g) = \chi(1)$, and obviously, this can be read off from the table, at least for the irreducible ones. The kernel of the others are accounted for by the following:

Lemma 4.12 Every normal subgroup of $G$ is the intersection of kernels of irreducible representations of $G$

Proof: If $V = \bigoplus W_i$ it holds true that $\ker \rho_W = \bigcap_i \ker \rho_{W_i}$, hence it suffices to observe that if $N \subseteq G$ is normal, the kernel of the regular representation $k[G/N]$ equals $N$.

For instance, consider the quaternion group $Q_8$. The character $\chi_1$ has as kernel the conjugacy class $4a$ (union with $\{1\}$, of course), $\chi_2$ the class $4b$ union $\{1\}$, the character $\chi_3$ the class $4c$ union $\{1\}$. These are the kernels of the irreducible ones, the character $\chi_4$ is faithful.

The sum $\chi_i + \chi_j$ of two of the $\chi_i$'s with $i < j < 4$ has the class $2a$ union $\{1\}$
as kernel, as the sum $\chi_1 + \chi_2 + \chi_3$ has. Hence there are four non-trivial normal subgroups, forming a lattice like:

(4.5)—A useful lemma about the exterior square. The tensor square $V \otimes V$ of a representation $V$ decomposes as

$$V \otimes V = \bigwedge^2 V \oplus \text{Sym}^2(V)$$

and it is of interest to determine the corresponding decomposition of the characters involved:

**Lemma 4.13** Let $G$ be a group and $V$ a representation of $G$. For the character of the second alternating power $\bigwedge^2 V$ it holds true that

$$\chi_{\bigwedge^2 V}(g) = ((\chi_V(g))^2 - \chi_V(g^2))/2.$$  

for any element $g \in G$.

**Proof:** Let $\lambda_1, \ldots, \lambda_d$ be the eigenvalues of $g|_V$ and let $v_1, \ldots, v_d$ be the corresponding eigenvectors. The eigenvectors of $g$ acting in $\bigwedge^2 V$ are the vectors $v_i \wedge v_j$ with $i \neq j$ and corresponding eigenvalues equal to $\lambda_i \lambda_j$. It follows that

$$\chi_{\bigwedge^2 V}(g) = \sum_{i<j} \lambda_i \lambda_j = ((\lambda_1 + \ldots + \lambda_d)^2 - (\lambda_1^2 + \ldots + \lambda_d^2))/2 = ((\chi_V(g))^2 - \chi_V(g^2))/2.$$ 

Since the charater of the square $V \otimes V$ is the square $\chi_V(g)^2$, the lemma immediately yields a formula for the character of the symmetric power:

$$\chi_{\text{Sym}^2(V)}(g) = ((\chi_V(g))^2 + \chi_V(g^2))/2.$$ 

(4.6)—The symmetric group $S_5$. As the size of the group grows the character table becomes gradually more challenging to establish. And one has only to kneel in the dust for the mathematicians Bernd Fischer and Donald Livingstone that computed (with the aid of a computer) the character table of the monster group. The order of the monster is

$$808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000$$

and it has 194 conjugacy classes. The smallest non-trivial representation is of dimension 196883 (the highest dimension of an irreducible representation is 258823477531055064045234375).

We shall not push our computations very far, but as is customary in courses like ours, we include $S_5$ as an example (later on we shall study representations
of the symmetric groups systematically). The group $A_5$ is as well interesting being the first simple non-abelian group one meets (and being related to equations of the fifth degree).

The conjugacy classes of $S_5$ are with their GAP-names the following: $1a = \{1\}, 2a = \{(a,b)\}, 2b = \{(a,b)(c,d)\}, 3a = \{a,b,c\}, 4a = \{(a,b,c,d)\}, 5a = \{(a,b,c,d,e)\}$ and $6a = \{(a,b,c)(d,e)\}.$

So let us come to the representations. First of all there is the 4-dimensional representation $U_4$ that we met in the paragraph 3.6 on page 76. Its character $\chi_4$ is given as $\psi - 1$ where $\psi$ is the character of the constituting permutation representation on $X_5 = \{1, 2, 3, 4, 5\}.$ And one easily checks that $\chi_4$ and $\chi'_4 = \chi_4 \chi_4$ are irreducible.

The next character of $S_5$ to consider is the alternating product $\Lambda_2 U_4.$ Its dimension equals six, and we denote its character by $\chi_6.$ Generally if $V$ is any representation, the character of the alternating power $\Lambda_2 V$ is given by the formula

$$\chi_{\Lambda_2 V}(g) = (\chi(V(g))^2 - \chi(V(g^2)))/2.$$ 

The computation of $\chi_6$ is summarized in the small table below, where we also have indicated in which conjugacy classes the squares from the different conjugacy classes lie.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>30</th>
<th>24</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2a</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>2b</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3a</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>4a</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>5a</td>
<td>16</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>6a</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Again, one sees that $(\chi_6(\chi_6) = 1,$ so that $\chi_6$ is irreducible.

We have up to now laid hands on five irreducibles, and there being seven conjugacy classes, we are still missing two. The squares of the dimensions so far found add up to 50, and it is easy to see that the only solution for the remaining two is that both are of dimension 5. The character table of $S_5$ starts to
emerge from the darkness, and below we have drawn it with letters in the unknown slots. Some relations between the unknowns which follow immediately from the orthogonality of the columns, are incorporated.

<table>
<thead>
<tr>
<th>1</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>30</th>
<th>24</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>1S₅</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>₂χ₅</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>₄χ₅</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>₄χ₄</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>₅χ₅</td>
<td>5</td>
<td>x</td>
<td>y</td>
<td>z</td>
<td>w</td>
<td>u</td>
</tr>
<tr>
<td>₅χ₅'</td>
<td>5</td>
<td>-x</td>
<td>y'</td>
<td>z'</td>
<td>-w</td>
<td>u'</td>
</tr>
<tr>
<td>₆χ₆</td>
<td>6</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>₆χ₆'</td>
<td>6</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Now, by the second orthogonality theorem, the square sum of the second column equals the order of the centralizer of any element \( g \) in \( 2a \), which is given as \( |C_{S₅}(g)| = 12 \). This gives \( x = \pm 1 \), and we can assume \( x = 1 \). Since the character \( ₄χ₅ \) is irreducible, it either equals \( χ₅ \) or \( χ₅' \) (they are the only two of dimension five), but since \( x = 1 \), it must equal \( χ₅' \). It follows that \( y' = y \), \( z' = z \) and \( u' = u \), and the actual values are trivially computed by the second orthogonality relation. The complete table is as follows:

<table>
<thead>
<tr>
<th>1</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>30</th>
<th>24</th>
<th>20</th>
</tr>
</thead>
<tbody>
<tr>
<td>1S₅</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>₂χ₅</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>₄χ₅</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>₄χ₄</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>₅χ₅</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>₅χ₅'</td>
<td>5</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>₆χ₆</td>
<td>6</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>₆χ₆'</td>
<td>6</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

(4.7)—The Alternating Group \( A₅ \).

(4.8)—The Alternating Group \( A₅ \). When searching for the conjugacy class of \( A₅ \) we meet a phenomenon called fusion. Elements that are not conjugate in \( A₅ \) becomes conjugate in \( S₅ \), and their conjugacy classes fuse into one class in \( S₅ \). Or seen from the view point of \( S₅ \), one of its conjugacy classes is contained in \( A₅ \) but there it splits into to different classes. In \( A₅ \) this happens for the conjugacy class \( 5a \) of \( S₅ \). To cope with this situation, we resort to the following almost trivial lemma:

**Lemma 4.14.** Let \( H \) be a subgroup in \( G \) and \( x \) and \( y \) be two elements in \( H \). Assume

\( It is a matter of giving names which of the characters χ₅ and χ₅' assumes the value 1 on 2a.
that they are conjugate in \( g \), that is \( y = gxg^{-1} \) for \( g \in G \). Then \( x \) and \( y \) are conjugate in \( h \) if and only if \( g = ha \) with \( a \in C_G(x) \) and \( h \in H \).

**Proof:** Assume that \( g = ha \) like in the lemma. Then \( y = gxg^{-1} = hx(a^{-1}h)^{-1} = hxh^{-1} \) since \( a \) commutes with \( x \). For the other implication, if \( y = hxh^{-1} \) with \( h \in H \), we find \( hxh^{-1} = gxg^{-1} \) and consequently \( x = h^{-1}gxg^{-1}h \). One deduces that \( a = h^{-1}g \) centralizes \( x \).

In the present case of \( G = S_n \) and \( H = A_n \), a factorization \( g = ha \) with \( g \) odd and \( h \) even implies of course that \( a \) is odd. So we can replace a conjugacy relation \( y = gxg^{-1} \) with \( g \) odd by \( y = hxh^{-1} \) with \( h \) even if and only if there are odd elements in the centralizer \( C_{S_n}(x) \).

The centralizer \( C_{S_n}(\sigma) \) of a five cycle \( \sigma = (1,2,3,4,5) \) is just the cyclic group the cycle generates \( < \sigma > \). There are 4! different 5-cycles. Hence the centralizer is of order 5, and \( \sigma \) is obviously centralized by \( < \sigma > \).

Since the centralizer \( < \sigma > \) is entirely contained in \( A_5 \) it has no odd element, and the conjugacy class of \( \sigma \) in \( S_5 \) splits up into two conjugacy classes in \( A_5 \), one formed by the 5-cycles conjugate to \( \sigma \) by odd elements, and one consisting of those conjugate to \( \sigma \) by even elements. There are 12 elements in each.

The powers \( \sigma^2 \) and \( \sigma^3 \) lie in the former and \( \sigma \) and \( \sigma^{-1} \) belongs to the latter. Indeed, \( \sigma^{-1} = (5,4,3,2,1) \) is conjugate to \( \sigma = (1,2,3,4,5) \) by \((1,5)(2,4)\) and \( \sigma^2 = (1,3,5,2,4) \) by the 4-cycle \( g = (2,3,5,4) \) as is readily verified.

The conjugacy classes are \( 1a = \{1\}, 2a = \{(a,b)(c,d)\}, 3a = \{(a,b,c)\} \) and the two 5a and 5b containing 5-cycles.

The natural tactics for finding irreducible representations of \( A_5 \) is to restrict irreducibles from \( S_5 \) and “hope for the best”; i.e., if the restriction persists being irreducible we are happy, if not we try decomposing it. The four different and non-trivial restrictions are listed in the table below:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>15</th>
<th>20</th>
<th>12</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2a</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>3a</td>
<td>5</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5a</td>
<td>6</td>
<td>-2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>5b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An easy calculation shows that \( (\chi_4, \chi_4) = (\chi_5, \chi_5) = 1 \), so those two are irreducible, but \( (\chi_6, \chi_6) = 2 \). Since there is merely one way of writing 2 as a sum of squares, we conclude that \( \chi_6 = \chi_3 + \chi_3' \) with \( \chi_3 \) and \( \chi_3' \) irreducible. Moreover, trivially one finds \( (\chi_4, \chi_6) = (\chi_4, \chi_6) = 0 \), so neither \( \chi_3 \) nor \( \chi_3' \) equals \( \chi_4 \) or \( \chi_5 \). Hence \( \chi_3 \) and \( \chi_3' \) are the two missing children. The sum of the squares of the three known dimensions is 42, and the only way to 18 write 18 as a sum of squares is as 9 + 9 and we can conclude that \( \chi_3(1) = \chi_3'(1) = 3 \). Filling in the table wit unknowns yields...
Te second orthogonality relation gives as the centralizer $C(2b) = 4$, that $|x| = |x'| = 1$, and hence $x = x' = -1$ since the two first columns are orthogonal.

And again, te second orthogonal gives $y = y' = 0$. hence

Now, from the square sums along the two last columns being equal to 5 (the order of the centralizer of a five-cycle) we deduce that both $z$ and $w$ satisfy the equation $5 = 1 + 1 + x^2 + (1 - x)^2$, which has the solutions $(1 \pm \sqrt{5})/2$, and the table can be completed:

<table>
<thead>
<tr>
<th>1</th>
<th>15</th>
<th>20</th>
<th>12</th>
<th>12</th>
<th>1a</th>
<th>2a</th>
<th>3a</th>
<th>5a</th>
<th>5b</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\chi^5$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\chi_4$</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$\chi_5$</td>
<td>5</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>$\chi_3$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>$z$</td>
<td>$w$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>$1-z$</td>
</tr>
<tr>
<td>$\chi_3'$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>$(1 + \sqrt{5})/2$</td>
<td>$(1 - \sqrt{5})/2$</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>$(1 - \sqrt{5})/2$</td>
</tr>
</tbody>
</table>

**Problem 4.25.** Describe the restriction of $\chi_3$ to the cyclic group $<\sigma>$. Show that $\cos 2\pi/5 = (\sqrt{5} - 1)/4$.

**Problem 4.26.** Let $G$ be a group and let $V$ be a faithful representation of $G$ of dimension $d$. Let $g \in G$ be an element and assume that $g|V$ has $d$ distinct eigenvalues. Show that the centralizer $C_G(g)$ is abelian. **Hint:** An $x \in C_G(g)$ share eigenvectors with $g$.

(4.9)—REAL AND NON-REAL REPRESENTATIONS. Given an irreducible representation $V$ of $G$ whose characters are all real valued, like $A_5$ for example. It is natural question whether $V$ has a real incarnation; that is, if there is a representation $V_0$ of $G$ over the reals $\mathbb{R}$ such that $V \cong C\otimes_{\mathbb{R}} V_0$. In general this is not
true, but there is a nice criterion, that builds on an analysis of the symmetric power of $V$ and the following criterion.

**Lemma 4.15** Let $V$ be an irreducible complex representation of the group $G$. Then $V$ is a real representation if and only if there is a non-degenerate invariant symmetric bilinear form on $V$.

**Proof:** When $V$ is real, say $V \cong \mathbb{C} \otimes_{\mathbb{R}} V_0$ a construction like the one in $\text{xxx}$ produces a positive definite $G$-invariant form on $V_0$ whose extension to $V$ will be symmetric, non-degenerate and $G$-invariant.

For the other implication, let $B(v, w)$ be symmetric and non-degenerate. Let $(v, w)$ be a hermitian $G$-invariant form on $V$ (exists after $\text{xxx}$). As any linear functional on $V$ is of the form $v \mapsto (v, w)$ for some uniquely defined vector $w$, there is unique map $\theta : V \to V$ such that $B(v, w) = (v, \theta(w))$ for all $v$ and $w$. By uniqueness it is clear that $\theta$ is additive, and it anti-linear by the little computation

$$(v, \theta(aw)) = B(v, aw) = aB(v, w) = a(v, \theta(w)) = (v, a\theta(w)).$$

Uniqueness yields that $\theta$ is equivariant as well:

$$(v, \theta(gw)) = B(v, gw) = B(g^{-1}v, w) = (g^{-1}v, \theta(w)) = (v, g\theta(w))$$

and as this holds for all $v$ it follows that $\theta(gw) = g\theta(w)$.

For the other implication, let $B(v, w)$ be symmetric and non-degenerate. Let $(v, w)$ be a hermitian $G$-invariant form on $V$ (exists after $\text{xxx}$). As any linear functional on $V$ is of the form $v \mapsto (v, w)$ for some uniquely defined vector $w$, there is unique map $\theta : V \to V$ such that $B(v, w) = (v, \theta(w))$ for all $v$ and $w$. By uniqueness it is clear that $\theta$ is additive, and it anti-linear by the little computation

$$(v, \theta(aw)) = B(v, aw) = aB(v, w) = a(v, \theta(w)) = (v, a\theta(w)).$$

Uniqueness yields that $\theta$ is equivariant as well:

$$(v, \theta(gw)) = B(v, gw) = B(g^{-1}v, w) = (g^{-1}v, \theta(w)) = (v, g\theta(w))$$

and as this holds for all $v$ it follows that $\theta(gw) = g\theta(w)$.

Next, he square $\theta \circ \theta$ is a $G$-linear and $G$-equivariant automorphism of $V$, and as $V$ is irreducible by hypothesis, it ensues from Schur’s lemma that $\theta^2 = \lambda \text{id}_V$ for some some complex constant $\lambda$. And $\lambda$ must be real because applying $\theta$ to the identity $\theta(\theta(v)) = \lambda v$ yields $\lambda \theta(v) = \theta(\lambda v)$ from which one infers that $\lambda = \bar{\lambda}$ since $\theta$ is anti-linear. Thus rescaling the quadratic form $B$ by $\lambda$, one may assume that $\theta^2 = \text{id}_V$, and $\theta$ is what one calls a real structure on $V$.
The subset $V_0 = \{ v \in V \mid \theta(v) = v \}$ of $V$ is real and $G$-invariant vector subspace and $V = V_0 \oplus iV_0$ which is isomorphic to $C \otimes_R V_0$. Indeed, one has

$$v = (v + \theta(v))/2 - i(iv + \theta(iv))/2$$

and obviously it holds true that $V_0 \cap iV_0 = 0$.

As we observed already that a necessary condition that $V$ be defined over the reals is of course that all the values assumed by the character $\chi_V$ be real. Since the contragredient representation $V^*$ and $V$ has complex conjugate characters; that is, $\chi_{V^*} = \bar{\chi}_V$, this is equivalent to $V^*$ being isomorphic to $V$. Hence $V \otimes V \simeq V^* \otimes V = \text{Hom}_k(V, V)$. When $V$ is irreducible,

First of all, if as usual $V^*$ denotes the contragredient of $V$ it holds true that $\chi_{V^*} = \bar{\chi}_V$, so that the character $\chi_V$ of $V$ only assumes real values if and only if $V$ is isomorphic to its contragredient; that is $V \simeq V^*$. One has $\text{Hom}_k(V^*, V) \simeq V \otimes V$, and a test for whether $V \simeq V^*$ or not would be whether $V \otimes V$ has a non-trivial invariant element or not; that is whether the hermitian product $(\chi^2_V, 1_G)$ vanishes or not. By Schur’s lemma, $(\chi^2_V, 1_G)$ can merely assume the values 1 or 0.

When this is the case it holds true that

$$(\chi_V, \chi_{V^*}) = |G|^{-1} \sum_g \chi_V(g) \bar{\chi}_V(g)$$

(4.10)—The linear group $\text{PSL}(2,7)$. As a precursor to a more general treatment of the special linear groups $\text{SL}(2, q)$ with $q$ a prime power and their relatives the projective special linear groups $\text{PSL}(2, q)$ (which we hopefully will have time to do) we shall determine the character table of the group $\text{PSL}(2,7)$.

This group is famous for several things. It is the next smallest simple group (only $A_5$ has fewer elements) and it is the smallest so called Hurewitz-group, which are automorphism groups of Riemann-surfaces of maximal order. This maximal order depends on the genus of the surface, and for $g = 3$ it equals 168. The Riemann-surface having $\text{PSL}(2,7)$ as symmetry group is as famous as the group. It was intensively studied by Felix Klein and consequently has become named after him. It is called the Klein-quartic and has homogenous equation

$$x^3y + y^3z + z^3x = 0.$$
which are not in the subspace generated by the first column, and there are 
$q^2 - q$ such vectors. This shows that the order of $\text{Gl}(2, q)$ equals 
$(q^2 - 1)(q^2 - q) = (q - 1)^2 q(q + 1)$. Imposing the constraint that the determinant be one, 
reduced the order by a factor $(q - 1)$ hence to $(q - 1)q(q + 1)$.

If the characteristic polynomial of an element $g$ from $\text{Sl}(2, 7)$ has two dis-
tinct roots, $g$ is conjugate in $\text{Gl}(2, 7)$ to a diagonal matrix; that is, there is a 
relation $\alpha d \alpha^{-1} = g$ with $d$ diagonal but with $\alpha \in \text{Gl}(2, 7)$. Obviously one can 
find a diagonal matrix $\beta$ with the same determinant as $\alpha$, and being diagonal 
the matrix $\beta = \begin{pmatrix} \det \alpha & 0 \\ 0 & 1 \end{pmatrix}$ will do 
and there four of these classes; two correspond to $\lambda = \pm 1$, and two to the 
pairs $\{\lambda, \lambda^{-1}\} = \{2, -3\}$ and $\{\lambda, \lambda^{-1}\} = \{3, -2\}$. However, in $\text{PSL}(2, 7)$ these 
four classes coalesce to merely two classes; one is the image of the classes with 
$\lambda = \pm 1$, and another arises from the two other pairs.

Assume next that the polynomial is irreducible. It is shaped like $t^2 + bt + 1$, 
and being irreducible means that $b^2 - 4$ is not a square in $\mathbb{F}_7$. As the non-
squares in $\mathbb{F}_7$ are $\{-1, -2, 3\}$, this occurs when $b^2 \in \{3, 2, 0\}$, that is $b^2 = 0$ or 
$b^2 = 2$.

If $b = 0$, $g$ is conjugate to 
$\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
in $\text{Gl}(2, 7)$. The matrix $\sigma$ is centralized by 
$\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$
and as all elements in $\mathbb{F}_7$ are sum of two squares, $g$ is conjugate to $\sigma$ in $\text{Sl}(2, 7)$.

The centre of $\text{Sl}(2, 7)$ consists of the subgroup of scalar matrices of determinant one; that is, the matrices $a \cdot I$ with $a^2 = 1$, and the projective special group 
$\text{PSL}(2, 7)$ is the quotient $\text{Sl}(2, 7)/\{ \pm I \}$. Its order equals $168 = 2^3 \cdot 3 \cdot 7$.

The group of units in $\mathbb{F}_7$ is cyclic of order 6, the squares being $1, 2, 4$ forming 
a subgroup of order three.

The group acts on the set $\mathbb{P}^1(\mathbb{F}_7)$ of lines in the two dimensional vector 
space $\mathbb{F}_7^2$; there are eight such, hence $\text{PSL}(2, 7) \subseteq S_8$. The action is transitive and 
the isotropy group of the point $(1, 0)$ is given as 
$\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix}$.
This group is of order 21 has a cyclic, normal subgroup of order seven:

Indeed,

\[
\begin{pmatrix}
a & b \\
c & d \\
\end{pmatrix}
\begin{pmatrix}
1 \\
0 \\
\end{pmatrix}
= 
\begin{pmatrix}
a \\
c \\
\end{pmatrix}
\]

So \(c = 0\). The is

4.7 Burnside’s \(p^aq^b\)-theorem

The theorem of this paragraph is one of the two early brilliant gems of representation theory—the other one being Frobenius’s result about so called “Frobenius groups”. Up to the invention of representation theory, all results about finite groups were based on Sylow’s three theorems combined with more or less virtuous counting technics, and Frobenius’ invention of representation theory was a fresh impetus into the theory. There was a lot of bad blood between the two giants of group theory of those days, but each obtained a great theorem that will stand for ever, so in some sense it was a draw (at least in that game).

Burnside’s \(p^aq^b\) theorem says that a finite group whose order involves only two primes (i.e., is of the form \(p^aq^b\) with \(p\) and \(q\) primes) is solvable. The theorem dates from 1904 but as it frequently occurs, many special cases were known before.

This theorem of Burnside’s is the first result in a long row that eventually lead to the Feit-Thomson’s result of ultrasonic fame, The Odd order theorem, stating that any group of odd order is solvable (which in fact was first conjecture by Burnside), and the Odd order theorem is the bedrock of the classification theorem of the finite simple groups.

Recap of solvable groups

To the benefit of those student following the course that are fluent in the language of group theory, we give a super-quick-fast-food version of what a solvable groups is. A finite group \(G\) is solvable if it possesses a strictly descending chain \(\{G_i\}\) of subgroups such that \(G_{i+1}\) is normal in \(G_i\) and the quotients \(G_i/G_{i+1}\) all being abelian. They owes their naming to Galois theory; an equation can be solved by radicals precisely when its Galois group is solvable. If \(H\) is a normal subgroup of \(G\) and both \(H\) and \(G/H\) are solvable, then \(G\) is solvable. One just splices the appropriate descending chains in the two to obtain one in \(G\).
Every \( p \)-group is solvable, since the centre \( Z(G) \) of any \( p \)-group (that is, a group of order a prime power \( p^n \)) is non-trivial and normal (centres are always normal). This is a consequence of the so-called “class equation”. A conjugacy class of an element in \( G \) reduces to singleton if only if the element is central. Hence

\[
|G| = |Z(G)| + \sum x |G| / |C_G(x)|
\]

where the sum to the right extends over an exhaustive list of representatives of the non-trivial conjugacy classes of \( G \). Since all terms in the equation other \( |Z(G)| \) has \( p \) as a factor, \( |Z(G)| \) must be divisible by \( p \) as well; in particular it cannot be one.

The theorem

So we have come to the theorem.

**Theorem 4.8 (Burnside’s \( p^a q^b \)-theorem)** Assume that \( G \) is a finite group with \( |G| = p^a q^b \) where \( p \) and \( q \) are prime numbers. Then \( G \) is solvable.

The proof boils down to finding a non-trivial, proper subgroup of such a \( G \).

Indeed, if \( N \) is one, the orders \( |G/N| \) and \( |N| \) are both of the shape \( p^d q^d' \) (of course with smaller exponents than the ones for \( G \)) and so by induction on the order they are both solvable. Whence \( G \) is solvable. The centre \( Z(G) \) of \( G \) being a normal abelian subgroup, a similar induction argument allows us to assume that \( Z(G) = \{1\} \).

Now, let \( S \) be a Sylow \( p \) subgroup of \( G \). As is true for all \( p \)-groups, it has a non-trivial centre \( Z(S) \), so let \( z \in Z(S) \) be different from 1. This means that all elements in \( S \) commute with \( z \). Hence the centralizer \( C_G(z) \) contains the entire \( S \), and its order therefore has \( p^a \) as factor. Consequently the conjugacy class \( C \) where \( z \) lies, has a cardinality of the form \( q^c \) (for some \( c \geq 1 \)); indeed, it holds that \( |C| = |G| / |C_G(z)| \). And \( C \) is non-trivial since \( z \) is not central in \( G \), the centre of \( G \) being trivial by assumption.

This reduces the proof to the following:

**Theorem 4.9 (Burnside)** Assume that \( G \) is a finite group with a non-trivial conjugacy class of prime power cardinality. Then \( G \) has a non-trivial, proper normal subgroup.

**Proof:** Let \( C \) be the conjugacy class with prime power order; that is, \( |C| = q^b \) for \( q \) a prime with \( b > 0 \).

The brilliant trick of Burnside’s is to exhibit a non-trivial irreducible representation \( \rho : G \to \text{Aut}_c(V) \) such that \( \rho(x) \) is a homothety for all \( x \in C \). If \( \rho \) is faithful, it follows that \( x \) is central which is not the case since the conjugacy
The character $\chi$ of the wanted representation will be one such that $\chi(x) \neq 0$ for $x \in \mathbb{C}$ and $\chi(1) \neq 0 \mod q$. To establish the existence of an animal like that, we resort to the second orthogonality theorem (Theorem 4.4 on page 98). As usual we let $\chi_1, \ldots, \chi_r$ be the irreducible characters of $G$ listed in any order, but with $\chi_1 = 1_G$. The second orthogonality relation when applied to the elements 1 and $x$ then assumes the form

$$0 = \sum_i \chi_i(1)\chi_i(x) = 1 + \sum_{i>1} \chi_i(1)\chi_i(x).$$

Because of the 1 not all the terms in the rightmost sum (with $i > 0$) can be congruent zero mod $q$, and we can choose $\chi$ to be one of the characters with $\chi(1)\chi(x) \neq 0 \mod q$. This entails that $\chi(x) \neq 0$ and $\chi(1) \neq 0 \mod q$.

By 4.15 the number $\omega = |C| \chi(x) / \chi(1)$ lies in $\mathbb{A}$, and since $|C| = q^b$ and $q$ does not divide $\chi(1)$, Lemma 4.16 below implies that $\chi(x) / \chi(1)$ is an algebraic integer as well. By Lemma 4.7 on page 104 one has $|\chi(x) / \chi(1)| \leq 1$, and the scoop is that by Lemma 4.17 below, all the eigenvalues of $x$ are equal. Hence $x|_V$ is a homothety. But now if the kernel $\ker \chi$ were trivial, $\rho_V$ would map $G$ injectively into $\text{Aut}_\mathbb{C}(V)$ and as the homotheties are central in $\text{Aut}_\mathbb{C}(V)$ it would follow that $x$ were central. But it is not and hence the kernel is non-trivial.

The two lemmas

Here comes the two lemmas as indicated above. The first is really straightforward of the just-follow-you-nose type, but the second requires some knowledge of the norm of algebraic integers that we provide in a telegraphic style. (to the benefit of students not conversant with this).

**Lemma 4.16** Let $a$ be an algebraic integer and let $b$ and $c$ be two relatively prime integers. If $ab/c$ is an algebraic integer, then $a/c$ is one as well.

**Proof:** Since $b$ and $c$ are relatively prime, one may write $1 = sb + tc$ with $s, t \in \mathbb{Z}$. Then $a/c = s(ab/c) + ta$, and as both $ab/c$ and $a$ are algebraic integers by hypothesis, the same holds for $a/c$. 

(4.1)—**Recap of the norm of algebraic numbers.** Let $a$ be an algebraic number. The set of polynomials in $\mathbb{Q}[t]$ having $a$ as a root constitute an ideal which by definition of $a$ being algebraic is non-zero. As the polynomial ring $\mathbb{Q}[t]$ is a PID, this ideal has a unique monic generator. That generator is the minimal
polynomial $P(t)$ of $a$. It is irreducible and can be characterised as the monic polynomial in $\mathbb{Q}[t]$ of least degree having $a$ as a root.

The polynomial $P(t)$ splits completely over $\mathbb{C}$. One has a factorization

$$P(t) = \prod_i (t - \alpha_i),$$

where the $\alpha_i$’s are different complex numbers, and one of them, say $\alpha_1$, equals $a$. The $\alpha_i$’s are called the algebraic conjugates of $a$.

Being the constant term of $P(t)$ up to sign the product of the $\alpha_i$’s is a rational number. This product is called the norm of $a$ and denoted by $N(a)$. The norm of an algebraic integer $a$, being an algebraic integer means that the minimal polynomial $P(t)$ has integral coefficients. In particular, the norm $N(a)$ will in that case be an integer.

The smallest subfield $K$ of $\mathbb{C}$ containing the roots $\alpha_i$’s is named the root field of $P$. It is a Galois extension of $\mathbb{Q}$, with Galois group written as $\text{Gal}(K/\mathbb{Q})$.

An important point is that $\text{Gal}(K/\mathbb{Q})$ acts transitively on the roots of $P(t)$. This is a consequence of $P(t)$ being irreducible over $\mathbb{Q}$. Indeed, if a proper subset $\{\beta_i\}$ of $\{\alpha_i\}$ constituted an orbit, the polynomial $Q(t) = \prod_j (t - \beta_j)$—which obviously is a factor of $P(t)$—would be invariant under the Galois group, and its coefficients would be rational numbers, contradicting the fact that $P(t)$ is irreducible over $\mathbb{Q}$.

Our modest need in this context is the following

**Lemma 4.17** Let $a = \sum_{1 \leq i \leq d} \eta_i/d$ where the $\eta_i$-s are roots of unity and $d$ is an integer. Assume that $a$ is an algebraic integer. Then $a = d\eta$ for an appropriate root of unity $\eta$ (that is, all the $\eta_i$’s are equal).

**Proof:** Let $K$ be the root field of the minimal polynomial of $a$. Assume that $|a| < 1$. If $\sigma$ is an automorphism of $K$ over $\mathbb{Q}$ and $\eta \in K$ is a root of unity, say it satisfies $\eta^n = 1$, it obviously holds true that $\sigma(\eta)^n = 1$. Since the Galois group $\text{Gal}(K/\mathbb{Q})$ acts transitively on the algebraic conjugate $\alpha_i$’s of $a$, any $\alpha_i$ is of the same form as $a$; that is, $d\alpha_i$ is the sum of $d$ roots of unity, and hence $|\alpha_i| \leq 1$. It ensues that $|N(a)| = \prod_i |N(\alpha_i)| < 1$ which is absurd because $N(a)$ is a non-zero integer $a$ being an algebraic integer. Hence $|a| = 1$, and by lemma 4.8 on page 104 we conclude that all the $\eta_i$’s are all equal. \(\Box\)

**Problem 4.27.** Let $a$ be an algebraic number and let $L = \mathbb{Q}(a)$. The map $m_a : L \rightarrow L$ sending $x$ to $ax$ is $\mathbb{Q}$-linear and has a characteristic polynomial $P(t)$. 

...
Show that \( P(t) \) is the minimal polynomial of \( a \). Conclude that \( N(a) = \det m_a \) and that the norm is multiplicative; that is, \( N(ab) = N(a)N(b) \).

### 4.8 Appendix: Recap about traces

This section is devoted to a short and dirty recap about traces. So \( k \) will be any field and \( V \) a vector space of finite dimension over \( k \).

Recall that if \( \sigma \) is an endomorphism of \( V \) one has the **determinant** of \( \sigma \). It is defined as the determinant of the matrix representing \( \sigma \) in any basis, and of course, it is independent of the basis, since the determinant of conjugate matrices coincide; indeed, \( \det ABA^{-1} = \det A \det B (\det A)^{-1} = \det B \). In fact there is a slightly stronger statement. If \( \phi: V \to W \) is any isomorphism, it holds true that \( \det \phi \circ \sigma \circ \phi^{-1} = \det \sigma \).

The **characteristic polynomial** of \( \sigma \) is defined as \( \det(t \cdot \text{id}_V - \sigma) \). It is a monic polynomial of degree equal to the dimension of \( V \). It vanishes at \( \lambda \) if and only if \( \lambda \text{id}_V - \sigma \) is not invertible; that is, if and only if there exists a vector \( v \) with \( \sigma(v) = \lambda v \); i.e., \( v \) is an eigenvector with eigenvalue \( \lambda \).

Two conjugate endomorphisms \( \sigma \) and \( \tau \sigma \tau^{-1} \) have the same characteristic polynomial, hence the coefficients are class functions; they the same value on conjugate endomorphism. Two of the coefficients are of special importance. The constant term which up to sign equals the determinant of \( \sigma \) and the subleading term, whose negative is called the trace of \( \sigma \). One has

\[
P_{\sigma}(t) = t^n - \text{tr}(\sigma)t^{n-1} + \ldots + (-1)^n \det \sigma.
\]

Extending the field \( k \) if necessary, one may factor the characteristic poly as

\[
P_{\sigma}(t) = \prod_i (t - \lambda_i)
\]

where the \( \lambda_i \)'s are the eigenvalues of \( \sigma \). If \( k \) is algebraically closed (e.g., equal to \( \mathbb{C} \)), this factorization takes place in \( k \), but in general one has to pass to the root field \( K \). Anyhow, the trace is the sum the eigenvalues. In \( K \) one has the identity

\[
\text{tr}(\sigma) = \lambda_1 + \ldots + \lambda_n
\]

(*4.1*) **Multiplicative along exact sequences.** The characteristic polynomial behaves very well with respect to invariant subspaces, it is “multiplicative along exact sequences”. Spelled out this statement, that many might find cryptic, means the following. Assume \( W \subseteq V \) is an subspace invariant under
the endomorphism $\sigma$ of $V$. Then $\sigma$ “passes to the quotient” and induces an endomorphism of the quotient $V/W$ (sending a coset $v + W$ to $\sigma(v) + W$), as display in the commutative diagram

$$
\begin{array}{cccc}
0 & \rightarrow & W & \rightarrow & V & \rightarrow & V/W & \rightarrow & 0 \\
\sigma_W & & \sigma & & \sigma_V/W & & \\
0 & \rightarrow & W & \rightarrow & V & \rightarrow & V/W & \rightarrow & 0
\end{array}
$$

where $\sigma_W$ and $\sigma_{V/W}$ denote respectively the restriction of $\sigma$ to $W$ and the endomorphism induced on the quotient.

**Lemma 4.18** Let $\sigma$ be an endomorphism of $V$ and assume that $W \subseteq V$ is an invariant subspace. Let $\sigma_W$ denote the restriction of $\sigma$ to $W$ and $\sigma_{V/W}$ the induced endomorphism of $V/W$. Then one has the following relation between characteristic polynomials:

$$P_\sigma(t) = P_{\sigma_W}(t)P_{\sigma_{V/W}}(t).$$

**Proof:** Pick a basis $v_1, \ldots, v_r$ for $W$, and extend it to a basis $v_1, \ldots, v_r, v_{r+1}, \ldots, v_n$ for $V$. The images of $v_{r+1}, \ldots, v_n$ form a basis for $V/W$. In this basis the matrix $C$ of $\sigma$ has a block decomposition like in the figure in the margin, with $A$ being the matrix of $\sigma_W$ and $B$ the one of $\sigma_{V/W}$ both in the relevant basis just described. Clearly $t \cdot I - C$ has a corresponding block decomposition, and it follows that $\det(t \cdot I - C) = \det(t \cdot I - A) \det(t \cdot I - B)$. \[\Box\]

**Problem 4.28.** Show that $\det C = \det A \det B$ when $C$ has a block structure like in the figure. Let *.

(4.2)—**The trace is the sum along the diagonal.** One reason for the trace being so popular is that it can be found without knowing the eigenvalues values. It can be readily computed from the matrix of the endomorphism in any basis.

**Lemma 4.19** The trace of $\sigma$ equals the sum of the diagonal elements of the matrix representing $\sigma$ in any basis. In particular, the trace is linear in $\sigma$; that is, $\text{tr}(a\sigma + b\tau) = a\text{tr}(\sigma) + b\text{tr}(\tau)$.

**Proof:** Recall that the determinant of an $n \times n$-matrix $(a_{ij})$ is a huge sum of terms each up to sign being a product of entries neither two in the same row nor two in same column. To be precise, the determinant is the sum of all terms shaped like

$$\text{sign}(\pi)a_{1\pi(1)}a_{2\pi(2)} \cdots a_{n\pi(n)}$$

where $\pi$ is a permutation of $\{1, 2, \ldots, n\}$.
where \( \pi \) is a permutation of the set \( \{1, \ldots, n\} \). Now, if \( \pi(i) = i \) for all but one \( i \), say \( i_0 \), one obviously has \( \pi(i_0) = i_0 \) since \( \pi \) is a bijection. So the moral is that if one term contains all but one of the diagonal entries, it contains the last diagonal entry as well. Applying this to the determinant \( \det(t \cdot I - A) \), we see that all other terms than
\[
(t - a_{11}) \ldots (t - a_{nn})
\]
have degree at most \( n - 2 \) in \( t \), and it follows that
\[
\det(t \cdot I - A) = t^n - (\sum_{1 \leq i \leq n} a_{ii}) t^{n-1} + \text{terms of lower degree}
\]

\[\square\]

(4.3)—The “original fix point theorem”. At the bottom of many fix points theorem in mathematics is the following lemma telling us that the trace of a projection equals the dimension of its image; the point is that the matrix of the projection in an appropriate basis has a shaped like the one depicted in the margin (a square block being the \( r \times r \)-identity matrix and zeros elsewhere with \( r \) the dimension of the image).

Lemma 4.20 Assume that \( k \) is of characteristic zero. If \( \pi \) is a projection, that is \( \pi^2 = \pi \), then \( \text{tr}(\pi) = \dim_k \text{im} \pi \).

In case the characteristic of \( k \) is positive and equal to \( p \), one can only conclude that \( \text{tr}(\pi) \equiv \dim_k \text{im} \pi \mod p \).

Proof: Let \( r = \dim_k \text{im} \pi \). As for projections in general one has the decomposition \( V = \text{im} \pi \oplus \ker \pi \), and we can chose a basis for \( V \) such that the \( r \) first elements lie in \( \text{im} \pi \) and the remaining \( n - r \) in \( \ker \pi \). Then as \( \pi(v_i) = v_i \) for \( i \leq r \) and \( \pi(v_i) = 0 \) for \( i > r \) obviously \( \text{tr}(\pi) = r \).

Since \( \pi^2 = \pi \) it follows readily that \( \pi \) is the vectors fixed by \( \pi \); that is, \( \text{im} \pi = V^\pi = \{ v \mid \pi(v) = v \} \), so one may rephrase the lemma saying that \( \dim_k V^\pi = \text{tr}(\pi) \).

(4.4)—Trace of a tensor product. Let \( \sigma \) and \( \tau \) be two endomorphisms of respectively the vector spaces \( V \) and \( W \). The following lemmas gives the trace of endomorphism \( \sigma \otimes \tau \) of \( V \otimes_k W \):

Lemma 4.21 One has
\[
\text{tr}(\sigma \otimes \tau) = \text{tr}(\sigma) \text{tr}(\tau).
\]

Proof: Again, we resort to basis, one \( \{v_i\} \) for \( V \) and another \( \{w_j\} \) for \( W \). The vectors \( v_i \otimes w_j \) constitute a basis for the tensor product \( V \otimes_k W \). Let \( A = \{a_{ij}\} \).
respectively $B = \{ b_{ij} \}$ be the matrices of $\sigma$ and $\tau$ in the two basis. Then one has

$$\sigma v_i \otimes \tau w_j = a_{ii} b_{jj} v_i \otimes w_j + \sum_{s \neq i, t \neq j} a_{is} b_{jt} v_s \otimes w_t$$

hence the diagonal elements in the matrix of $\sigma \otimes \tau$ are $a_{ii} b_{jj}$, and it follows readily that

$$\text{tr}(\sigma \otimes \tau) = \sum_{i,j} a_{ii} b_{jj} = (\sum_i a_{ii})(\sum_j b_{jj}) = \text{tr}(\sigma) \text{tr}(\tau).$$

**Problem 4.29.** Let $\pi: V \to V$ be an endomorphism that satisfies $\pi^2 = \pi$. Show that $\text{im} \, \pi = \{ v \in V \mid \pi(v) = v \}$. Show that there is a decomposition $V = \text{im} \, \pi \oplus \ker \, \pi$. **Hint:** $v = v - \pi(v) + \pi(v)$.

**Problem 4.30.** If $A$ is any algebra an element $e \in A$ is called an idempotent if $e^2 = e$. Show that if $e$ is an idempotent $1 - e$ is one as well. Show any $A$ module decomposes as the direct sum $\ker \, e \oplus \ker(1 - e)$.

**Problem 4.31.** Show that if $L$ is a one-dimensional vector space there is a canonical isomorphism $\text{End}_k(L) \simeq k$ sending $a$ to the “multiplication-by-$a$-map”. Show that if $n$ denotes the dimension of $V$ it holds that $\Lambda_n V$ is one dimensional. Show that $\det \sigma \in k$ equals the number corresponding to $\Lambda_n \sigma \in \text{End}_k(\Lambda)_n V$. 

\[ \square \]
5
Induction and Restriction

Very preliminary version 0.7 as of 14th November, 2017
Klokken: 09:24:36
Changes: 7/10: Reworked mostly everything until the section 5.2.3 on page 148 called The projection formula. From there on it still a mess.
9/9: Added a paragraph about restriction to normal subgroups; page 134.
10/10: Tidied up a little.
12/10: Rewritten the paragraph about Mackey’s irred criterion. Added an example about principal series of Sl(2, k).
Fredag 13/10: Started on the section about Induction Theorems, section ??.
15/10: Added a lot to section ??.
2017-11-14 09:20:12: Brushed up example 5.14 on page 153 about the principal series of Sl(2, Fq).

In this section we explore the relations between the representations of two groups related by a homomorphism; the all important case being when \( H \) is a subgroup of \( G \) and the homomorphism the inclusion. But the general case points to the place in the landscape of mathematics where these constructions belong.

As frequently happens in mathematics (especially in geometry), one can associate to a homomorphism \( \phi: \, H \rightarrow G \) two functors; one depends contravariantly on \( \phi \), sends \( G \)-modules to \( H \)-modules and its geometric analogue is the pullback, while the other depends covariantly on \( \phi \), sends \( H \)-modules to \( G \)-modules, and is analogue to the pushout. The two are adjoint functors (which in our present context goes under the name of Frobenius reciprocity). They satisfy a projection formula and are tightly related in several other ways; the Mackey’s induction formula being the most important.

In the all important case that \( H \) is a subgroup of \( G \), the former is called restriction and latter induction, while when \( \phi \) is the quotient map \( G \rightarrow G/H \),
where $H$ is a normal subgroup, the two functors are called \textit{deflation} and \textit{inflation}.

\textbf{5.1} Let $G$ and $H$ be two groups with a group homomorphism $\phi: H \to G$. In an obvious manner $\phi$ gives rise to an algebra homomorphism $\phi: k[H] \to k[G]$, which we abusing the language continue to denote by $\phi$. One simply puts

$$f(\sum_{h \in H} a_h h) = \sum_{h \in H} a_h f(h),$$

or in words, the induced map is the $k$-linear map sending a basis vector $h$ from the canonical basis of $k[H]$ to the basis vector $\phi(h)$ from the canonnic basis of $k[G]$. One easily checks that one in this way obtains an algebra homomorphism. In the frequently occurring case that $H$ is a subgroup, it is nothing but the natural inclusion $k[H] \subseteq k[G]$.

\textbf{5.1 Restriction}

Of the two stable-mates pushout and pullback, one is simple and one subtle, and we begin with the simple one, the \textit{pullback}, or the \textit{restriction} in case $H \subseteq G$. In the general setting we shall denote it by $\phi^*$ and it is a functor

$$\phi^*: \text{Rep}_G, k \to \text{Rep}_H, k.$$

This is a quit natural and non-nonsense functor, which we already have met at several occasions. If $V$ is the representation of $H$ we are to pullback, the underlying vector space of $\phi^* V$ is just $V$, and the representation map is given as the composition:

$$\rho_{\phi^* V} = \rho_V \circ \phi.$$

In the same manner, when acting on map in $\text{Rep}_G, k$ the restriction leaves the underlying linear map unchanged, and one only has to observe that if $\psi(g \cdot v) = g \cdot \psi(v)$, trivially it holds true that $\psi(\phi(g) \cdot v) = \phi(g) \cdot \psi(v)$. The underlying functor on vector spaces is thus the identity functor. Consequently the functor $\phi^*$ is exact, takes direct sums to direct sums and tensor products to tensor products. It induces therefore a ring-homomorphism

$$\phi^*: K_0(G, k) \to K_0(H, k)$$

between the representation rings.
The action of a group element \( h \in H \) on a vector \( v \) is thus given as \( h \cdot v = \phi(h) \cdot v \), and with reference to paragraph 5.1 above, the same holds for elements of \( \alpha \) from the group algebra \( \mathbb{k}[H] \); they act as \( \alpha \cdot v = \phi(\alpha) \cdot v \).

(5.1) In the all important case when \( H \) is a subgroup of \( G \) we shall suppress the reference to inclusion map \( H \hookrightarrow G \) and simply write \( \text{res}^G_H V \) for the restriction, and sometimes, when reference to the involved groups is unnecessary, we simplify the notation further to \( \text{res} V \) or even to \( V \mid_H \).

(5.2) Any class function on \( G \) pulls back to a class function on \( H \), so restriction induces a ring homomorphism \( \text{Cfu}_k(G) \rightarrow \text{Cfu}_k(H) \). The character \( \chi_V \) of \( V \) pulls back to the character of \( \phi^*V \); or expressed in formulae \( \chi_{\phi^*V} = \chi_V \circ \phi \). In the case that \( H \subseteq G \), this is nothing but the restriction \( \chi_V \mid_H \).

(5.3) Recall that the underlying vector space of the restriction \( V \mid_H \) of a \( G \)-module \( V \) is just \( V \). Assume given a \( H \)-invariant subspace \( W \) in \( V \). The image \( gW \) under the endomorphism \( g\mid_V \) is of course a \( \mathbb{k} \)-linear subspace of \( V \) for any \( g \in G \), and it merely depends on the left coset \( gH \): Indeed, for every \( h \in H \) one has \( gW = gW \) because \( hW = W \). This means that \( G \) acts on the set of \( H \)-invariant subspaces of \( V \). Summing over the orbit of \( W \) in this action, we obtain the \( G \)-invariant subspace \( GW \) that is given as

\[
GW = \sum_{gH \in G/H} gW
\]

with a slightly abuse of language. In the case that \( V \) is irreducible (and \( W \neq 0 \)) this gives a representation

\[
V = \sum_{gH \in G/H} gW,
\]

of \( V \) as the sum of translates of \( W \). However, in general the sum is far from being direct, there might repetitions and non-trivial intersections among the summands.

Appealing to lemma 3.5 on page 57 we can conclude

**Proposition 5.1** Let \( k \) be any field. For every subgroup \( H \subseteq G \) and every irreducible \( G \)-module \( V \) over \( k \), then \( \text{res} V \mid_H \) is a semi-simple \( H \)-module over \( k \).

**Proof:** We saw that for any submodule \( W \subseteq V \), one has \( V = \sum_{gH \in G/H} gW \) and lemma 3.5 directly gives that \( V \mid_H \) is semi-simple when we take \( W \) to be irreducible. \( \square \)

One can get rid of the repetitions \( \text{in} \) \((5.1)\) above by introducing the *isotropy group* \( T \) of \( W \); that is, the subgroup of \( G \) given as \( T = \{ g \in G \mid gW = W \} \). It is...
obvious that $H \subseteq T$ and that $W$ is a $T$-invariant subspace. One has

$$GW = \sum_{gT \in G/T} gW,$$

and in that sum every summand appears merely once; since an equality like $gW = g'W$ implies that $g^{-1}g' \in T$. Albeit every summand only appears once, there still can be non-trivial intersections. For instance, if $V = k_G \oplus V'$, and $W = k_H \oplus W'$ with $W' \subseteq V'$ having $H$ as isotropy group, the trivial summand will be part of any of the translates $gW$.

**Restriction to normal subgroups**

We continue the discussion in the previous paragraph, but in the context where $H$ is a normal subgroup of $G$. One can then say a lot more of the structure of the restriction $V|_H$—a circle of ideas that go under the name of Clifford’s theorem. This theorem appears in different guises and different complexities, but we confine ourselves to the most modest form.

**(5.4)—Conjugate representations.** The surrounding group $G$ acts by conjugation on the normal subgroup $H$ and this action induces an action on the set of $H$-modules (even on the category $\text{Rep}_{H,k}$). We let $c_g(x) = g^{-1}xg$. This action is described in the following way. For any element $g \in G$ and any $G$-module $V$, one has the module $V^g$ whose underlying vector space still is $V$, but the effect of $g$ acting on a vector $v$ is $c_g(x) \cdot v = (g^{-1}xg) \cdot v$.

**(5.5)—Isotypic components.** As we observed, in the decomposition (5.1) above the summands may be repeated and even different summands may intersect in a non-trivial way. However, there is one important case when non-trivial intersections between different summands do not appear, and that happens when the $H$-invariant subspace we departed from is an isotypic component of $V|_H$.

For a while we shall work over an arbitrary field, but to have the notion of isotypic components, we need $V|_H$ to be semi-simple, and by lemma 5.1 above, assuming $V$ to be irreducible will suffice.

So assume that $V$ is irreducible and that $U \subseteq V$ is one of the isotypic components of $V|_H$; that is, $U \simeq mW$ for some irreducible $G$-module $W$ (which we can assume lies in $V|_H$) and some natural number $m$. Then clearly $gW = W^g$ is still irreducible, and $gU = U^g \simeq mW^g$ looks like being an isotypic component, and indeed, by the little lemma 3.2 on page 59, it is. If $U'$ is the isotypic component containing $gW$ to lemma gives $gU \subseteq U'$, and the reverse inclusion follows by the same argument applied to $g^{-1}$.
The final piece of notation we need, is the *isotropy group* \( T \) of \( U \) defined as

\[
T = \{ g \in G \mid gU = U \}.
\]

The orbit of \( U \) is naturally identified with \( G/T \), and it holds that \( gU = gTU \).

Clearly \( H \subseteq T \).

We have almost established the following characterization of the restrictions of irreducible representations to normal subgroups

**Proposition 5.2 (Clifford’s theorem)** Assume that \( H \subseteq G \) is a normal subgroup and that \( V \) is a semi-simple representation of \( G \). Assume that \( U \subseteq V|_H \) is an isotypic component of the \( H \)-module \( V|_H \). Then

- The translates \( gU \) are isotypic,
- For any isotypic component \( U' \) of \( V|_H \), the translate \( gU \) and \( U' \) are either equal or their intersection is trivial.
- If \( V \) is irreducible and \( T \) is the isotropy group of \( U \), then

\[
V = \bigoplus_{g \in G/T} gU
\]

is the isotypic decomposition of \( V|_H \). Moreover, \( U \) is an irreducible \( T \)-module.

**Proof:** Only the last statement remains to be proven. Consider the sum

\[
\sum_{g \in G/T} gU
\]

of submodules in the orbit of \( U \) under the action of \( G \). It is \( G \)-invariant and hence equal to \( V \) since \( V \) is irreducible by hypothesis. The sum is also a direct sum since any two of the summands intersect trivially by the second statement of the lemma, and by the first \( gU \) is isotypic, so that we have the isotypic decomposition of \( V|_H \). Assume that \( W \subseteq U \) is a non-trivial \( T \)-invariant subspace. Then \( \bigoplus_{g \in G/T} gW \subseteq \bigoplus_{g \in G/T} gU \) would be \( G \)-invariant and hence equal to \( V \) as \( V \) is irreducible, and it follows that \( W = U \).

\[\text{(5.6)}\]

It is noteworthy that each of the isotypic components of \( V|_H \) has the same number of irreducible summands. If \( m \) is this number, one has

\[
V|_H \simeq m \left( \bigoplus_{g \in G/T} gW \right)
\]

where \( W \subseteq V|_H \) is any (non-trivial) irreducible \( H \)-module. And of course, it follows that \( \dim_k V = m \dim_k W \).

Likewise, it is noteworthy that the restriction \( V|_H \) is isotypic if and only if \( T = G \). So if it is not, the isotropy group \( T \) is a proper subgroup of \( G \) and there is a decomposition \( V = \bigoplus_{g \in G/T} gW \) with \( W \) being an irreducible \( T \)-module.

---

1 We are indulged in the mild abuse of language of confusing cosets and group elements in this particular context.
More on divisibility. We saw that when \( k = \mathbb{C} \), the dimension of any irreducible representation \( V \) of \( G \) is a factor in the index \([G : Z]\) of the centre \( Z \) of \( G \) (theorem 4.7 on page 109). This can strengthened considerably; the dimension divides the index of any normal abelian subgroup.

Notice that with notation as above, the restriction \( V|_H \) is isotypic if and only if \( T = G \), and if it is not, there is a decomposition \( V = \bigoplus_{g \in G/T} gW \) where \( W \) is an irreducible \( T \)-module.

**Proposition 5.3** Assume that \( A \subset G \) is an abelian normal subgroup and \( V \) is any irreducible complex representation of \( V \). Then \( \dim V \) divides the index \([G : A]\).

**Proof:** The proof goes by induction on the order \(|G|\).

If \( V \) is not faithful but has a non-trivial kernel \( N \), then \( V \) is an irreducible module over \( G/N \). Furthermore \( AN/N \) is abelian and normal subgroup of \( G/N \). Hence \( \dim V \) divides \([G/N, A/A \cap N] \) by induction, but \([G : A] = [G/N, A/A \cap N][N : A \cap N] \) and we are through.

So assume that \( V \) is faithful. If \( V|_A \) is not isotypic, the isotropy group \( T \) is non-trivial, and there is an irreducible \( T \)-module \( W \) such that

\[
V = \bigoplus_{g \in G/T} gW
\]

It follows that \( \dim W \) divides \([T : A]\) and hence that \( \dim V = [G : T][T : A] = [G : A] \).

Finally, if \( V|_A \) is isotypic, one has \( V|_A = mL \) where \( L \) is one-dimensional. It follows that \( A \) acts by homothety, and as \( V \) is faithful it ensues that \( A \) is central in \( G \), and we conclude by the theorem on Frobenius divisibility (theorem 4.7 on page 109).

**Examples**

5.1. Let \( g \) be an element of \( G \) and let \( H \) be the subgroup generated by \( g \); that is, \( H = < g > \), and let \( V \) be a complex representation of \( G \) (or a representation over a big friendly field for \( G \)). The restriction \( \text{res}^G_H V \) decomposes as the direct sum of the eigenspaces \( V_{\chi} \) of the endomorphism \( g|_V \) of \( V \); that is, one has

\[
V = \bigoplus_{\chi \in \hat{H}} V_{\chi}.
\]

If \( x \in G \) is any element, the subspace \( xV_{\chi} \) is the eigenspace of the conjugate element \( gxg^{-1} \) associated with the same eigenvalue \( \chi \); indeed, if \( v \in V_{\chi} \), one finds

\[
xg^{-1}(x \cdot v) = x \cdot (g \cdot v) = x(\chi(g)v) = \chi(g)x \cdot v
\]

5.2. Let \( G = S_n \) and \( H \) be the subgroup isomorphic to \( S_{n-1} \) that fixes 1. Then \( V_n|_{S_{n-1}} \) decomposes at \( 1_{S_{n-1}} \oplus V_{n-1} \), where \( V_n \) and \( V_{n-1} \) are the natural representations of \( S_n \) and \( S_{n-1} \) respectively.
5.3. Let $H \subseteq G$ be a subgroup. The character of the complex regular representation of any group vanishes everywhere except at the unit element where its value is the order of the group. Restricting $\chi_{\text{reg},G}$ to $H$, one obtains thus the relation

$$\text{res}_H^G \chi_{\text{reg},G} = \frac{1}{|G : H|} \chi_{\text{reg},H}.$$ 

This indicates that $\mathbb{C}[G]$ is free over $\mathbb{C}[H]$ as a left module whose rank is the index $[G : H]$. Indeed, this is true over any ground field; see lemma 5.1 below.

Problems

5.1. Determine the restriction $\text{res} k[D_n]$ of the regular representation of the dihedral group $D_n$ to the normal, cyclic subgroup $R_n$.

5.2. Let $V_n$ be the basic representation of the symmetric group $S_n$ (the one of dimension $n$). Let $H$ be the subgroup generated by a full cycle. Show that $\text{res} V$ is the regular representation of $H$.

5.3. Let $V$ be the basic, irreducible representation of the symmetric group $S_n$ of dimension $n - 1$, and let $A$ be a subset of $[1, n]$. Determine the restriction $\text{res}^S_A V$ of $V$ to $S_A$. If $B$ is another subset of $[1, n]$ disjoint from $A$, what is $\text{res}^S_{A \times B} ?$

5.4. Let $C_n$ be a cyclic group of order $n$ and let $d$ be divisor of $n$. Let $C_d$ be the subgroup of $C_n$ of index $nd^{-1}$. What is the restriction map $\hat{C}_n \to \hat{C}_d$?

5.2 Induction

The induction is best defined in the language of $G$-modules and is a special case of a very general construction, namely the tensor product $B \otimes_A M$ where $B$ is any $A$-algebra and $M$ any $A$-module. So as we just disclosed, if $V$ is a $H$-module, the induced $G$-module $\text{ind}_\phi V$ is the tensor product

$$\text{ind}_\phi V = k[G] \otimes_{k[H]} V$$

where as in 5.1 we view $k[G]$ as a right $k[H]$-algebra via the map $\phi: k[H] \to k[G]$ extending the homomorphism $\phi: H \to G$. It is immediate that induction is a functor

$$\text{ind}_\phi: \text{Rep}_{H,k} \to \text{Rep}_{G,k}.$$
and by transitivity of the tensor product one has \( \text{ind}_\phi \circ \text{ind}_\psi = \text{ind}_{\phi \circ \psi} \) whenever \( \psi : K \to H \) is another group homomorphism. Indeed, for any \( K \)-module \( V \) one has

\[
k[G] \otimes_{k[H]} (k[H] \otimes_{k[K]} V) = k[G] \otimes_{k[K]} V.
\]

(5.1) We shall apply induction almost exclusively when \( H \) is a subgroup of \( G \), and this paragraph is a closer description in that context. First of all, the notation will be \( \text{ind}_{G/H} V \) for the induction of the \( H \)-module \( V \), or to ease the notation, just \( \text{ind} V \) when the groups \( H \) and \( G \) are understood.

**Lemma 5.1** Let \( H \) be a subgroup of \( G \). Then the group algebra \( k[G] \) is a free right \( k[H] \)-module, and any set \( S \) of representatives for the left cosets in \( G/H \) form a basis.

**Proof:** The members of \( S \) generate \( k[G] \) over \( k[H] \) since any element \( g \) in \( G \) is of the form \( sh \) for some \( s \in S \) and some \( h \in H \). Hence the \( k \)-linear map

\[
\bigoplus_{s \in S} k[H] \to k[G]
\]

(5.2)

that sends \( (a_s)_{s \in S} \) to \( \sum_{s \in S} sa_s \) is a surjective homomorphism of right \( k[H] \)-modules. Now, the number of elements in \( S \) equals the index \( [G : H] \), and consequently the dimension over \( k \) of the two sides in (5.2) are equal; indeed, one has

\[
\]

It follows that the map in (5.2) is an isomorphism, and the set \( S \) is basis as required.

Just to have mentioned it, there is of course a corresponding statement for \( k[G] \) as a left \( k[H] \)-module with an exhaustive list of representatives for the right cosets giving a basis.

(5.2) The image of the summand in (5.2) above corresponding to the element \( s \) is the subspace \( sk[H] \) of \( k[G] \), and it should be clear that this subspace depends solely on the coset \( sH \). In view of the isomorphism (5.2) one has the following precise (but slightly language abusive) description of \( k[G] \) as a (right) \( k[H] \)-module:

**Proposition 5.4** Assume that \( H \subseteq G \) is a subgroup. Then one has a canonical direct sum decomposition \( k[G] = \bigoplus_{s \in G/H} sk[H] \) of the group algebra \( k[G] \) as a right \( H \)-module.

Notice that in general only the right \( H \)-module structure respects the decomposition in the proposition; unless \( H \) is a normal subgroup, left multiplication by elements from \( H \) will permute the summands according to the
action of $H$ on $G/H$. However, when $H$ is a normal subgroup, it holds true that $h \cdot sa = s(s^{-1}hs)a$ for any $a$ in $k[H]$ and any element $h$ from $H$, so $sk[H]$ is invariant under $H$ and is isomorphic to the conjugate representation $k[H]^s$.

**Corollary 5.1** Assume that $H \subseteq G$ is a subgroup and that $V$ is an $H$-module. Then $\dim_k \text{ind}_H^G V = [G : H] \dim_k V$.

**Proof:** Since $k[G]$ is free of rank $[G : H]$ over $k[H]$, the module $k[G] \otimes_{k[H]} V$ is as a $k[H]$-module isomorphic to the direct sum of $[G : H]$ copies of $V$, whence the formula for the dimension. \qed 

(5.3) The functor $\text{ind}_H^G$ is exact (since the group algebra $k[G]$ is a free module over $k[H]$), and it takes direct sums to direct sums.

(5.4) We now extend the description in the previous paragraph of $k[G]$ as a direct sum to any induced module; so let $V$ be an $H$-module. The induced module is given as $\text{ind} V = k[G] \otimes_{k[H]} V$, and it is quite natural to identify the space $V$ with the subspace $1 \otimes V$ of $\text{ind} V$. With that identification in place the subspace $sV$ coincides with $s \otimes V$ whatever group element $s$ is.

Elements from $H$ can “be moved through the tensor product” and one has the identity $s \cdot k[H] \otimes_{k[H]} V = s \otimes V = sV$ for any $s \in G$. This leads, in view of the isomorphism (5.2) above, to the direct sum decomposition

$$\text{ind}_H^G V = \bigoplus_{s \in S} sV,$$

where $S$ as usual denotes a set of representatives of the left cosets of $H$.

Notice that there is no natural right module structure on $\text{ind}_H^G V$, so (5.3) is just a decomposition as vector spaces over $k$. Of course, the induced module $\text{ind}_H^G V$ has a left $k[H]$-module structure inherited from that of $k[G]$, but the decomposition in (5.3) is in general not compatible with that structure. Unless $H$ is a normal subgroup, elements from $H$ permute the summands. However, the subspaces $sV$ only depends on the left coset $sH$, and one can write mildly abusing the language

$$\text{ind}_H^G V = \bigoplus_{s \in G/H} sV.$$ 

**Proposition 5.5** Assume that $H \subseteq G$ is a subgroup and that $V$ is an $H$-module. With the identifications above of $V$ with the subspace $1 \otimes V$ of the induced module $\text{ind}_H^G V$, one has the decomposition

$$\text{ind}_H^G V = \bigoplus_{s \in G/H} sV.$$ 

In particular it holds true that $\dim_k \text{ind}_H^G V = [G : H] \dim_k V$. 

\[\text{DimDeskrip} \]

\[\text{IndDeskrip} \]
Examples

The first two examples are important albeit trivial.

5.4. Obviously one has \( k[G] \otimes_{k[H]} k[H] = k[G] \), so inducing the regular representation of \( H \) up to \( G \) one arrives at the regular one of \( G \).

5.5. In the other end, inducing the trivial representation \( k_H \) up to \( G \) one obtains the permutation representation associated to the action of \( G \) on the set \( G/H \) of left cosets by left multiplication. In formulae, one has \( \text{ind}_H^G k_H = L(G/H) \). Indeed, the decomposition (5.3) assumes the shape

\[
\text{ind}_H^G k_H = \bigoplus_{s \in G/H} sk
\]

with elements from \( G \) permuting the summands.

Induction from a normal subgroup

When the subgroup \( H \) is normal, the induced module \( \text{ind}_H^G \) is easier to grasp. The induced representation \( \text{ind}_H^G V \) has a decomposition

\[
\text{ind}_H^G V = \bigoplus_{s \in G/H} sV
\]

as described in proposition 5.5 above. Now, for every elements \( s \in G \) and any \( h \in H \) one has obviously \( hs = s(s^{-1}hs) \), and therefore \( hsV = s(s^{-1}hs)V \). This shows that the translated subspace \( sV \) is invariant under \( H \), and secondly that the action of \( H \) induced on it, makes it equal to the conjugate representation \( V^s \). Summing up, one has

**Proposition 5.6** Assume that \( H \subseteq G \) is a normal subgroup and that \( V \) is a representation of \( H \). Then

\[
\text{ind}_H^G V = \bigoplus_{s \in G/H} V^s
\]

where \( V^s \) is the representation of \( H \) associated to the conjugation automorphism \( h \rightarrow s^{-1}hs \) of \( H \).

Problems

5.5. Let \( G \) and \( H \) be to groups, and indentify \( H \) with the subgroup \( H \times 1 \) of the direct product \( H \times G \). Let \( V \) be a representation of \( H \). Show that \( \text{ind}_H^G V = V \otimes \mathbb{C}[G] \).
5.6. The aim of this exercise is to show that induction respects the exterior tensor product. Let $H_1 \subseteq G_1$ and $H_2 \subseteq G_2$ be two pairs of a group and a subgroup. Let $V_1$ and $V_2$ be representations of respectively $H_1$ and $H_2$. Show that
\[
\text{ind}_{G_1 \times G_2}^{G_1} V_1 \boxtimes V_2 = \text{ind}_{H_1}^{G_1} V_1 \boxtimes \text{ind}_{H_2}^{G_2} V_2.
\]

5.7. Let $H \subseteq G$ be a subgroup, and let $C$ be a right coset of $H$. Show that $a_C = \sum_{g \in C} g$ is invariant under the action of $H$ on $k[G]$ through left multiplication. Show that the $a_C$'s when $C$ runs through $G/H$ constitute a $k$-basis for the space of invariants $k[G]^H$. Show that $k[G]^H$ is isomorphic to $k[G/H]$ as algebras whenever $H$ is a normal subgroup.

5.8. Let $H \subseteq G$ be normal subgroup and let $\pi: G \to G/H$ be the quotient map. Let $V$ be a representation of $G$ over $k$. Show that $G/H$ acts on $V^H$ in a natural manner, and that $\text{ind}_\pi V$ equals $V^H$ endowed with that action.

5.2.1 Induction of characters and class functions

Naturally it is of great interest to have a formula for the character of the induced representation $\text{ind} V$ in terms of the character $\chi_V$. To pin down that formula one needs the auxiliary function $\hat{\chi}_V$ on $G$ that extends $\chi_V$ by zero; that is, it is defined as

\[
\hat{\chi}_V(g) = \begin{cases} 
0 & g \notin H \\
\chi_V(g) & g \in H.
\end{cases}
\]

With that in place we can formulate and prove

**Proposition 5.7** Let $H \subseteq G$ be a subgroup and let $V$ be an $H$-module. Let $S$ be an exhaustive list of representatives of the left cosets of $H$. With $\hat{\chi}_V$ as introduced above, one has

\[
\chi_{\text{ind} V}(g) = \sum_{s \in S} \hat{\chi}_V(s^{-1} gs).
\]

**Proof:** The induced representation $\text{ind}^G_H V$ decomposes as the direct sum $\text{ind} V = \bigoplus_{s \in S} s V$ since $S$ is a set of representatives for the left cosets of $H$. The trace of $g|_V$ is the sum of the diagonal entries of any matrix representing $g$, in particular of one with respect to a basis compatible with the decomposition above, and we deduce that only summands with $gsV = sV$ contribute to the trace; that is, the summands $sV$ with $s^{-1} gs \in H$. And as $g$ acts on $sV$ as $s^{-1} gs$, the contribution is $\chi_V(s^{-1} gs)$. \qed
Corollary 5.2 With notation as in the previous proposition, one has
\[ \chi_{\text{ind}} V(g) = |H|^{-1} \sum_{x \in G} \chi_V(x^{-1}gx). \]

Proof: We split the sum to the right into sums over cosets \( sH \) the contribution of each to the grand total being
\[ \sum_{x \in sH} \chi_V(x^{-1}gx) = \sum_{h \in H} \chi_V(hs^{-1}gsh) = \sum_{g \in G} \chi_V(s^{-1}gs) = |H| \chi_V(s^{-1}gs), \]
and the corollary follows.

The following reformulation of corollary 5.2 is sometimes instructive to use:

Corollary 5.3 Let \( C \) be one of the conjugacy classes of \( G \) and let \( g \) be an element in \( C \). Then
\[ \chi_{\text{ind}} V(g) = |C_G(g)| |H|^{-1} \sum_{x \in C \cap H} \chi_V(x), \]
where as usual an empty sum is interpreted as being zero.

Proof: For those conjugates \( x^{-1}gx \) of \( g \) that contribute to the sum in corollary 5.2, one clearly has \( x^{-1}gx \in C \cap H \). Each \( y \in C \cap H \) can be written as \( y = x^{-1}gx \) in several ways, and it holds true that \( x_1^{-1}gx_1 = x_2^{-1}gx_2 \) if and only if \( x_2 = x_1z \) with \( z \in C_G(g) \). Hence the number of ways \( y \) can be expressed as \( x^{-1}gx \) equals \( |C_G(g)| \), from which one readily deduces the corollary.

Example 5.6. Recall the dihedral group \( D_n \) of order \( 2n \) with its cyclic subgroup \( R_n \) of order \( n \) generated by \( r \), and for simplicity we assume that \( n \) is odd. Then each non-trivial power \( r^i \) has \( R_n \) as its centralizer.

In section 3.6 (that starts on page 76) we studied the dihedral groups in detail and found all their conjugacy classes. Some of them were shaped like \( na_i = \{ r^i, r^{-i} \} \) (in GAP-notation), with \( 1 \leq i \leq (n - 1)/2 \). Let \( \psi \) be the character on \( R_n \) with \( \psi(r) = \eta \) where \( \eta \) is an \( n \)-th root of unity. For the value \( \text{ind}_{D_n}^{D_n} \psi(r^i) \) we find
\[ \text{ind}_{D_n}^{D_n} \psi(r^i) = |C(r^i)| |R|^{-1} \sum_{x \in R \cap R} \psi(x) = n / n (\psi(r^i) + \psi(r^{-i})) = \eta^i + \eta^{-i}. \]

The “big” conjugacy class \( 2a \) of involutions does not intersect \( R \) at all, so the corollary gives that \( \text{ind}_{D_n}^{D_n} \psi(\sigma) = 0 \) for any involution \( \sigma \).
(5.1)—**Induction of class functions.** Mimicking the formula in proposition 5.7 one may extend the concept of induction to all functions on $H$ with values in $k$. So if $a$ is a $k$-valued function on $H$, we let—in analogy with 5.7—$\hat{a}$ denote the extension of $a$ by zero to the whole of $G$; that is,

$$
\hat{a}(g) = \begin{cases} 
0 & \text{if } g \in H, \\
a(g) & \text{if } g \in H,
\end{cases}
$$

and subsequently we define the induction $\text{ind}_H^G a$ by putting

$$
\text{ind}_H^G a(g) = \sum_{s \in S} \hat{a}(sgs^{-1}).
$$

where $S$ is an exhaustive list of representatives for the left cosets of $H$. When $a$ is a class function on $G$, the induced function $\text{ind}_H^G a$ is a class function on $G$, and the formulas from both corollaries 5.2 and 5.3 persist, the proofs being mutatis mutandis the same. When the class function is a character say $\chi_V$, one obviously has $\text{ind}_G^V \chi = \chi \text{ind}_V$.

From corollary 5.3 it is an easy matter to deduces the following:

**Lemma 5.2** The induced class function $\text{ind}_H^G a$ vanishes on the conjugacy classes $C$ of $G$ not meeting $H$; that is, $\text{ind}_H^G a(g) = 0$ if $g$ is not conjugate to any element in $H$.

**Proof:** In this case the sum in corollary 5.3 that gives $\text{ind}_H^G a(g) = 0$ is empty.

**Example 5.7.**—The abelian case. Induction in the context of abelian groups is, as one would suspect, much simpler than in the general case, and it is worth while making explicit what happens.

So we assume that $A$ is an abelian group with a subgroup $B$, and we are given a class function $a$ on $B$. The conjugacy classes of $A$ are all singletons and the vanishing lemma 5.2 above then implies that the induced class function $\text{ind}_B^A a$ vanishes off $B$. For elements $g \in B$ it holds true that the centralizer $C_a(g) = A$, and the formula in corollary 5.3 assumes the form $\text{ind}_B^A a(g) = |A| |B|^{-1} a(g) = [A : B] a(g)$. Hence we have

**Proposition 5.8** Let $B$ be a subgroup of the abelian group $A$ and let $a$ be a class function on $B$. Then the induced class function $\text{ind}_B^A a$ is given by

$$
\text{ind}_B^A a(g) = \begin{cases} 
0 & \text{when } g \not\in B, \\
[A : B] a(g) & \text{when } g \in B.
\end{cases}
$$
5.2.2 Frobenius reciprocity

A basic ingredient in understanding induced representations is the so called Frobenius’ reciprocity theorem and it is an unsurpassed tool when it comes to decomposing induced representations in irreducibles. Frobenius’ reciprocity theorem can be stated in several ways. With a categorical flavour, it says that the two functors $\phi_!$ and $\phi^!$ associated with a group homomorphism $\phi: H \to G$ are adjoint functors. Adjoint functors appear naturally in many places in contemporary mathematics (and there are general theorems guaranteeing their existence), but Frobenius reciprocity is probably the first occurrence of the concept in the history of mathematics.

Of course Frobenius’s version was in quite another guise. His formulation was in terms characters and their scalar products, which was the lingua franca in the world of representation theory at that time. In terms of representations, the reciprocity theorem takes the form (valid over any field):

**Proposition 5.9 (Frobenius reciprocity)** Given two groups $G$ and $H$ and a group homomorphism $\phi: H \to G$. For any two representations $V$ and $W$ over a field $k$ of respectively $H$ and $G$, there is a canonical isomorphism

$$\text{Hom}_G(\phi_! V, W) \simeq \text{Hom}_H(V, \phi^! W).$$

We prefer giving the proof in the context of general rings and modules. This is a reasonable level where to place the reciprocity theorem in the hierarchy of mathematical structures, and we find the proof more transparent in the general setting—in fact it is a no-nonsense proof of type “do-the-natural-things”. The connection between representations and modules is of course that any representation of $G$ is a module over the group algebra $k[G]$.

**Proposition 5.10** Let $\phi: A \to B$ be a homomorphism between two rings. Let $V$ and $W$ be modules respectively over $A$ and $B$. Then there is a canonical isomorphism

$$\text{Hom}_B(B \otimes_A V, W) \simeq \text{Hom}_A(V, W).$$

Notice that the term “module” means “left module”, except when forming the tensor product $B \otimes_A V$ the ring $B$ is considered to be a right $A$-module. But the tensor product itself is a left $B$-module; multiplication by elements from $B$ being performed in the first factor.

The observant student should have wondered what the term isomorphism in the proposition means. The minimal interpretation is being an isomorphism of abelian groups, but depending on the answer to the notorious soap opera question “who commutes with whom”, the isomorphism can preserve much
more structure. For instance, if $W$ also has a right $B$-module structure, it is an isomorphism of right $B$-modules.

The signification of the term “canonical” is that the map is functorial in both $V$ and $W$. In categorical terms one would rather called it a natural transformation between the bifunctors.

**Proof:** The proof consists of defining mutually inverse maps between the two $\text{hom}$-sets, and to begin with we define the map

$$\Psi : \text{Hom}_B(B \otimes_A V, W) \to \text{Hom}_A(V, W).$$

There is a canonical $A$-homomorphism $V \to B \otimes_A V$ sending $v$ to $1 \otimes v$, and the map $\Psi$ is just “composing with this map”. That is, if $\alpha : B \otimes_A V \to W$ is a $B$ homomorphism, one puts $\Psi(\alpha)(v) = \alpha(1 \otimes v)$.

The second map

$$\Phi : \text{Hom}_A(V, W) \to \text{Hom}_B(B \otimes_A V, W),$$

is induced by the tensor product. Let $\beta : V \to W$ be given. The action of $\Phi(\beta)$ on decomposable tensors $b \otimes v$ is defined as $b \otimes v \mapsto b \beta(v)$, and the expression $b \beta(v)$ being $A$-bilinear in $b$ and $v$, the action extends to map defined on the entire module $B \otimes_A V$ (and the map is $B$-linear).

We leave it to the zealous student to verify that $\Psi \circ \Phi = \text{id}$ and $\Phi \circ \Psi = \text{id}$. 

—The Frobenius way. Returning to the context of complex representation where we have the hermitian product of characters to our disposal, the reciprocity takes the following form (which is Frobenius’s original way of formulating it).

**Proposition 5.11** Let $H \subseteq G$ be two groups and let $V$ and $W$ be complex representations over of respectively $H$ and $G$. Then one has the following equality

$$(\text{ind}_H^G V, W)_G = (V, \text{res}_H^G W)_H.$$

**Proof:** The proof is just taking dimensions in 5.9 and using the relation

$$(\chi_V, \chi_W) = \dim C \text{Hom}_G(V, W),$$

valid for any group $G$ and any two representations $V$ and $W$ of $G$. 

There is also a formulation for class function

**Proposition 5.12** Let $H \subseteq G$ be two groups and let $a$ and $b$ be complex class functions on respectively $H$ and $G$. Then one has the following equality

$$(\text{ind}_H^G a, b)_G = (a, \text{res}_H^G b)_H.$$
Restriction is a much simpler operation than induction, and once the character table of \( G \) is known, it can be directly read off the table. The reciprocity theorem expresses the scalar product \((\text{ind} \chi_V, \chi_W)\) of an induced character \( \chi_V \) against an irreducible character \( \chi_W \) as the product \((\chi_V, \text{res} \chi_W)\) of characters of \( H \). So as observed, if the character table of \( G \) (or the appropriate part of it) is known, this product can be often computed (some minimal knowledge of \( H \) is of course required).

**Example 5.8.** Our first example is a really easy one. We let \( G = C_2 \times C_2 \) be the Klein four-group and \( H = C_2 \subseteq G \) be one of the the cyclic subgroups; for instance, the one generated by \( \sigma \) and whose non-trivial element constitute the class \( 2a \). Let \( \psi \) be the non-trivial character on \( H \), i.e., the one with \( \psi(\sigma) = -1 \). From the table below we see that \( \chi_1 + \chi_2 \) has properties the required by proposition 5.2 on page 143; that is, vanishes off \( H \) and equals \( 2\psi \) on \( H \), so that \( \text{ind} \chi_H = \chi_1 + \chi_2 \).

**Example 5.9.** Let \( G = S_3 \) and \( C_3 \) the cyclic subgroup of order three. Let \( \psi \) be one of the non-trivial characters on \( C_3 \), so that if \( \sigma \) generates \( C_3 \) one has \( \psi(\sigma) = \eta \) with \( \eta \) a primitive 3rd root of unity. Hence \( \psi(\sigma^2) = \eta^2 = -\eta - 1 \).

Using Frobenius reciprocity and referring to table of \( S_3 \) (reproduced in the margin) we find
\[
(\text{ind} \chi_{C_3} \psi, \chi_2) = 3^{-1} (\psi(1)\chi_2(1) + \psi(\sigma)\chi_2(\sigma) + \psi(\sigma^2)\chi_2(\sigma^2) = \\
= 3^{-1} (1 \cdot 2 - (\eta - \eta - 1)) = 1.
\]
Since both \( \chi_2 \) and \( \text{ind} \chi_{C_3} \psi \) are of degree two, it follows that \( \text{ind} \chi_{C_3} \psi = \chi_2 \). And one easily finds \( \text{ind} \chi_{C_3} 1 = 1 + \chi_a \)—they both vanish on the class \( 2a \) and assume the value two on \( 1a \) and \( 3a \).

So what about the characters on the subgroups of order two? If \( \chi_- \) is the non-trivial character on one of them, call it \( C_2 \) and let \( \sigma \) be a generator, one has \( \text{ind} \chi_{C_2} \chi_- = \chi_a + \chi_2 \). Indeed, they both vanish on the class \( 3a \) and coincide on \( 1a \) and \( 2a \): For example, by using 5.3 and observing that \( 2a \cap C_2 = \{\sigma\} \) and that \( \sigma \) is self centralizing, we obtain
\[
\text{ind} \chi_{C_2} \rho(\sigma) = |\text{CG}(\sigma)| / |C_2| \rho(\sigma) = -1.
\]
Finally on \( 1a \) both attain the value 3. Summing up, below is the complete picture of the complex characters of \( S_3 \) that are induced from irreducible cha-
ters of subgroups (the induction of $\text{ind}_{C_2}^{S_3} 1$ and $\text{ind}_{C_1}^{S_3} 1$ are left to the zealous student to work out).

- From the cyclic subgroup $C_3$ of order three one has $\text{ind } \psi = \text{ind } \psi^2 = \chi_2$ and $\text{ind } 1 = 1 + \chi_a$.
- From cyclic subgroups $C_2$ of order two one has $\text{ind } \chi_1 = \chi_a + \chi_2$ and $\text{ind } 1 = 1 + \chi_2$.
- From the trivial subgroup $\text{ind } 1 = 1 + \chi_4 + 2\chi_2$.

**Example 5.10.** The dihedral group $D_n$ of order $2n$ is generated by $r$ and $s$ with relations $r^n = s^2 = 1$ and $srs = r^{-1}$. The cyclic subgroup $R_n$ of $D_n$ generated by $r$ is of order $n$.

Let $\eta$ be a $n$-th root of unity in $k$ and let $L(\eta)$ denote the one-dimensional representation of $R_n$ given by the multiplicative character $\chi_\eta(r^i) = \eta^i$. We are interested in the induced representation $\text{ind}_{R_n}^{D_n} L(\eta)$.

There are two left cosets modulo $R_n$ represented by 1 and $s$. Hence after (5.3), one has

$$\text{ind } L(\eta) = L(\eta) \oplus sL(\eta)$$

and the involution $s$ acts by swapping the two summands. The $R_n$-structure on $sL(\eta) = L(\eta^s)$ is the one given by conjugation, and as $srs = r^{-1}$ it ensues that $sL(\eta)^s = L(\eta^{-1})$. Choosing a basis $v$ for $L$, the two vectors $v$ and $sv$ form a basis for $\text{ind } L(\eta)$, and relative to this basis the action of $D_n$ is given by

$$\rho(r^i) = \begin{pmatrix} \eta^i & 0 \\ 0 & \eta^{-i} \end{pmatrix}, \quad \rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

that is, the induced representation $\text{ind } L$ is nothing but the representation $W_\eta$.

It is irreducible if $\eta \neq \eta^{-1}$, but decomposes otherwise in the sum of two one-dimensional ones. When $\eta = 1$ one has with reference to the notation in paragraph 3.6.1 on page 79 the decomposition $\text{ind } L(1) = L(\chi_0) \oplus L(\chi_a)$ and when $\eta = -1$ it holds that $\text{ind } L(-1) = L(\chi_+) \oplus L(\chi_-)$.

As an illustration of the use of Frobenius reciprocity, we shall find the decomposition of the characters induce from $H = <s>$ into irreducibles. Recall the character $\psi$ of the subgroup $H = <s>$ with $\psi(s) = -1$.

Letting $w_\eta$ be the character of the irreducible $W_\eta$ (so that $\eta^2 \neq 1$) one has $\text{res } w_\eta = 1 + \psi$, and Frobenius reciprocity gives

$$(w_\chi, \text{ind } \psi) = (\text{res } w_\chi, \psi) = (1 + \psi, \psi) = (\psi, \psi) = 1,$$
so that $W_\chi$ occurs once in the decomposition of $\text{ind} \psi$ in irreducibles. Furthermore $\text{res} \chi_+ = \text{res} \chi_0 = 1$ and $\text{res} \chi_a = \text{res} \chi_- = \psi$ which gives

\[
\begin{align*}
(\chi_0, \text{ind} \psi) &= (\chi_+, \text{ind} \psi) = (1, \psi) = 0 \\
(\chi_a, \text{ind} \psi) &= (\chi_-, \text{ind} \psi) = (\psi, \psi) = 1
\end{align*}
\]

Combining all this, we find the decomposition of the induced character $\text{ind} \psi$ in terms of the irreducible characters:

\[
\text{ind} \psi = \begin{cases} \\
\chi_a + 1 & \text{when } n \text{ is odd,} \\
\chi_a + \chi_- + \sum_{\chi \neq \psi_0} w_{\chi} & \text{when } n \text{ is even .}
\end{cases}
\]

### 5.2.3 The projection formula

In geometry one has a projection formula (valid in wide generality, but for instance for maps induced on any cohomology theory), formally it takes the shape:

\[
\phi_*(y \cdot \phi^* x) = x \phi_* y
\]

In our setting and in a simplified and mnemotechnical guise, it looks like

\[
x \text{ ind } y = \text{ ind}(y \text{ res } x).
\]

The real and formally correct formulation is as follows

**Proposition 5.13** Let $H \subseteq G$ be a subgroup and $V$ and $W$ a $k[G]$ and a $k[H]$-module respectively. One has a canonical isomorphism

\[
V \otimes_k \text{ind}_H^G W \simeq \text{ind}_H^G (V|_H \otimes_k W)
\]

**Proof:** To begin with, notice that the underlying vector space of the left side is $V \otimes_k (k[G] \otimes_k H) W$ while that on the right equals $k[G] \otimes_k H (V \otimes_k W)$. We shall define two mutually inverse maps between them. On decomposable tensors they are given as by

\[
\begin{align*}
v \otimes g \otimes w &\mapsto g \otimes g^{-1} v \otimes w \\
g \otimes v \otimes w &\mapsto g v \otimes g \otimes w,
\end{align*}
\]

and since these assignments are linear in each of the three variables and behaves well when moving elements $k[H]$ through the tensor product, they
induce linear maps between the tensor products; indeed, the two identities
\[ v \otimes (gh \otimes w) = v \otimes (g \otimes hw) \] and
\[ g \otimes (g^{-1}v \otimes hw) = gh \otimes (h^{-1}g \otimes w) \] show that
they behave well with respect to moving elements in \( k[H] \) through the tensor
product. They are both \( G \)-equivariant; we shall check that the first one is, leav-
ing the second to the zealous students. For \( s \in G \) one has:
\[ s \cdot (g \otimes w) = sv \otimes sg \otimes w \mapsto sg \otimes (sg)^{-1}sv \otimes w = s \cdot (g \otimes g^{-1}v \otimes w). \]

It is a matter of easy verification that the two maps are mutually inverses on
the decomposable tensors, hence the induced linear maps are as well (they are
uniquely defined by their behavior on the decomposable tensors).

(5.1) When a group homomorphism \( \phi : H \to G \) is given, induction and restric-
tion gives rise to two maps \( \phi^* \) and \( \phi_* \) between the different groups and rings
associated to two groups groups, and in these terms, the projection formula
takes the familiar form
\[ \phi_*(x \cdot \phi^*(y)) = x \cdot \phi^*(y) \]
where \( x \in K_0(H, k) \) and \( y \in K_0(G, k) \) (or in any of the other rings associated to
the groups, like the rings of characters \( \text{Ch}(G) \) or class functions \( \text{Cfu}(G) \)).

Example 5.11. The example is \( C_p \supset C_{pq} \) when \( p \) and \( q \) are two different
prime numbers.

Problem 5.9. Assume that \( N \) is a normal subgroup of \( G \) and \( H \) is another
subgroup containing \( N \). Denote \( G/N \) by \( G' \) and \( H/N \) by \( H' \). Let \( V \) be an
\( H' \)-module, and let \( V_H \) be the inflated module; that is, \( V \) considered as an \( H \)-
module. Show that \( \text{ind}_{G/H'} V \) equals \( \text{ind}_{G/H} V_H \) considered as a \( G \)-module.

HINT: \( k[G] \otimes_{k[H]} V = k[G] \otimes_{k[H]} k[H] \otimes_{k[H']} V \)

5.3 Mackey’s theorems

We present two of Mackey’s central theorems which are frequently applied in
group theory and which are standard parts of the body of theorems usually
included in courses on the subject. They are generally valid regardless of how
the characteristic of the ground field \( k \) relates to the order of \( G \), but the proofs
are slightly longer in the general case than over \( \mathbb{C} \) where one can resort to
to characters.
(5.1) **Double cosets.** To every pair of subgroups $H$ and $K$ of $G$ one has for each element $s \in G$ the double cosets $KsH$; the subsets $\{ ksh \mid k \in K, h \in H \}$ of $G$. They form a partition of $G$; that is, two of them are either disjoint or coinciding, which follows directly from the fact that $KsH \subseteq Ks'H$ if and only if $s \in Ks'H$.

For any element $g \in KsH$ it obviously holds true that $gH \subseteq KsH$, so that $KsH$ is the union of the left cosets of $H$ contained in it. Hence these cosets form a partition of the double coset $KsH$. Moreover, the group $K$ acts on the left cosets $gH$ contained in $KsH$ by multiplication from the left with the isotropy group of $sH$ being the group $Ks = sHs^{-1} \cap K$; one has $KsH = sH$ if and only if $k = sshs^{-1}$ for some $h \in H$. To ease the presentation of some formulas we adopt the notation $H$ for the conjugate subgroup $sHs^{-1}$.

**Example 5.12.** In the benign case that $K = H$ and $H$ is a normal subgroup, the double cosets $HsH$ coincide with the simple cosets $sH$; indeed, since $H$ is normal, one has $Hs = sH$ so that $HsH = sHH = sH$.

(5.2) Fix an element $s \in G$. Any $H$-module $V$ carries by “transport of structure” a natural structure as $sH$-module. This means that action of $sH$ is induced by the action of $H$. With the conjugation map $s'H = sHs^{-1} \rightarrow H$ as a go between; in other words, an element $x \in sHs^{-1}$ acts on a vector $w$ as $k \cdot w = s^{-1}xs \cdot w$.

The representation obtained in this way will be denoted by $V^s$ and is said to be conjugate to $V$.

**Problem 5.10.** Show that one has an equality $\text{ind}_{G}^{G} V = \text{ind}_{sHs^{-1}}^{G} V^s$. **Hint:** One has $\text{ind}_{sHs^{-1}}^{G} V^s = \bigoplus_{x \in G/sHs^{-1}} xV^s$ and $\text{ind}_{H}^{G} V = \bigoplus_{y \in G/H} yV$. Map $G/sHs^{-1}$ to $G/H$ by $x \mapsto s^{-1}xs$.

**Example 5.13.** When $H$ is normal, the conjugate module $V^s$ is the one we met earlier and it is again a $H$-module. In general, however, it is not isomorphic to $V$. Of course, for all $s$ belonging to the centralizer $C_G(H)$ it will be equal to $V$, but for other elements $s$ the module $V^s$ may or may not be isomorphic to $V$. For example, consider the cyclic subgroup $R_n$ of the dihedral group $D_n$. The involution $s$ acts on $R_n$ as $srs = r^{-1}$ so for characters of $R_n$ one has $\chi^s = \chi^{-1}$, and characters satisfying $\chi^2 = 1$ are the only invariant ones.

5.3.1 **The decomposition theorem**

The first of the two theorems of Mackey we treat in this section, deals with what happens if one induces a module from one subgroup and then restricts
it to another; that is, a description of the operation \( \text{res}_K^G \circ \text{ind}_H^G \). The theorem gives a decomposition of the result of this up-down-operation in terms of the original module, the double cosets of the two subgroups and conjugations in the group.

One has, with notation as above, the following theorem:

**Theorem 5.1 (Mackey’s decomposition)** Let \( k \) be any field. Let \( G \) be a group and \( H \) and \( K \) two subgroups. For any \( H \)-module \( V \) one has

\[
(\text{ind}_H^G V)|_K = \bigoplus_s \text{ind}_{Ks}^K (V^s|_{Ks})
\]

where in the direct sum the index \( s \) runs over a set of representatives for the double cosets \( KsH \).

Notice that \( Ks \) depends on the choice of \( s \) in the class \( KsH \), in that \( Ks = kKs^{-1} \), but the summand \( \text{ind}_{Ks}^K (V^s|_{Ks}) \) does not (hopefully you solved problem 5.10).

**Proof:** After proposition 5.5 on page 139 the induced module decomposes as \( \text{ind} V = \bigoplus_{g \in G/H} gV \) where the sum is over the left cosets \( gH \). Grouping together those summands whose indexing coset lie in the same double coset \( KsH \) one constructs the subspace \( V(s) = \bigoplus_{gH \subseteq KsH} gV \) of \( \text{ind} V \); a subspace that clearly is invariant under the action of \( K \), since the indexing set is.

One has \( \text{ind}_H^G V = \bigoplus_s V(s) \), so what remains to be proven, is that the summands appearing on the right side in the theorem are precisely the spaces \( V(s) \). To that end, observe that \( sV \) is invariant under the action of \( K_s = sHs^{-1} \cap K \); indeed, if \( k = shs^{-1} \) one has

\[
ksV = shs^{-1}sV = shV = sV.
\]

This also shows that the actions of \( shs^{-1} \) on \( sV \) is induced by the action of \( h \) on \( V \); in other words, \( sV \) is isomorphic to \( V \) as an \( sHs^{-1} \)-module and therefore to \( V \) as a \( Ks \)-module.

Again by proposition 5.5 the induced module \( \text{ind}_{Ks/Ks} sV \) decomposes as a direct sum \( \bigoplus_{k \in Ks/Ks} ksV \) indexed by the representatives \( k \) of the left cosets \( kKs \) in \( K \). To connect up with the cosets of \( H \), when \( gH \subseteq KsH \) one may represent \( gH \) by an element of the form \( g = ks \). Moreover, two such elements represent the same left coset of \( H \) if and only if \( ksh = k's \); that is, if and only if \( k' = ks^{-1}sh \), which amounts to \( k \) and \( k' \) representing the same left coset of \( Ks \) in \( K \). Sending \( ksH \) to \( kKs \) therefore gives a well defined map from the set of left cosets of \( H \) contained in \( KsH \) to the set \( Ks/Ks \) of left cosets of \( Ks \) in \( K \). It is obviously surjective (given \( k \in K \), then \( ksH \) maps to \( kKs \)) and injective (is \( k' = ks^{-1} \) clearly \( k'sH = ksH \)). Hence both the index sets and summands in the two decomposition coincide, and we are happy.
(5.1) Specializing the situation to the case that $K = H$ and $H$ is a normal subgroup Mackey’s decomposition takes the following form.

**Corollary 5.4** Assume that $H$ is a normal subgroup of $G$ and that $V$ is an $H$-module. Then it holds true that

$$\left(\text{ind}_H^G V\right)|_H = \bigoplus_{s \in G/H} V^s,$$

where the $V^s$ are the conjugate representations of $V$.

(5.2) It is enlightening to go through the proof of Mackey’s decomposition theorem by the use characters. In the particularly simple case when $K = H$ and $H$ is a normal subgroup, the formula in corollary 5.4 is nothing but the one in 5.7 that reads

$$\psi(g) = |H|^{-1} \sum_{s \in G} \chi(s^{-1}gs) = \sum_{s \in G/H} \chi(s^{-1}gs),$$

where $\chi$ is the extension by zero of $\chi$, and the last sum is over a set of representatives of the left cosets $sH$. Indeed, when restricting to $H$ one gets

$$\psi(h) = \sum_{s \in G/H} \chi^s(h)$$

since by definition $\chi^s(h) = \chi(s^{-1}hs)$ and the “dot” doesn’t matter as $H$ is a normal subgroup.

5.3.2 Mackey’s criterion

A very natural question is whether the induced representation of an irreducible representation is irreducible or not, and Mackey’s criterion gives an answer to that. Both cases can occur; for instance in the case of the dihedral groups, the induced representations $\text{ind}_{D_n}^{R_n} \chi$ will be irreducible when $\chi^2 \neq 1$ but decompose into two one-dimensional representations when $\chi^2 = 1$ (see example 5.10 on page 147).

(5.1) We begin by explaining some the ingredients. As usual in this section, $H \subseteq G$ is a group and subgroup and $V$ is an $H$-module. Associated to any element $s \in G$ one has the subgroup $^sH = sHs^{-1}$ the conjugate to $H$. There will be two modules in play; over $H$ one has the original module $V$ and over $H^s$ the conjugate module $V^s$. By restricting these we obtain two modules over the intersection $H^s \cap H$, namely $\text{res}_{H^s \cap H}^H V$ and $\text{res}_{H^s \cap H}^H V$. When $s = 1$ they both coincide with $V$, but for $s \neq 1$ they may or may not shear an irreducible summand. The outcome of this dichotomy, is precisely what matters for $\text{ind} V$ to be irreducible.
Theorem 5.2 (Mackey’s irreducibility criterion) Let $G$ be a group whose order is prime to the characteristic of the ground field and let $H$ be a subgroup of $G$. Assume that $V$ is an irreducible $H$-module. Then the induced module $\text{ind}^G_H V$ is irreducible if and only if $V_{|H\cap H}$ and $V^s_{|H\cap H}$ have no common irreducible component for $s \notin H$.

**Proof:** We give the proof over the complex field $\mathbb{C}$, and have characters and Frobenius reciprocity at our disposal$^2$. We let $\chi$ be the character of $V$ and $\chi^s$ to one of $V^s$. Applying Mackey’s decomposition formula (theorem 5.1 on page 151) with $K = H$ and Frobenius reciprocity (theorem 5.9 on page 144) twice gives

$$\left(\text{ind}^G_H \chi, \text{ind}^G_H \chi\right)_G = \left(\chi, \left(\text{ind}^H_H \chi\right)_{|H}\right)_H = \sum_{H \cap H} \left(\chi_{|H\cap H}, \chi^s_{|H\cap H}\right)_{H\cap H} = 1 + \sum_{H \cap H \neq H} \left(\chi_{|H\cap H}, \chi^s_{|H\cap H}\right)_{H\cap H}$$

where the sum is over a set of representatives of the double cosets $HsH$. Notice that $HsH = H$ if and only if $s \in S$, and for this double coset one can use 1 as the representative so that $\chi^s = \chi$ and $H^s = H$. Hence the corresponding term in the huge sum reduces to $(\chi, \chi)$, which equals one as $\chi$ is irreducible.

The terms in the huge sum are all non-negative integers being hermitian product of characters (non merely class functions), and one deduces from the equality above that $(\text{ind}^G_H \chi, \text{ind}^G_H \chi)_G = 1$ if and only if $(\chi_{|H\cap H}, \chi^s_{|H\cap H})_{H\cap H} = 0$ for all $s \notin H$, but that is exactly to say that $V_{|H\cap H}$ and $V^s_{|H\cap H}$ do not share any irreducible component.

Example 5.14. —The principal series of $\text{Sl}(2, \mathbb{F}_q)$. In this example we shall construct some of the irreducible representations of the group $G = \text{Sl}(2, \mathbb{F}_q)$, where $\mathbb{F}_q$ is the field with $q$ elements, the so called principal series. It is a nice illustration of how one can exhibit irreducible representations with the help of induction technics. We shall assume that $q \geq 4$ and for simplicity that $q$ is odd.

Fix a non-zero vector $v \in \mathbb{F}_q^2$ and let $H \subseteq G$ be the subgroup of elements $h \in \text{Sl}(2, \mathbb{F}_q)$ having $v$ as eigenvector. Denote the corresponding eigenvector by $\lambda(h)$; that is, one has

$$H = \{ h \in \text{Sl}(2, \mathbb{F}_q) \mid h(v) = \lambda(h)v \text{ for some } \lambda(h) \in \mathbb{F}_q \}.$$  

The eigenvalue $\lambda(h)$ of $h$ is a multiplicative character on $H$, and in fact, assumes values in $\mathbb{F}_q^\ast$. 

$^2$ This is merely of typographical (and hence pedagogical) reasons. Replacing the hermitian product between characters with the appropriate hom-groups, the proof goes through *mutatis mutandis.*
For instance, for the particular choice \( v = (1,0) \), the group \( H \) becomes the subgroup of lower triangular matrices; that is,

\[
H_0 = \{ h = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \}.
\]

Obviously the order of \( H_0 \) equals \( (q - 1)q \) and as a general \( H \) is conjugate to \( H_0 \), one has \(|H| = (q - 1)q\).

Let \( \eta : \mathbb{F}_q^* \to \mathbb{C} \) be a homomorphism (taking values in \( \mu_{q-1} \)) and assume that \( \eta^2 \neq 1 \). Let \( \chi \) be the multiplicative character on \( H \) defined by \( \chi(k) = \eta(\lambda(h)) \).

We shall apply Mackey’s criterion to show that \( \text{ind}_H \chi \) is irreducible. So let \( s \in \text{Sl}(2, \mathbb{F}_q) \) but \( s \not\in H \); that is, \( v \) is not an eigenvector for \( s \). The salient point (which is elementary to check) is that if for some \( h \in H \) the conjugate \( shs^{-1} \) lies in \( H \) then \( s^{-1}v \) is both an eigenvector of \( h \) and of \( s^{-1}hs \). So two things can happen, either \( s^{-1}v \) is a scalar multiple of \( v \) or \( s^{-1}v \) is an eigenvector of \( h \) different from \( v \). In the former case \( s \) would be in \( H \), which by assumption does not occur. So \( s^{-1}v \) is an eigenvector of \( h \) different from \( v \), and the corresponding eigenvalue is therefore \( \lambda(h)^{-1} \). But then \( \lambda(s^{-1}hs) = \lambda(h)^{-1} \), and the conjugate character \( \chi^s \) of \( \chi \) is given as \( \chi^s = \chi^{-1} \). Since \( \chi^2 \neq 1 \), one has \( \chi^s \neq \chi \) and Mackey’s criterion applies.

The degree of \( \text{ind} \chi \) is \( q + 1 \) (in general when a character is induced, the degree becomes multiplied by the index of the subgroup, which in the present case equals \( q + 1 \)). Moreover, the groups \( \mathbb{F}_q^* \) and \( \mu_{q-1}(\mathbb{C}) \) are both cyclic of order \( q - 1 \), and there are \( q - 1 \) homomorphisms from one to the other. Only \( q - 3 \) of them are useful for our purpose, we must exclude the trivial one and the one sending a generator of \( \mathbb{F}_q^* \) to \(-1 \). This construction hence gives us \( q - 3 \) irreducible complex representations of \( \text{Sl}(2, \mathbb{F}_q) \) of degree \( q + 1 \).

The inverse pair of characters \( \chi \) and \( \chi^{-1} \) gives rise to isomorphic representations, but this is also the only isomorphisms that occur; hence, we obtain in this way \( (q - 3)/2 \) non-isomorphic irreducible representations of \( \text{Sl}(2, \mathbb{F}_q) \). To give an argument for this, we shall compute the values of the induced characters \( \text{ind} \chi \).

If an element \( g \in \text{Sl}(2, \mathbb{F}_q) \) has two distinct eigenvalues, say \( a \) and \( a^{-1} \), its centralizer \( C_G(g) \) is of order \( q - 1 \) (the centralizer is conjugate to the group of diagonal matrices of determinant one). The conjugacy class where \( g \) lies intersects \( H \) in the union of two \( H \)-conjugacy classes; those having eigenvalue \( a \) at the distinguished vector, and those having eigenvalue \( a^{-1} \) there. In both there are \( q \) elements. Applying the formula in corollary 5.3 on page 142 gives

\[
\text{ind} \chi(g) = |C_G(g)| |H|^{-1} \sum_{x \in C_G(g) \cap H} \chi(x) = (q - 1)(q(q - 1))^{-1} q(\eta(a) + \eta(a^{-1})) = \eta(a) + \eta(a)^{-1}.
\]

The matrices in \( \text{Sl}(2, \mathbb{F}_q) \) with only one eigenvalue are conjugate to upper
triangular matrices with 1’s on the diagonal:

\[
\begin{pmatrix}
1 & b \\
0 & 1
\end{pmatrix}.
\]

Those with \(b \neq 0\) constitute two conjugacy classes in \(\text{Sl}(2, \mathbb{F}_q)\) according to \(b\) being a square or not in \(\mathbb{F}_q\); indeed, one has

\[
\begin{pmatrix}
x & c \\
0 & x^{-1}
\end{pmatrix}
\begin{pmatrix}
1 & b \\
0 & 1
\end{pmatrix}
\begin{pmatrix}
x^{-1} & -c \\
0 & x
\end{pmatrix}
= 
\begin{pmatrix}
1 & x^{2}b \\
0 & 1
\end{pmatrix}.
\]

The centralizer of such a matrix is of order \(2q\) (it must hold that \(x = \pm 1\) since \(x^2 = 1\), but \(c\) can be an arbitrary element of \(\mathbb{F}_q\)), and there are \((q - 1)/2\) elements in each of the two classes lying in \(H\) (the elements of \(\mathbb{F}_q^*\) are evenly distributed among squares and non-squares). Hence for elements \(g\) in either class it holds that

\[
\text{ind } \chi(g) = |C_G(g)| |H|^{-1} \sum_{x \in C \cap H} \chi(x) = 2q(q(q - 1))^{-1}(q - 1)/2 = 1.
\]

Finally, on the trivial class all the induced characters \(\text{ind } \chi\) take the value \(q + 1\).

To sum up, two homomorphisms \(\eta\) and \(\epsilon\) give isomorphic induced representations if and only if \(\eta + \eta^{-} = \epsilon + \epsilon^{-}\) as functions on \(\mathbb{F}_q^*\), but different multiplicative characters are linearly independent, so it follows that this occurs if and only if either \(\eta = \epsilon\) or \(\eta = \epsilon^{-}\).

**Problem 5.11.** Do example 5.14 for the case \(q\) being even.

(5.2) The simpler case when \(H\) is a normal subgroup is of special interest. In that case all the conjugate groups \(H^\prime\) coincide with \(H\), and the representations in play are the conjugate representations \(V^s\). The criterion takes the form

**Theorem 5.3** Assume that \(H \subseteq G\) is a normal subgroup, and that the order of \(G\) is prime to the characteristic of \(k\). Let \(V\) be an irreducible \(H\)-module. Then \(\text{ind}_H^G V\) is irreducible if and only if \(V\) is not isomorphic to any of its non-trivial conjugates; i.e., \(V \nmid V^s\) for \(s \notin H\).

**Problem 5.12.** Assume that \(H \subseteq G\) is a normal subgroup such that the conjugation map \(G/H \to \text{Aut}(H)\) has a non-trivial kernel. Show that \(\text{ind}_H^G \) never is irreducible.

**Problem 5.13.** Let \(H\) and \(K\) be two subgroups of \(G\) and let \(V\) and \(W\) be two representations of respectively \(H\) and \(K\). Show that

\[
\text{ind}_H^G V \otimes \text{ind}_K^G W = \bigoplus_{K \subseteq H} \text{ind}_H^G (V^s|_{K_s} \otimes W|_{K_s})
\]

**Hint:** Combine Mackey’s decomposition theorem with the projection formula.
**Problem 5.14.** Keeping the notation from the previous exercise, show that
\[ \text{Hom}(\text{ind}^{G}_{H}V, \text{ind}^{G}_{K}W) = \bigoplus_{K \leq H} \text{ind}^{K}_{K} \text{Hom}(V^{s}|_{K_{s}}, W^{s}|_{K_{s}}). \]

5.3.3 Recap about trace

Let \( V \) a finite dimensional vector space over a field \( k \) and let \( \sigma \) be an endomorphism of \( V \). The trace of \( \sigma \) is by definition the negative of coefficient of the subdominant term of the characteristic polynomial of \( \sigma \). That is, one has
\[ \det(t \cdot \text{id}_{V} - \sigma) = t^{m} - \text{tr}(\sigma)t^{m-1} + \ldots \]
Since the characteristic polynomial is invariant under conjugation, it follows immediately that the trace is as well. The subdominant coefficient of every monic polynomial equals the negative sum of the roots, so the trace is equal to the sum of the eigenvalues of \( \sigma \) (repeated as their multiplicities indicate).

In particular, if \( \sigma = s + n \) is the Jordan decomposition of \( \sigma \), i.e., \( s \) and \( n \) are commuting endomorphisms with \( s \) semi-simple and \( n \) nilpotent, then \( \text{tr}(\sigma) = \text{tr}(s) \).

and of course, the trace is additive \( \text{tr}(\sigma + \sigma') = \text{tr}(\sigma) + \text{tr}(\sigma') \).

Writing down a matrix for \( \sigma \) in some basis and developing the determinant \( \det(t \cdot I - A) \) one sees that the trace equals the sum of the diagonal elements; so if \( A = (a_{ij}) \) one has
\[ \text{tr}(\sigma) = \sum_{i} a_{ii}, \]

It is a fact that a tuple of numbers \( (\lambda_{1}, \ldots, \lambda_{r}) \) from \( k \), repetitions are allowed, is determined by the power sums \( \sum_{i} \lambda_{k}^{i} \) for \( k \leq r \). This hinges on a result from the theory of symmetric functions that says that with some restrictions on the characteristic of \( k \), both the power sums and the elementary symmetric functions form a basis for the vector space of symmetric polynomials. In the transition from power sums to elementary symmetrics the numbers \( k! \) appear as denominators, so in characteristic zero it works well, but care must be shown in positive characteristic. However if \( \sigma \) semi-simple and of finite order, it is OK.

**Lemma 5.3** Let \( V \) be a finite dimensional vector space over a field \( k \) of characteristic zero, and let \( p : V \rightarrow V \) be a projection operator, i.e., \( p^{2} = p \). Then the trace of \( p \) equals the dimension of its image; that is, one has then \( \text{tr}(p) = \dim \text{im} p \).
Over a field of positive characteristic $p$, one can only conclude that $\text{tr}(p)$ and $\dim \text{im } p$ are congruent modulo $p$.

**Proof:** Let $r = \dim V$. The space $V$ decomposes as the direct sum of $\ker p$ and $\text{im } p$. Hence any basis for $\text{im } p$ can be complemented by any basis for $\ker p$ to form a basis for $V$. In this basis the matrix of $p$ has the identity $r \times r$-identity matrix as an $r \times r$-block in the upper left corner and the rest of the entries are all zero. Hence $\text{tr}(p) = r$. 

**Lemma 5.4** \( \dim V^G = |G|^{-1} \sum_{g \in G} \chi_V(g) \)

**Proof:** In the proof of Maschke’s theorem we introduced the averaging operator (formula (??) on page ??) defined by $E = |G|^{-1} \sum_{g \in G} g$. It is a projection onto $V^G$ so taking traces and using lemma 5.3 above we obtain

$$\dim V^G = \dim \text{im } E = \text{tr}(E) = |G|^{-1} \sum_{g \in G} \chi_V(g).$$

**Theorem 5.4** Let $V$ and $W$ be two representations of $G$. Then

$$\dim \text{Hom}_G(V, W) = |G|^{-1} \sum_{g \in G} \chi_W(g) \chi_V(g^{-1})$$

**Proof:** This follows immediately from lemma 5.4 above applied to the representation $\text{Hom}_k(V, W)$. One has $\text{Hom}_G(V, W) = \text{Hom}_k(V, W)^G$ and $\text{Hom}_k(V, W) \simeq V^* \otimes_k W$ so that

$$\chi_{\text{Hom}_k(V, W)}(g) = \chi_{V^* \otimes W}(g) = \chi_V(g^{-1}) \chi_W(g).$$

Assume now that $a$ is a class function that is orthogonal to the space of characters; i.e., one has $(a, \chi) = 0$ for all irreducible characters $\chi$. It follows that $a = 0$. Indeed, it follows that

$$0 = \sum_{g \in G} a(g) \chi_V(g) = \lambda \dim V$$

hence that $\lambda = 0$ and $E_a = \sum_{g \in G} a(g)g$ acts as zero on any irreducible, it must be irreducible.

The functorial way of defining the determinant of $\sigma$ is as $\wedge_m \sigma : \wedge_m V \to \wedge_m V$ where $m$ is the dimension of $V$. The exterior power $\wedge_m V$ is one dimensional, and as $\text{End}_k(U)$ is canonically isomorphic to $k$, the $\det \sigma$ is a number in $k$. 


Lemma 5.5 The characters form a basis for the class functions.

Proof: First of all they are class functions since $\text{tr}(\sigma)\tau\sigma^{-1} = \text{tr}(\sigma)$.

The character is a class function; constant on conjugacy classes. $\chi_{V+V'} = \chi_V + \chi_{V'}$, $\chi_{V\otimes V'} = \chi_V \chi_{V'}$.

5.4 Examples

5.4.1 The quaternionic group

Recall that the quaternionic group $Q_8$ is the subgroup of $H^*$ consisting of $\pm1, \pm i, \pm j, \pm k$. It holds that $i^2 = j^2 = k^2 = -1$ and $ij = k, ki = j$ and $jk = i$; moreover the $i, j$ and $k$ anti-commute pairwise. It is of order 8. The centre equals $\{\pm 1\}$ and $-1$ is the only involution (i.e., element of order two). There are five conjugacy classes, $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}$ and $\{\pm k\}$.

Dividing out the centre one obtains the short exact sequence

$$1 \longrightarrow C_2 \longrightarrow Q_8 \longrightarrow C_2 \times C_2 \longrightarrow 1$$

The quaternionic group thus has four one-dimensional representations inflated from the ones of $C_2 \times C_2$ which account for the lower $4 \times 5$ part of the character table below. As the are five conjugacy classes there is one more representations, whose dimension must be 2 (it satisfies $x^2 + 4 = 8$).

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>-1</th>
<th>±i</th>
<th>±j</th>
<th>±k</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi$</td>
<td>2</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<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>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>$1_Q$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

5.4.2 The dihedral groups

5.4.3 The generalized quaternionic groups

A class of groups that frequently show up in group theory are the so called Generalized quaternionic groups. They are all 2-groups an there is one $Q_a$ for each natural number $a \geq 2$. The order of $Q_a$ is $2^{a+1}$. One might be tempted to include the cyclic group $C_4$ among the generalized quaternionic groups as $Q_1$, but it would be trivial and abelian cousin, and we shall not do it. For $a = 2$ one gets back the quaternionic group $Q$ of order 8; hence the name generalized quaternionic.
The generalized quaternionic group $Q_{a}$ is generated by two elements $\sigma$ and $\tau$ that satisfy the relations

$$\tau^{2^a} = 1, \quad \sigma^2 = \tau^{2^a - 1}, \quad \sigma \tau \sigma^{-1} = \tau^{-1}. \quad (5.4)$$

The last being equivalent to $\sigma \tau = \tau^{-1} \sigma$ or to $\tau \sigma = \sigma \tau^{-1}$, so a power $\tau^i$ can be moved beyond a $\sigma$ when inverted. It is a straightforward exercise that every element in $Q_{a}$ can be uniquely written as $\tau^i \sigma^j$ with $0 \leq i < 2^a$ and $j = 0$ or $j = 1$. It is well an easy exercise to check that the centre of $Q_8$ is generated by the involution $\sigma^2$; that is, $Z(Q) = \langle \sigma^2 \rangle$.

The subgroup $T = \langle \tau \rangle$ is cyclic of order $2^a$, and it is normal of index $2$ and has $S = \langle \sigma \rangle$ as a partial complement, this means that $ST = Q$ and the intersection $S \cap T$ is central; indeed, it equals $Z(Q_{a})$. There is an exact sequence

$$1 \rightarrow T \rightarrow Q_{a} \rightarrow C_2 \rightarrow 1.$$  

The commutator subgroup of $Q_{a}$ equals the cyclic subgroup $\langle \tau^2 \rangle$ and the quotient $Q_{a} / \langle \tau^2 \rangle$ is isomorphic to the Klein four group $C_2 \times C_2$.

We proceed to determine the conjugacy classes of $Q_{8}$. They come in two flavours; some are contained in $T$ and some intersect $T$ trivially. For the former, one has for every $b$ and every $i$ equality

$$(\tau^b \sigma) \tau^i (\tau^b \sigma)^{-1} = \tau^{-i},$$

so that $C_i = \{ \tau^i, \tau^{-i} \}$ is a conjugacy class. $T$. If $i = 0$ or $i \equiv 2^{a-1} \mod 2^a$, the class $C_i$ is a singleton, but the remaining $(2^a - 2)/2 = 2^a - 1$ all have two elements. For the classes not in $T$, one finds that

$$\tau^b \tau^i \sigma \tau^{-b} = \tau^{i+2b} \sigma$$

for every $b$ and $i$. Hence the elements not belonging to $T$ split into two conjugacy classes

$$C_{even} = \{ \tau^i \sigma \mid i \text{ even} \} \quad \text{and} \quad C_{odd} = \{ \tau^i \sigma \mid i \text{ odd} \}$$

each having $2^{a-1}$ elements.

Among the representations of $Q_{8}$ there are four of dimension one. We can give $\chi(\tau)$ and $\chi(\sigma)$ any combination of $\pm 1$, that is $\chi(\tau) = \epsilon_1$ and $\chi(\sigma) = \epsilon_2$ for any choice of $\epsilon_1, \epsilon_2 \in \{ \pm 1 \}$, and since the defining relations (5.4) are satisfied, we obtain a group homomorphism $Q_{8}$ into $\{ \pm 1 \} = \mu_2$.

The remaining $2^{a-1} - 1$ irreducible representations are all of dimension two and are all induced from $T$. To describe them we pick a primitive $2^a$-th root of unity $\eta$. For $c \in \mathbb{Z}/2^a \mathbb{Z}$ we let let $\phi_c : T \rightarrow \mathbb{C}^*$ be the homomorphism characterized by $\phi_c(\tau) = \eta^c$, and set $V_c = \text{ind}_{Q_{a}/T}^Q \phi_c$. The conjugate representation
\( \phi_c^\sigma \) equals \( \phi_{-c} \), so unless \( \eta^c = \eta^{-c} \), that is \( c = 2^{a-1} \), one has \( \phi_c \neq \phi_c^\sigma \) and \( V_c \) is irreducible by Mackey’s criterion (theorem 5.2 on page 153). More over, since \( V_c \) and \( V_{-c} \) are conjugate representations, we obtain \( (2^a - 2)/2 = 2^a - 1 \) non-isomorphic representations in this way. All together we have found \( 2^a - 1 + 3 \) irreducible representations which is the same as the number of conjugacy classes, and this means that we have found all.

Let \( \psi_c \) denote the character of \( V_c \), it vanishes at \( \sigma \) and \( \tau \sigma \) since the classes they belong intersect \( T \) trivially, and the value at 1 equals the index of \( T \), that is 2 As \( \sigma^2 \) is central, its centralizer equal \( Q \) (obviously!!); hence the value of \( \psi_c \) on \( \sigma^2 = \tau^{2^a-1} \) equals \( 2 \phi_c(\tau^{2^a-1}) = \eta^{2^{2a-1}} = 2^{-1} \). The centralizer of \( \tau \) being \( T \) the value of \( \psi_c \) on the conjugacy class \( \{ \tau, \tau^{-1} \} \) equals \( \phi_c(\tau) + \phi_c(\tau^{-1}) = \eta^c + \eta^{-c} \). We thus have the character table of \( Q \):

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>( \sigma^2 )</th>
<th>( \tau^i )</th>
<th>( \tau \sigma )</th>
<th>( \tau )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1_Q )</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2^{-1}</td>
<td>2^{-1}</td>
</tr>
<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)^i)</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>( \chi_3 )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>( \eta )</td>
<td>( 2^{a-1} - 1 )</td>
<td>2</td>
<td>((-1)^{2^a-1})</td>
<td>( \eta^c + \eta^{-c} )</td>
<td>0</td>
</tr>
</tbody>
</table>

**Problem 5.15.** Let \( G \) be the semi-direct product of the cyclic group \( C_{2^a} = \langle \tau \rangle \) and \( C_4 = \langle \sigma \rangle \) with \( \sigma \) acting as \( \sigma \tau \sigma^{-1} = \tau^{-1} \). Show that \( \sigma^{-2} \tau^{2^a-1} \) is a central involution in \( G \) and that \( G/\langle \sigma^{-2} \tau^{2^a-1} \rangle \) is isomorphic to \( Q \).  

**Problem 5.16.** Show that \( Q_a/\mathbb{Z}(Q_a) \) is a semi-direct product \( C_{2^{a-1}} \rtimes C_2 \).  

**Problem 5.17.** Let \( k \) be a field whose characteristic is not two. Show that the Sylow 2-subgroup of \( \text{SL}(2, k) \) are generalized quaternionic.

**Proposition 5.14** Assume that every abelian subgroup of the p-group \( G \) is cyclic. Then \( G \) is either cyclic or generalized quaternionic.

**Proof:** xaxaxax

5.4.4 \( \text{SL}(2, 3) \)

The special linear group \( \text{SL}(2, q) \) over a field of \( q \) elements has \( (q - 1)q(q + 1) \) elements. It acts transitively on the projective line \( \mathbb{P}^1(q) \) with \( q + 1 \) elements.

With isotropy groups being conjugate to the group \( H \) of upper triangular matrices:

\[
H = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}
\]
5.4.5 Metabeliangulars
6

Induction theorems

In analyzing representations of a “big and complicated” group $G$ it is tempting to utilize some of the “small and easy” subgroups of $G$. In example 5.14 above we found many irreducible representations of $\text{Sl}(2, \mathbb{F}_q)$ by inducing one-dimensional representations (which are of the simplest sort) from group of triangular matrices.

The ideas of this section centre around the following general question: Which representations of $G$ are induced from subgroups? Which subgroups can be used and what type of representations can the one chose as source of the induction? The simpler subgroups and the simpler sources, the better.

It is fruitful to split the question in two, and first relax the requirements substantially and ask for what “virtual characters” are induced. Subsequently, when you have written your favorite character as an induces character you can check if the source is a character or not. It will not always be, but in any case, there is information to gain.

The setup

Given a collection $\mathcal{X}$ of subgroups of $X$ consider the map

$$\Psi_{\mathcal{X}} : \bigoplus_{H \in \mathcal{X}} \text{Ch}_Z(H) \to \text{Ch}_Z(G)$$

that sends a tuple $(\chi_H)$ to $\sum_{H \in \mathcal{X}} \text{ind}^G_H \chi_H$. What can one say about the image of $\Psi$?

It turns out to be useful to consider other coefficients than $Z$, so we shall
also use the maps of the shape

\[ \Psi_{X,R} : \bigoplus_{H \in X} \text{Ch}_R(H) \to \text{Ch}_R(G) \]

where \( R \) is a commutative ring. The group \( \text{Ch}_R(G) = \text{Ch}_Z(G) \otimes Z R \) is a free \( R \)-module, and it consists of linear combinations \( \sum a_i \chi_i \) where \( \chi_1, \ldots, \chi_r \) are the irreducible characters of \( G \) and the coefficients \( a_i \) all lie in \( R \).

Our first observation is that the image of \( \Psi_{X,R} \) is an ideal in the commutative ring \( \text{Ch}_R(G) \):

**Proposition 6.1** With notation above, the image \( \text{im} \Psi_{X,R} \) is an ideal in \( \text{Ch}_R(G) \).

**Proof:** It follows directly from the projection formula

\[ x \text{ind}_H^G(y) = \text{ind}_H^G(y \text{res}_H^G x) \]

that the image of each component of \( \Psi_{X,R} \) is an ideal, hence the image of their sum will be as well.

\( \square \)

(6.1) In the particular case that \( R = Q \), and the coefficients are rational numbers, there is an interpretation of what an equality of the form \( \chi_V = \sum a_i \chi_{V_i} \) means in terms of isomorphisms of modules. One writes \( a_i = b_i/c \) with the \( b_i \)'s and \( c \) being integers and \( c > 0 \), and then divide the \( a_i \)'s into two groups according to their sign by letting \( a_i > 0 \) for \( i \leq s \) and \( a_i < 0 \) for \( i > s \). Then the equality \( \chi_V = \sum a_i \chi_{V_i} \) of characters translates into an isomorphism

\[ cV \oplus a_{s+1} V_{s+1} \oplus \ldots \oplus a_r V_r \simeq a_1 V_1 \oplus \ldots \oplus a_s V_s \]

of representations (this follows from the fact that characters characterize representations up to isomorphism).

**Example 6.1.** Characters induced from a subgroup \( H \) assume the index \( [G : H] \) as their value at \( 1 \in G \), so in case the indices of all proper subgroups have a common factor, the map \( \Psi_{X,Z} \) cannot be surjective (albeit \( \Psi_{X,Q} \) could be) except in the uninteresting situation that \( G \) belongs to \( X \). A simple example would be any non-cyclic \( p \)-group. For example, the quaternion group \( Q_8 \) has all elements of order 2 or 4, so taking \( X \) to be the collection of all cyclic subgroups, the elements in the image \( \text{im} \Psi_{X,Z} \) will all be divisible by 2.

* 

A necessary criterion

Any induced class function a subgroup \( H \) of \( G \), vanishes on the conjugacy classes of \( G \) that do not meet \( H \). Hence a necessary criterion for \( \Psi_{X,R} \) to be
surjective is that any conjugacy class of $G$ meets at least one of the subgroups from the collection $\mathcal{X}$. Phrased slightly differently, any element $x$ must belong to a conjugate of at least one of the subgroups in $\mathcal{X}$: The conjugates of the groups in $\mathcal{X}$ must cover $G$, i.e., $\bigcup_{H \in \mathcal{X}, g \in G} H^g = G$. This property turns out to be equivalent to $\Psi_{\mathcal{X}, \mathcal{Z}}$ being surjective up to to finite groups:

**Theorem 6.1** Let $G$ be a group and let $\mathcal{X}$ be a collection of subgroups of $G$ and let $\mathbb{R}$ be a subring of $\mathbb{C}$. Then the following two conditions are equivalent:

- The conjugates of the subgroups in $\mathcal{X}$ cover $G$.
- The induction map $\Psi_{\mathcal{X}, \mathbb{R}}$ has a finite cokernel.

**Proof:** The map $\Psi_{\mathcal{X}, \mathbb{R}}$ having finite cokernel is equivalent to $\Psi_{\mathcal{X}, \mathbb{C}} = \Psi_{\mathcal{X}, \mathbb{R}} \otimes \mathbb{R} \mathbb{C}$ being surjective. Hence we consider

$$
\Psi_{\mathcal{X}, \mathbb{C}} : \bigoplus_{H \in \mathcal{X}} \text{Ch}_\mathbb{C}(H) \to \text{Ch}_\mathbb{C}(G)
$$

and assume that $\Psi_{\mathcal{X}, \mathbb{C}}$ is not surjective. The image of $\Psi_{\mathcal{X}, \mathbb{C}}$ is then a proper linear subspace, and there exists a non-zero element orthogonal to it; i.e., an element $\psi$ such that $(\psi, \text{ind}^G_H \chi) = 0$ for all $H \in \mathcal{X}$ and all characters $\chi$ of $H$. Let $H \in \mathcal{X}$. Frobenius reciprocity gives $(\psi|_H, \chi) = 0$ for all characters on $H$, since the characters form a basis for the class function on $H$, it follows that $\psi|_H = 0$. This holds for all $H \in \mathcal{X}$, and since the conjugates of the $H$’s cover $G$, we can conclude that $\psi = 0$.

The implication the other way is clear since there are class functions not vanishing at any given element $g \in G$ (e.g., the indicator function of the conjugacy class where $g$ belongs). 

### 6.1 Artin’s induction theorem

Specializing $\mathcal{X}$ in the theorem 6.1 above to be the collection of all cyclic subgroups, which obviously covers $G$, we arrive at a result of Emil Artin’s:

**Theorem 6.2** Let $G$ be a group. Any character $\chi$ on $G$ may be written as a linear combination with rational coefficients of characters induced from cyclic subgroups.

**Proof:** By theorem 6.1 above, the cokernel of $\Psi_{\mathcal{X}, \mathbb{Z}}$ is finite, hence tensorizing by $\mathbb{Q}$ kills it, and $\Psi_{\mathcal{X}, \mathbb{Q}}$ is surjective.
Example 6.2. There are easy examples that $\Psi_{X,Z}$ has a non-trivial cokernel. For example, the alternating group $A_4$, which is of order 12, has no elements of order 6. Hence the cyclic subgroups are of index 12, 6 or 4, and for any induced class function $\psi$ the value $\psi(1)$ must therefore be even. The four irreducible characters of $A_4$ are all of odd dimension, so none of them belongs to $\text{im} \Psi_{X,Z}$.

Example 6.3. We continue the previous example and shall verify that the trivial character $1_{A_4}$ cannot be expressed as a linear combinations with positive rational coefficients of characters induced from cyclic subgroups. In fact none of the three one-dimensional characters of $A_4$ can, but we leave the two others to the students.

Recall that there are four conjugacy classes in $A_4$; in addition to the trivial one, there is one containing $\sigma = (1, 2)(3, 4)$ (2a in GAP-notation), one containing $\tau = (1, 2, 3)$ (denoted 3a) and one containing $\tau = (1, 3, 2)$ (called 3b). The group $A_4$ has three cyclic subgroups of order two, all conjugate, and four cyclic subgroups of order three, also all conjugate. Finally, the seven non-trivial cyclic subgroups are all self-centralizing.

With this information, it is a matter of easy computations to find all class-functions of $A_4$ that are induced from characters of cyclic subgroups. As an illustration we do one of them, leaving the rest to the zealous students. The result is listed in a table in the margin where $w$ designates a cube root of unity.

The upper part of the table is the character table of $A_4$ and the lower part a listing of the values assumed by the six induced characters.

On the subgroup $C_2 = \langle \sigma \rangle$ of order two we consider the non-trivial character $\zeta$ taking the value $-1$ on $\sigma$. Using the formula in corollary 5.3 on page 142 one finds for $y \in 2a$ that

\[ \text{ind}_{C_2}^{A_4} \zeta(y) = |C_G(y)| |H|^{-1} \sum_{x \in C_G y \cap H} \chi_V(x) = 4 \cdot 2^{-1} \zeta(\sigma) = -2. \]

The induced character $\text{ind}_{C_2}^{A_4} \zeta$ assumes the value 6 at 1 and vanishes on the classes 3a and 3b.

Now, let $\zeta_i$ for $1 \leq i \leq 6$ be the induced characters as listed from top to bottom in the table, and assume that $1_{A_4} = \sum_{1 \leq i \leq 6} a_i \zeta_i$. From the two first columns we infer the two constraints

\[ -2a_2 + 2a_3 = 1, \]
\[ 12a_1 + 6a_2 + 6a_3 + 4a_4 + 4a_5 + 4a_6 = 1, \]

which combine to

\[ 12a_1 + 8a_2 + 4a_3 + 4a_4 + 4a_5 + 4a_6 = 0. \]
Obviously this can not be satisfied solely with positive $a_i$’s.

**Problem 6.1.** Check that neither the two other one-dimensional characters of $A_4$ are positive rational combinations of the induced $\zeta_i$’s.

A more specific version of Artin’s theorem

There is a more specific version of Artin’s theorem including an estimate of the size of the cokernel. It says that admitting the order $|G|$ as denominators in the coefficients will suffice:

**Theorem 6.3** Let $G$ be a group. Any virtual character $\chi$ on $G$ may be written as a linear combination

$$|G| \chi = \sum_{A \subseteq G} n_A \text{ind}_G^A \chi|_A$$

where the $n_A$’s are integers and the summation extends over all cyclic subgroups $A$ of $G$.

In view of the projection formula (proposition 6.1 on page 164) if we can show that $|G| \cdot 1_G$ belongs to the image of $\Psi_{\mathcal{X}, Z}$, with $\mathcal{X}$ being the collection of cyclic subgroups, $|G| \cdot \psi$ of any virtual character $\psi$ would lie there, and the theorem follows.

There is an explicit expression for $|G| \cdot 1_G$ as an integral combination of characters induced from cyclic subgroups. It involves the following class function, which in turns out to be a virtual character, defined on cyclic groups $A$, by

$$\theta(x) = \begin{cases} |A| & \text{if } x \text{ generates } A \\ 0 & \text{otherwise} \end{cases}$$

**Example 6.4.** To understand the function $\theta_A$ better, we begin with an example. Recall that the order of the day when inducing in abelian groups is: “Extend by zero and scale by index!” Our example is the cyclic group $A$ of prime power order, say $p^n$. The elements that do not generate $A$ are those lying in the subgroup $B$ of $p$-th powers. Hence

$$\theta_A = p^n \cdot 1_A - p^{n-1} \cdot \text{ind}_B$$

Indeed, $p^n \cdot 1_A$ assumes the value $p^n$ everywhere. The induced character $\text{ind}_B$ takes the value $p$ on $B$ and vanishes off $B$ so that the second term cancels the first along $B$.

In the second example we consider a cyclic group of order $pq$ where $p$ and $q$ are two different primes. It can be written as $AB$ where $A$ and $B$ are of order
$p$ and $q$ respectively, and $A$ and $B$ are the two only maximal proper subgroups.

hence an element $x \in AB$ generates $AB$ if and only it does not lie in the union $A \cup B$. The character $\theta_{AB}$ is therefore $pq \cdot \delta_{AB \setminus A \cup B}$, and one has

$$
\theta_{AB} = pq \cdot 1_{AB} - p \cdot \text{ind} \ 1_B - q \cdot \text{ind} \ 1_A + pq \cdot \text{ind}_{\{1\} \setminus \{1\}} 1_{\{1\}}
$$

the last term being there to compensate for having subtracted the contributions from $A \cap B$ twice.

The salient property of the functions $\theta_A$ is expressed in the following proposition:

**Proposition 6.2** It holds true that

$$
|G| \cdot 1_G = \sum_{A \subseteq G} \text{ind}_A^G \theta_A
$$

where the summation extends over all cyclic subgroups of $G$.

**Proof:** Let $A \subseteq G$ be a cyclic subgroup and let $y \in G$ be any element. The formula in corollary 5.2 on page 142 reads

$$
\text{ind}_A^G \theta_A(y) = |A| \sum_{x \in G} \theta_A(x) = |A|^{-1} \sum_{yxy^{-1} \text{ generate } A} |A| = \sum_{yxy^{-1} \text{ generate } A} 1
$$

Subsequently when summing over all cyclic subgroups, the result follows since any element $yxy^{-1}$ generates just one subgroup.

**Proposition 6.3** Let $A$ be a cyclic group. The function $\theta_A$ is a linear combination of functions of the shape $\text{ind}_B^A 1_B$ with $B \subseteq A$ and integral coefficients; that is one has

$$
\theta_A = \sum_{B \subseteq A} n_B \text{ind}_B^A 1_B
$$

where $n_B \in \mathbb{Z}$, and where the summation extends over all (cyclic) subgroups of $A$. In particular, $\theta_A$ is a virtual character.

**Proof:** From proposition 6.2 above one has $|A| = \sum_{B \subseteq A} \text{ind}_B^A \theta_B$. The term in the sum corresponding to $B = A$ is of curse equal to $\theta_A$, and for the others the order of $B$ is less than the order of $A$. By induction we may assume that for those $B$’s one has

$$
\theta_B = \sum_{C \subseteq B} n_{BC} \text{ind}_C^B 1_C.
$$

The transitivity of induction then yields

$$
\theta_A = |a| \cdot 1_A - \sum_{C \subseteq B} n_{CB} \text{ind}_C^A 1_C
$$

where the sum extends over all pairs $C \subseteq B$ of subgroups. Grouping together the $C$’s that are equal yields the proposition.
Combining the two last propositions one obtains the following version of Artin’s induction theorem:

**Proposition 6.4** Let \( G \) be a group. There is a linear combination

\[
|G| \cdot 1_G = \sum_{A \subseteq G} n_A \text{ind}^G_A 1_A
\]

where \( n_A \in \mathbb{Z} \) and the summation extends over all cyclic subgroups \( A \) of \( G \).

An explicit formula for \( \theta_A \)

It might be of interest to see a closer description of the character \( \theta_A \), and there is a complete explicit formula for it.

Let \( A \) be a cyclic group. The partially ordered set of subgroups of \( A \) is the same as the partially ordered set of divisors of \( |A| \). Hence the maximal, proper subgroups correspond to the maximal, proper divisors of \( |A| \); that is, those divisors \( d \) such that \( |A|/d \) are prime.

Let \( \{A_i\}_{i \in I} \) be the set of maximal subgroups of \( A \). The quotients \( A/A_i \) are of prime index, say \( p_i \). The point is the tautology that an element \( x \in A \) generates \( A \) if and only if it is not contained in any of the maximal proper subgroups \( A_i \), and this means that we can express \( \theta_A \) as a multiple of the indicator function of the complement of the union \( \bigcup_i A_i \); that is, it holds true that \( \theta_A = |A| \delta_{A \setminus \bigcup_i A_i} \).

For any subset \( J \subseteq I \) we denote by \( A_J \) the intersection \( \bigcap_{j \in J} A_j \). It is a subgroup of index \( p_J = \prod_{j \in J} p_i \). With this notation in place the following nice formula holds true:

\[
\theta_A = \sum_{J \subseteq I} (-1)^{|J|} |A_J| \text{ind}^A_{A_J} 1_{A_J}.
\]

The proof is a combinatorial “include-exclude” argument. The function \( \text{ind}^A_{A_J} 1_{A_J} \) is supported along \( A_J \) and assumes the constant value \([A : A_J]\) there, hence it equals \([A : A_J] \delta_{A_J}\). The right side of the formula above takes shape

\[
|A| \sum_{J \subseteq I} (-1)^{|J|} \delta_{A_J} = |A| \delta_{A \setminus \bigcup_i A_i} = \theta_A
\]

where the first equality is the classical “inclusion-exclusion” formula (see exercise 6.2 below).

**Problem 6.2.** Assume that \( \{X_i\}_{i \in I} \) is a finite set of subsets of a set \( X \). Let for each \( J \subseteq I \) let \( X_J \) denote the intersection \( \bigcap_{j \in J} X_j \) and let \( Y \) be the complement of the union \( \bigcup_{i \in I} X_i \). Prove that the indicator function of \( Y \) satisfies the relation

\[
\delta_Y = \sum_{J \subseteq I} (-1)^{|J|} \delta_{X_J}.
\]

**Hint:** One has \( \delta_Y = \prod_i (1 - \delta_{X_i}) \)
Problem 6.3. Show that

\[ 1_G = \sum_{B \subseteq G} [G : B]^{-1} \sum_{A \supseteq B} \mu([A : B]) \text{ind}_{B}^{G} 1_B \]

where \( A \) and \( B \) are cyclic subgroups of \( G \) and \( \mu \) is the Möbius function from number theory.\(^1\)

The map \( \Psi_{X,R} \) is not injective. There are two obvious classes of elements in the kernel.

6.2 Brauer’s theorem

The denominator in coefficients in Artin’s theorem are inevitable if one insists on using the collection of cyclic subgroups as the groups one induces from. However, relaxing that requirement, and using a larger collections \( X \) of subgroups, one can represent characters as integral linear combinations of induced characters from groups in \( X \).

The class of subgroups that figures in Brauer’s theorem consists of the so-called *elementary* subgroup. They are groups isomorphic to a product \( C \times P \) of a \( p \)-group \( P \) and a cycle group whose order is prime to \( p \). If one wants to put emphasis on the prime \( p \) one says that the group \( C \times P \) is \( p \)-elementary. We let \( E \) denote the class of elementary subgroups of \( G \).

There is also a great interest in limiting the type of the characters needed to induce. One wants them as simple as possible, the optimal being the one-dimensional ones, and those are exactly which appears in Brauer’ theorem:

\[ \text{Brauer Induction} \]

\[ \text{Theorem 6.4 (Brauer’s induction theorem)} \] Let \( G \) be a group. Every virtual character is an integral linear combinations of characters induced from one-dimensional characters on elementary subgroups.

There are several approaches to Brauer’s theorem and we follow the one by Goldschmidt and Isaacs. The proofs are somehow involved, with several steps and reductions. The first reduction is the observation that elementary groups are supersolvable (see section 6.4 on page 179), and hence all their representation are induced from one-dimensional ones (proposition 6.8 on page 179). Hence it suffices to see that every virtual character on \( G \) is an integral linear combinations of characters induced from elementary groups, regardless of the

\[^1\] One has

\[ \mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if for some } p, p^2 | n, \\ (-1)^r & \text{if } n = p_1 \ldots p_r \end{cases} \]

where \( p \) designates a prime and the \( p_i \)'s are distinct primes.
shape of those characters. In other words it will be enough to show that the map

$$\Psi_{\mathcal{E}, \mathcal{Z}} : \bigoplus_{H \in \mathcal{E}} \mathrm{Ch}_{\mathcal{Z}}(H) \to \mathrm{Ch}_{\mathcal{Z}}(G)$$

is surjective.

**Example 6.5.** With every element $x \in G$ there is associated a $p$-elementary group $E(x)$ unique up to conjugacy by elements in the normalizer $N_G(x)$. The cyclic group $C$ involved is generated by be the $p'$-part $x'$ of $x$. To lay hands on the $p$-group $E(x)$ consider the centralizer $C_G(x')$ of $x'$ and let $P \subseteq C_G(x')$ be a Sylow $p$-subgroup of $C_G(x')$. Then $E(x) = C \cdot P \simeq C \times P$ is $p$-elementary. The subgroup $E(x)$ is a maximal $p$-elementary group containing $x'$ in the sense that a conjugate of any other $E$ is contained in $E(x)$.

Another class of subgroups that intervenes in the proof, are the so called *hypo-elementary* groups. They are slightly less elementary than the elementary ones (hence the name²), and form a slightly larger class. A hypo-elementary group is the product $CP$ of a $p$-subgroup $P$ and a normal, cyclic group $C$ of order prime to $p$, but—contrary to elementary groups—the subgroups $C$ and $P$ are not required to commute. Thus a hypo-elementary group $G$ is the semidirect product $C \rtimes P$ and sits in a split exact sequence

$$1 \to C \to G \to P \to 1.$$  \hspace{1cm} (6.1)

The class of hypo-elementary subgroups of $G$ will be denoted by $\mathcal{H}$.

**Lemma 6.1** If $P$ is a $p$-group and the order $|C|$ is prime to $p$, any sequence like (6.1) is split and $G \simeq C \rtimes P$.

**Proof:** Let $Q$ be a Sylow $p$-subgroup. The order $|C|$ is prime to $p$ and $|G| = |C| |P|$ so that $|Q| = |P|$. The restriction $\pi|_Q$ is injective since $Q \cap C = \{1\}$ (the order of one being prime to $p$ and of the other a power of $p$). Consequently $\pi(Q) = P$ and the sequence splits.

**Example 6.6.** In complete analogy to example 6.5 one may associated with
any element $x \in G$ and any prime $p$ a $p$-hypo-elementary group $H(x)$. Indeed, denote by $C$ the cyclic subgroup $C = \langle x' \rangle$ generated by the $p'$-part of $x$. Choose a Sylow $p$-subgroup $P$ of the normalizer $N_G(C)$ of $C$ and let $H(x) = C \cdot P$. Then $C$ is normal in $H(x)$ and $C \cap P = \{1\}$ so that $H(x)$ is the semi-direct product $C \rtimes P$.

The class of hypo-elementary groups has the nice property of being closed under the formation of subgroups and quotients:

**Proposition 6.5** Subgroups and quotients of hypo-elementary (resp. elementary) groups are hypo-elementary (resp. elementary).

**Proof:** Assume that $G$ is hypo-elementary and write $G = CP$ with $C$ and $P$ as above; i.e., $P$ is a $p$-group and $C$ a normal, cyclic subgroup whose order is prime to $p$. There is an exact sequence

$$1 \longrightarrow C \longrightarrow G \xrightarrow{\pi} P \longrightarrow 1.$$ 

Let $H \subseteq G$ be a subgroup, and put $P' = \pi(P)$ and $C' = C \cap H$. They fit into the exact sequence

$$1 \longrightarrow C' \longrightarrow G \xrightarrow{\pi} P' \longrightarrow 1.$$ 

and in view of lemma 6.1 above we are through.

To see that $H$ is elementary whenever $G$ is, notice that if the action of $P$ on $C$ is trivial, the action of the smaller group $P'$ will trivial as well.

As to quotients $H$ of $G$, the images of $C$ and $P$ in $H$ serve as the special subgroups.

6.2.1 **Brauer for hypo-elementary groups**

Our first step is to prove Brauer’s theorem for hypo-elementary groups; the map $\Psi_{E,Z}$ is surjective, or in words:

**Proposition 6.6** Let $G$ be a hypo-elementary group. Every virtual character is an integral linear combination of characters induced from characters on elementary subgroups.

**Proof:** The proof goes by the usual induction on the order of $G$.

By hypothesis $G$ is hypo-elementary and therefore of the form $G = C \cdot P$ with $P$ a $p$-group and $C$ a normal, cyclic subgroup of order prime to $p$.

The centralizer of $P$ in $C$ is denoted by $Z$. It is made up of the elements $x \in C$ such that $xy = yx$ for all $y \in P$, or phrased slightly different manner it si the
set of fixed point in \( C \) of \( P \) acting on \( C \) by conjugation. Put \( H = ZP \cong Z \times P \), it is an elementary subgroup of \( G \) that will play a special role\(^3\) in his proof. We begin with decomposing the induced \( \text{ind}_G^H 1_G \) into irreducibles

\[
\text{ind}_G^H 1_G = 1_G + \sum_i \chi_i
\]

and observe that \( 1_G \) appears with multiplicity one.

By induction on the order of \( |G| \) and by the projection formula, we will be through once we can show that all the irreducible constituents \( \chi_i \) are induced from proper subgroups.

We shall restrict \( \text{ind}_G^H 1_G \) to the cyclic subgroup \( C \), and for that we use Mackey’s decomposition formula. As \( G = CH \), there is no other double cosets, and Mackey formula reads

\[
(\text{ind}_G^H 1_G)|_C = \text{ind}_C^C \cap H = \text{ind}_C^C 1\Z.
\]

hence

\[
\text{ind}_C^C 1\Z = 1_C + \sum_i \chi_i|_C
\]

and it follows that

\[
(\chi_i|_C, 1\Z) = (\chi_i|_C, \text{ind}_C^C 1\Z) \geq (\chi_i|_C, \chi_i|_C) > 0,
\]

but \( \chi_i|_C \neq 1_C \) because \( (\text{ind}_C^C 1\Z, 1_C) = (1\Z, 1\Z) = 1 \).

Let \( \chi \) be one of the \( \chi_i \)'s and assume it is not induced from a proper subgroup. Clifford’s theorem tells us that the restriction \( \chi|_C \) then is isotypic. Hence, since \( C \) cyclic, it holds that \( \chi = n\lambda \) for some one-dimensional character \( \lambda \). The character \( \lambda \) must be invariant under the entire group \( G \); indeed, \( \lambda \) is invariant under the isotropy group \( G_{\lambda} = \{ x \mid \lambda^x = \lambda \} \) and \( \chi = \text{ind}_G^C \lambda \), and having assumed that \( \chi \) is not induced from a proper subgroup, we infer that \( G_{\lambda} = G \). Moreover, since \( (\chi|_Z, 1\Z) \neq 0 \) it holds true that \( \lambda|_Z = 1\Z \). Let \( K = \ker \lambda \), then \( Z \subseteq K \). The character \( \chi \) therefore descends to \( G/Z \), and if \( Z \) were non-trivial, induction would give that \( \chi \) was induced from a proper subgroup. So \( Z = \{1\} \).

Being multiplicative, the character \( \lambda \) assumes constant and different values on the different cosets \( zK \) of \( C \). (when \( z \in K \) on has \( \lambda(xz) = \lambda(x)\lambda(z) = \lambda(x) \) and \( \lambda(x) = \lambda(y) \) entails that \( \lambda(xy^{-1}) = 1 \)). Now, \( \lambda \) is invariant under \( G \) and therefore the cosets \( zK \) must be invariant under the action of \( P \) on \( C \). Now if the coset \( zK \) is non-trivial, \( i.e. \), different from \( K \), the order \( |zK| \) is prime to \( p \), and the \( p \)-group \( P \) has a fixed point in \( zK \); that is, for at least for one \( w \in zK \) and all \( s \in P \) one has \( s\omega s^{-1} = \omega \). Finally, we know that \( K \) is different from \( C \), so that there are non-trivial cosets, and we have exhibited non-trivial elements in \( Z \). Absurd!

\[Q.E.D.\]
Example 6.7. It is worthwhile to see what happens in the case of $A_4$. The subgroup $K = C_2 \times C_2$ is of index three, and if $\rho$ is any of the non-trivial one-dimension characters on $K$, the value of the induced character $\text{ind}_{A_4} K \rho$ on the conjugacy class $2a$ is given as

$$\text{ind} \rho = 4 \cdot 4^{-1}(+1 - 1 - 1) = -1,$$

whereas on the unit element $1 \in A_4$ naturally $\text{ind} \rho$ assumes the value 3 and it vanishes on the classes $3a$ and $3b$ that do not meet $K$. So $\psi = \text{ind} \rho$. And e.g., $1_{A_4} = \text{ind} 1_{C_3} - \text{ind} \rho$ where $C_3$ is cyclic subgroup of order three.

Louis Solomon’s theorem

Lemma 6.2 Let $X$ be a finite set and let $L_\mathbb{Z}(X)$ denote the ring of functions on $X$ with integral values. If $R \subseteq L_\mathbb{Z}(X)$ is a subring not containing the constant function $1_X$, then for some prime $p$ and some element $x \in X$ it holds true that $p|f(x)$ for all $f \in R$.

Proof: The set $I_x = \{ f(x) \mid f \in A \}$ with $x \in X$ are all in $\mathbb{Z}$, and the conclusion of the theorem is that at least one of them is a proper ideal. If not, there is for every $x$ a function $f_x$ such that $f_x(x) = 1$. Then

$$\prod_{x \in X} (f_x - 1_X) = 0$$

and multiplying out this product shows that $1_X \in R$. \hfill \Box

Theorem 6.5 (Solomon’s induction theorem) Let $G$ be a group. Then there is an expression

$$1_G = \sum_E a_E \text{ind}_E^G 1_E$$

where $E$ extends over the collection of hypo-elementary subgroups and $a_E \in \mathbb{Z}$. Consequently, any virtual character on $G$ is an integral linear combination of characters induced from hypo-elementary subgroups.

The second statement in the theorem follows as usual from the first since the images of the maps $\Psi_{X,Z}$ are ideals.
**Proof:** The first observation is that the subset of $\text{Ch}_Z(G)$ of integral linear combinations of characters induced from trivial representations on hypo-elementary subgroups is a subring. This follows from exercise 5.13 on page 155 with $V = 1_H$ and $W = 1_K$.

So with the lemma 6.2 above in mind, we have to show that for any $x \in G$ and any $p$ there is hypo-elementary subgroup $H$ of $G$ such that $p$ does not divide $\text{ind}_H^G 1_H(x)$. The hypo-elementary group that will do the job, is the group $H(x)$ from example 6.6 on page 171. That is, the semi-direct product $C \cdot P$ with $C = < y >$, where $y$ is the $p'$-part of $x$, and $P$ a Sylow $p$-subgroup of the normalizer $N = N_G(C)$.

Our task is to compute the value of $\chi = \text{ind}_H^G 1_H$ at $x$, or at least see that $\chi(x) \not\equiv 0 \mod p$. Now, the representation $\text{ind}_H^G k_H$ is nothing but the permutation representation built on the action of $G$ on the set $G/H$ of left cosets, and the value its character assumes at $x$ equals the number of fixed points of the action of $x$ on $G/H$.

We shall establish that $x$ has as many fixed points on $G/H$ as on $N/H$. To that end, consider the natural inclusion $N/H \subseteq G/H$, which (since $x \in N$) is invariant under the multiplication by $x$. A fixed point in $G/H$ is a coset $gH$ with $xgH = gH$, in other words a coset whose representative $g$ satisfies the equality $g^{-1}xg \in H$. But then $g^{-1}Cg \subseteq g^{-1}xg \subseteq H$, and since $C$ is the only subgroup in $H$ of order $|C|$, it holds true that $g^{-1}Cg = C$, and we infer that $g \in N$. Hence all fixed points in $G/H$ lie in $N/H$.

To proceed, recall that $x = zy$ where $z$ denotes the $p$-part of $x$ and $y$ is the $p'$-part. Now, $y \in H$ by the construction of $H$, and $y$ acts trivially on $N/H$. Hence, the actions of $x$ and $z$ has the same fixed points in $H/N$. The element $z$ being a $p$-element, the classical orbit-stabilizer formula entails that the number of fixed points of $z$ is congruent $|N/H|$ modulo $p$, but as $H$ contains a $p$-subgroup of $N$, we know that $|N/H| \not\equiv 0 \mod p$. And we are through. 

**6.3 Some Consequences of the induction theorems**

**Under arbeid.** The induction theorems have many applications in several fields of mathematics. We include two of the more known. The first is a criterion for a class function being a virtual character and the second is about realization of complex representations over cyclotomic fields.

**Brauer’s criterion for virtual characters**

The space of class functions $\text{Cfu}_G$ on the group $G$ is a complex vector space. It has the set of irreducible characters $\{\chi_i\}$ as a basis and the elements are linear
combinations of these with complex coefficients; moreover $\text{Cfu}_G$ is equal to $\text{Ch}_C(G)$. Inside $\text{Cfu}_G$ lies the subgroup $\text{Ch}_Z(G)$ of \textit{virtual characters}, which consists of the linear combinations of the $\chi_i$'s with \textit{integral} coefficients, so it lies like a lattice within $\text{Ch}_C(G)$, \textit{i.e.}, like the points in $\mathbb{C}$ all whose coordinates are integers. Given any element $\alpha \in \text{Cfu}_G$, it is \textit{a priori} not easy to decide if a class function $\alpha$ lies in $\text{Ch}_Z(G)$ or not— that is, if $\alpha$ is a virtual character or not—and a criterion for this is of interest.

**Proposition 6.7** Let $\alpha$ be a complex class function on $G$. Then $\alpha$ is a virtual character if and only if the restriction $\alpha|_E$ is a virtual character for all elementary subgroups $E$ of $G$.

**Proof:** Virtual characters restrict to virtual characters, so one implication is clear. Assume therefore that $\alpha|_E \in \text{Ch}_Z(E)$ for all elementary $E \subseteq G$. By Brauer’s induction theorem, one can write

$$1_G = \sum_{E \in \mathcal{E}} n_E \text{ind}_E^G \psi_E$$

with the the coefficients $n_E$ being integers and the $\psi_E$'s being characters on $E$. Applying the projection formula (for class functions) we infer the equality

$$\alpha = \sum_{E \in \mathcal{E}} n_E \text{ind}_E^G (\alpha|_E \cdot \psi_E).$$

But by hypothesis $\alpha|_E \cdot \psi_E$ is a virtual character (the product of two such is one), and the induction $\text{ind}_E^G (\alpha|_E \cdot \psi_E)$ is a virtual character as well. \qed

**Realization over cyclotomic fields**

Given a complex representation $V$ of a group $G$. For a subfield $K \subseteq \mathbb{C}$ we say that $V$ is \textit{defined} over $K$ or is \textit{realized} over $K$, if there is basis for $V$ in which the matrices of $\rho_V(x)$ all have entries in $K$. One may ask about the smallest field over which it can be realized. As a question about modules it takes the following form: Over which fields $K \subseteq \mathbb{C}$ can we find a representation $V_0$ of $G$ such that $V \simeq V_0 \otimes K \mathbb{C}$?

If $n$ denotes the exponent of $G$, all the eigenvalues of the endomorphisms $\rho_V(x)$ lie in the cyclotomic field $\mathbb{Q}(n)$, and a tantalizing thought would be that the representation itself is realized over $\mathbb{Q}(n)$. This was a long standing conjecture, and was first proven by Brauer in the 1950’s after he had established his induction theorem.

We begin by preparing the ground with some easily lemmas:

**Lemma 6.3** If $HG$ and $V$ is a representation of $H$ defined over $K$, then $\text{ind}_H^G V$ is defined over $K$ as well.
Proof: Let \( r \) be the index of \( H \) in \( G \) and \( n \) the dimension of \( V \). The induced module \( W = \text{ind}_{0}^{G} V \) is represented as the direct sum of vector spaces

\[
W = \bigoplus_{s \in S} sV,
\]

where the sum extends over an exhaustive list \( S \) of representatives of the left cosets of \( H \) in \( G \). As vector spaces the spaces \( sV \) are all equal to \( V \), but they are lying inside \( k[G] \otimes_{k[H]} V \) as \( s \otimes V \). Fix a basis \( \{ v_{i} \}_{i \in I} \) for \( V \) in which the matrices of \( \rho_{V}(x) \) all have entries in \( Q(n) \), and consider the basis \( \{ s \otimes v_{i} \} \) with \( s \in S \) and \( i \in I \) for \( W \). A basis is an ordered set of elements, so chose any ordering of \( S \), and order \( \{ s \otimes v_{i} \} \) “lexicographically” with elements from \( s \) being the first letter; that is, the pair \( (s, i) \) comes before \( (s', i') \) if \( s < s' \) or \( s = s' \) and \( i < i' \).

Pick an element \( g \in G \). The task is to describe the matrix of \( g|_{W} \) in this basis, and see it has entries in \( K \). To that end, let \( sH \) be a residue class, and write \( gs = s'h \) with \( s' \) in \( S \). Then \( g|_{W} \) maps \( sV \) to \( s'V \) and has the matrix of \( \rho_{V}(h) \) as matrix in the bases \( \{ s \otimes v_{i} \} \) and \( \{ s' \otimes v_{i} \} \) of respectively \( sV \) and \( s'V \), and this matrix has entries in \( Q(n) \). Now, the \( nr \times nr \)-matrix of \( g|_{W} \) has block decomposition into \( n \times n \)-blocks, the blocks being indexed by pairs \( (s, s') \in S \times S \), and the blocks under \( \{ s \otimes v_{i} \} \) are all zero except the one corresponding to \( \{ s' \otimes v_{i} \} \) which is the matrix of \( \rho_{V}(g) \). So clearly, the entries belong to \( K \).

A way of understanding this matrix is to start with the matrix of the permutation representation of \( G \) on \( k[G/H] \) in the basis \( S \). It is an \( r \times r \)-matrix with exactly one 1 in each row and column and zeros everywhere else. The one is placed at \( (s, s') \) if \( g|_{k[G/H]} \) maps \( sH \) to \( s'H \), that is if \( gs = s'h(s, s') \) for an element \( h(s, s') \in H \). Then “expand” each entry to an \( n \times n \)-matrix according to the rules: A zero expands to the zero-matrix and a 1 placed at \( (s, s') \) expands to the matrix \( h(s, s') \). The expanded matrix is the matrix of \( \rho_{W}(g) \).

The second lemma we shall need is a kind of cancellation property, from a representation defined over a field \( K \) you split off factors defined over \( K \) with out losing realization over \( K \). The lemma is true for any pair of friendly fields, one contained in the other, but we stick to \( C \) and subfields \( K \) of \( C \). Recall the notation \( V^{C} \) for \( V \otimes_{K} C \) where \( V \) is a representation of \( G \) over \( K \).

**Lemma 6.4** Assume that \( K \) is a subfield of \( C \). Let \( V \) and \( W \) be representations over \( K \) and let \( U \) be a complex representation. Assume that \( U \oplus V^{C} \simeq W^{C} \). Then \( U \) is defined over \( K \) as well, i.e., there is an \( U_{0} \) over \( K \) with \( U = U_{0}^{C} \).

Proof: Let \( V = X \oplus Z \) and \( W = Y \oplus Z \) where \( X \) and \( Y \) are without common irreducible components. Then \( \text{Hom}_{C}(Y, X) = 0 \), and hence \( \text{Hom}_{C}(Y^{C}, X^{C}) = 0 \).
as well. On the other hand one has
\[ V \oplus X^C \oplus Z^C \simeq Y^C \oplus Z^C, \]
and therefore
\[ V \oplus X^C \simeq Y^C. \]
But since there are no non-zero maps from \( Y^C \) to \( X^C \) we infer that \( X = 0 \).

**Example 6.8.** We finish this sequence of lemmas by an example. It can very well happen that a multiple \( nU \) of a complex representation \( U \) is defined over a smaller field \( K \), but the representation \( U \) itself is not. This illustrates the strength of Brauer’s induction theorem compared to Artin’s. The extra energy put into the proof to get rid of the denominators pays off!

The simplest example of such a situation is found among the representations of the quaternion group \( Q_8 \) whose character table we have reproduced in the margin. The quaternion group has an irreducible representation defined over \( \mathbb{Q} \) of dimension four, namely the rational quaternions \( \mathbb{H} = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k \), with the triplets \( i, j \) and \( k \) satisfying the usual quaternionic relations (see examples 4.6 on page 95 and 3.1 on page 52), but \( \mathbb{H} \otimes \mathbb{Q} \mathbb{C} \) splits at the sum of two copies of the representation \( U \) having the character \( \chi_4 \) in the table. Indeed, it is easy to compute the character of \( \mathbb{H} \). Clearly \( \chi_\mathbb{H}(\pm 1) = \pm 4 \) that takes care of the values on the classes \( 1a \) and \( 2a \), and it easy to see that \( \chi_\mathbb{H} \) vanishes on the three other classes (the matrix of multiplication by \( i \) in the basis \( 1, i, j, k \) is given in the margin).

With the lemmas in place we are ready to attack Brauer’s realization theorem:

**Theorem 6.6** Let \( n \) be the exponent of \( G \). Then every complex representation of \( G \) can be realized over the cyclotomic field \( \mathbb{Q}(n) \).

The theorem is in some sense optimal in that there are groups requiring the full cyclotomic field. The simplest example being a cyclic group of order \( n \). However, many groups have all there representations defined over smaller fields. The symmetric groups are classical and important examples of such groups. Their representations are all defined over the rationals \( \mathbb{Q} \).

**Proof of Theorem 6.6:** By Brauer’s induction theorem (theorem 6.4 on page 170) one has
\[ \chi_U = \sum_{E \in \mathcal{E}} n_E \text{ind}_E \lambda_E \]
where in this context what is significant, is that the $\lambda_E$’s all are characters of one-dimensional representations $L_E$ and the $n_E$’s are integers. The exponent of each subgroup $E$ divides $n$ and the one-dimensional representation $L_E$ is therefore defined over $\mathbb{Q}(n)$. Moreover, as states in lemma 6.3 above, induced representations of representations defined over $\mathbb{Q}(n)$ persist being defined over $\mathbb{Q}(n)$, so each of the summands $\text{ind} G E \lambda_E$ is the character of a representation defined over $\mathbb{Q}(n)$. Separating the terms in the sum with a negative coefficients from those with positive, we arrive at an equality like

$$U \oplus V \simeq W,$$

where $V$ and $W$ are complex representations of $G$ defined over $\mathbb{Q}(n)$, and by lemma xxx we are done.

6.4 Supersolvable groups

Among the many “superobjects” in mathematics one has the supersolvable groups—the name means that they are “more solvable” than solvable groups! They possess an ascending sequence of normal subgroups $\{G_i\}_{0 \leq i \leq r}$ with $G_0 = 1$ and $G_r = G$ such that the subquotients $G_{i+1}/G_i$ are cyclic of prime order; in other words $G$ is obtained through a sequence of extensions

$$1 \longrightarrow \mathbb{C}_{p_i} \longrightarrow G/G_i \longrightarrow G/G_{i+1} \longrightarrow 1$$

where each $p_i$ is a prime. The difference from solvable groups being that the subgroups $G_i$ are required to be normal in $G$ where as for a solvable group on merely demands that $G_i$ be normal in $G_{i+1}$.

Every $p$-group is supersolvable as any nilpotent group is. One need not go further than to the alternating group $A_4$ to find a solvable groups that is not supersolvable; indeed, $A_4$ has merely non-normal cyclic subgroups that are proper and non-trivial. There are four conjugate subgroups of order three (each fixing a letter), and each of them acts transitively on the set of involutions (of which there are three, the permutations of the form $(ab)(cd)$ so there are no normal subgroups of order two either.

(6.1) Non-abelian supersolvable groups always contain normal, abelian subgroups not lying in the centre; indeed, if $Z \subseteq G$ is the centre of $G$, the quotient $H = G/Z$ has a composition series whose first element $H_1$ is cyclic. The inverse image in $G$ of $H_1$ is normal and abelian.

**Proposition 6.8** If $G$ is supersolvable any complex, irreducible representation is induced from a one dimensional representation of a subgroup. That is $V = \text{ind} G/H L$ for some subgroup $H \subseteq G$ and some one-dimensional $H$-module $L$. 
Proof: The statement is trivial if $G$ is abelian. The proof goes by induction on the order $|G|$ of $G$, so we may assume that $V$ is faithful—if not, its kernel $N$ would be a normal, proper subgroup and $V$ would be defined as $G/N$-module; with the help of problem 5.9 on page 149 we could conclude by induction. So, let $A$ be a normal, abelian subgroup of $G$ not contained in the centre. Then $V$ being faithful $V|A$ is not isotypic, and hence there proposition ?? above, there is a proper subgroup $H \subseteq G$ and an $H$-module $W$ with $V = \text{ind}_{G/H} W$, and we are through by induction.

(6.2)—Monomial representations. Representations of shape $\text{ind}_{G/H} L$ with $L$ one-dimensional are said to be monomial. They are much simpler in structure than generic ones, although not as simple as permutation representations. In an appropriate basis, their matrices can be factored as $\rho(x) = D_x P_x$ with $D$ diagonal and $P$ a permutation matrix. The decomposition is unique as one easily sees (each row and each column of $\rho(x)$ has only one-zero element equal to the diagonal element on the same row). One has $\rho(xy) = D_x P_x D_y P_y = D_x (P_x D_y P_x^{-1}) P_y$, and since $(P_x D_y P_x^{-1})$ is diagonal (permutation matrices merely permutes basis elements), it follows by uniqueness of the factorization that $P_{xy} = P_x P_y$. Hence $P$ defines a permutation representation. What just did is just a matrix-version of the decomposition of $\text{ind}_{G/H} L = \bigoplus_{x \in G/H} xL$. Monomial representations
7

Frobenius Groups

Very preliminary version 0.0 as of 14th November, 2017
Just a sketch and will change

A Frobenius group $G$ is a special type of permutation groups. It acts transitively on a set $X$ with the property that only the identity fixes more than one element in $X$. In terms of the isotropy groups of the action this means that two different isotropy groups only have the unit element in common; that is, it holds that $G(x) \cap G(y) = \{1\}$ whenever $x$ and $y$ are distinct elements from the set $X$.

Every transitive action of $G$ is isomorphic to the natural action of $G$ on the set $G/G(x)$ of left cosets of one of the isotropy groups. Renaming $G(x)$ to $H$, we thus get the following equivalent definition of a Frobenius group: The group $G$ is a Frobenius group if and only if it possesses a subgroup $H$ such that $H^t \cap H = \{1\}$ for any element $t$ not in $H$. The subgroup $H$ is called a Frobenius complement of $G$.

Except the unit element, the elements in $G$ either have one fixed point in $X$, which is the case for elements in $\bigcup H^t$, or they act without fixed points. The latter form together with the unit element $1$ a subset of $N$ called the Frobenius kernel of $G$, that is

$$N = \{ g \in G \mid g \notin H^t \text{ for any } t \} \cup \{1\}.$$ 

A remarkable and famous theorem of Frobenius states that the Frobenius kernel is a subgroup. It is a normal subgroup such that $G = NH$ and $N \cap H = \{1\}$, and hence $G$ is the semidirect product of $N$ and $H$.

Historically the Frobenius result was the first of a long series leading up to the herostratically famous odd-order-theorem of Feit and Thompson stating that any finite group of odd order is solvable. And the Frobenius group pops up
many place in the theory of finite simple groups.

**Example 7.1.** A dihedral group $D_m$ of order $2m$ with $m$ odd is a Frobenius group. The subgroup generated by any involution $s$ is a Frobenius complement. This follows from the general (and easy) fact, that a subgroup of prime order being its own normalizer alway is a Frobenius complement, and it is easily checked that the subgroup of $D_m$ generated by $s$ is such.

**Example 7.2.** Let $k$ denote a finite field with $q$ elements. The linear maps given by

$$\Phi_{a,b}(x) = ax + b$$

where $a \in k^*$ and $b \in k$ constitute a group called the affine group. It is denoted by $\text{aff}^1(k)$ and has $q(q - 1)$ elements. The subgroup $H$ of rotations; i.e., those with $b = 0$, is a Frobenius complement in $\text{aff}^1(k)$ whose Frobenius kernel is the subgroup of translations; i.e., those linear maps with $a = 1$.

(7.1) Since $H^t \cap H = \{1\}$ for elements $t$ not belonging to $H$, the subgroup $H$ is its own normalizer; i.e., $N_G(H) = H$. The number of distinct conjugates of $H$ therefore equals the index $[G : H]$; indeed, when $G$ acts by conjugation on its subgroups, the isotropy group of $H$ is precisely the normalizer $N_G(H)$. Hence we find

$$\#(\bigcup H^t) = [G : H](|H| - 1) + 1 = |G| - [G : H] + 1,$$

and by consequence the following lemma (which by the way, is a a circumstantial evidence that $N$ is a Frobenius complement):

**Lemma 7.1** If $G$ is a Frobenius group with complement $H$ and kernel $N$, one has

$$|N| = [G : H].$$

**Problem 7.1.** Show that $N$ is closed under conjugation, and that $g^{-1} \in N$ when $g \in N$.

**Problem 7.2.** Show that the centralizer $C_G(h)$ of any non-trivial element $h \in H$ is contained in $H$. Conclude that the action of $H$ on $N$ by conjugation is free in the sense that $1$ is the only element possessing a fixed point other than $1$: If $hnh^{-1} = n$, then either $h = 1$ or $n = 1$.

**7.0.1 Conjugacy classes**

A basic property of a Frobenius complement $H$ is that conjugacy classes in $G$ either are disjoint from $H$ or meets $H$ in conjugacy classes, or phrased differently, no two conjugacy classes of $H$ are fused in $G$. Indeed, assume that two
elements \( h \) and \( h' \) in \( H \) are conjugate in \( G \) so that \( h' = t^{-1}ht \) for an element \( t \in G \). Since \( H^t \cap H = \{1\} \) when \( t \not\in H \), either \( h' = h = 1 \) or \( t \in H \), and in both cases \( h \) and \( h' \) are conjugate in \( H \).

It follows that a conjugacy class \( C \) that meets \( H \) can be expressed as the union of the conjugates of the conjugacy class \( c = C \cap H \); that is, one has \( C = \bigcup_t c^t \). This union will be disjoint when the index \( t \) is confined to a set of representatives of the left cosets of \( H \) (since \( c^t \cap c^s = \{1\} \) would imply that \( H^{ts^{-1}} \cap H = \{1\} \) and hence \( ts^{-1} \in H \)). It follows that \( C \) is the disjoint union of \([G : H]\) different sets, all conjugate to \( c \). Hence the relation

\[
n_C = [G : H] n_c
\]

holds between the numbers \( n_C \) and \( n_c \) of elements in respectively \( C \) and \( c \).

### 7.0.2 Extension of class functions

Given the relation between the conjugacy classes in \( G \) and \( H \), there is an easy way to extend a class function \( \psi \) on \( H \) to a class function \( \psi^* \) on \( G \). A conjugacy class \( C \) in \( G \) is either disjoint from \( H \) or intersects \( H \) in a unique conjugacy class. By assigning the value \( \psi(1) \) to the conjugacy classes of \( G \) contained in \( N \), and the value \( \psi \) takes on the conjugacy class \( c = C \cap H \) if \( C \not\subseteq N \), we get a class function extending \( \psi \). One thus has

\[
\psi^*(g) = \begin{cases} 
\psi(1) & \text{if } g \in N, \\
\psi(tgt^{-1}) & \text{if } tgt^{-1} \in H.
\end{cases}
\]

Unless \( \psi(1) = 0 \), the extended function \( \psi^* \) and the induced class function \( \text{ind}_H^G \psi \) differ on elements in \( N \), the latter vanishing in \( N \), but they coincide off \( N \). Indeed, at an element \( g \in G \) belonging to \( H^t \) for \( t \in G \), the induced character \( \text{ind}_H^G \psi \) takes the value

\[
|H|^{-1} \sum_{t \in G} \psi(tgt^{-1}),
\]

where \( \psi \) denotes the extension of \( \psi \) by zero. Now, the elements \( t \) with \( tgt^{-1} \in H \) form a left coset of \( H \), and their number therefore equals \(|H|\), and we conclude that \( \text{ind}_H^G \psi \) and \( \psi^* \) takes the same value at \( g \).

**Lemma 7.2** Let \( \phi \) and \( \psi \) be two class functions on \( G \). One has

\[
(\psi^*, \phi^*)_G = (\psi, \phi)_H.
\]

**Proof:** This is a simple and explicit computation splitting the sum giving \((\psi^*, \phi^*)_G\) in two parts. In the first part, we sum over the conjugacy classes
contained in $N$ and this contributes the amount

$$ |G|^{-1} \sum_{g \in N} \psi^*(g)\phi^*(g^{-1}) = |G|^{-1} |G : H| \psi(1)\phi(1) = |H|^{-1} \psi(1)\phi(1) $$

to the scalar product. Notice that number of elements in $N$ is $|G : H|$ by lemma 7.1 above.

The contribution from the rest of the conjugacy classes in $G$ is

$$ |G|^{-1} \sum_{C \subseteq N} n_C \psi_C \phi_C = |G|^{-1} \sum_{C \neq 1} |G : H| n_C \psi_C \phi_C = |H|^{-1} \sum_{c \neq 1} n_c \psi_c \phi_c, $$

where as usual a subscript $C$ (respectively $c$) indicates the value a class function takes on $C$ (respectively $c$). Putting the two parts together we obtain $(\psi, \phi)_H$. \[\square\]

(7.1) It is worth while formulating the lemma in the following way:

**Proposition 7.1** Let $G$ be a Frobenius group with complement $H$. Assume that $\psi$ is a class function with $\psi(1) = 0$. Then the restriction of $\text{ind}_H^G \psi$ to $H$ coincides with $\psi$; that is, $\text{res}_H^G \text{ind}_H^G \psi = \psi$. For any other class function $\phi$ on $H$, it holds true that

$$(\text{ind}_H^G \psi, \text{ind}_H^G \phi)_G = (\psi, \phi)_H.$$  

In particular, induction is an isometric imbedding of $\text{Ch}_0(H)$ into $\text{Ch}_0(G)$.

**Proof:** The only necessary observation is that in the proof of the lemma it suffices that $\psi(1)$ vanishes in $N$ for the equality $(\psi^*, \phi^*) = (\psi^*, \text{ind}_H^G \phi)$ to hold true. \[\square\]

(7.2) When $\psi$ is a character, the extended class function $\psi^*$ constructed above turns out to be a character:

**Lemma 7.3** If $\psi$ is a character, then $\psi^*$ is a character.

**Proof:** We may clearly assume that $\psi$ is irreducible. It suffices to show that $\psi^*$ is a virtual character (i.e., a linear combination of characters with integral coefficients). Indeed, by lemma 7.2 we know that $(\psi^*, \psi^*)_C = (\psi, \psi)_H = 1$ and by definition of $\psi^*$ it holds that $\psi^*(1) = \psi(1) > 0$. And these two properties imply that a virtual character is a genuine character as in corollary 4.7 on page 93.

One has the following identity which shows that $\psi^*$ is a virtual character:

$$ \psi^* = \text{ind}_H^G \psi - \psi(1)\theta, \quad (7.1) $$

where $\theta = \text{ind}_H^G 1_H - 1_G$. Indeed, recall that the induced character $\text{ind}_H^G 1_H$ is the character of the permutation representation associated to the action of $G$ on
$X = G/H$, and its value at a group element $g$ equals the number of fixed point $g$ has in $X$. Hence

$$\text{ind}^G_H 1_H(g) = \begin{cases} [G : H] & \text{if } g = 1, \\ 0 & \text{if } g \in N, \text{ but } g \neq 1, \\ 1 & \text{if } g \in H^t \text{ for some } t, \text{ but } g \neq 1. \end{cases}$$

and by consequence

$$\theta(g) = \begin{cases} [G : H] - 1 & \text{if } g = 1, \\ -1 & \text{if } g \in N, \text{ but } g \neq 1 \\ 0 & \text{if } g \in H^t \text{ for some } t, \text{ but } g \neq 1. \end{cases}$$

Then 7.1 follows immediately.

### 7.0.3 Frobenius’ theorem

One important, but simple, feature of a representation $V$ of $G$ is that the corresponding map $\rho_V : G \to \text{Gl}(V)$ is a homomorphism, and hence it has a kernel! This is a normal subgroup of $G$, which one in some cases and with some luck can prove to be non-trivial. So in favorable conditions, representations gives us a means to detect non-trivial normal subgroups. The proof of Frobenius’ theorem is a striking illustration of this feature. Recall that the kernel of the character $\chi_V$ is the collection of elements $g$ in the group with $\chi_V(g) = \chi_V(1)$. It coincides with $\ker \rho_V$ (paragraph 4.6 on page 105).

**Theorem 7.1** Assume that $G$ is a Frobenius group with complement $H$. Then the Frobenius kernel—that is, the set $N = \{ g \in G \mid g \notin H^t \}$—is a normal subgroup of $G$.

**Proof:** We shall establish the equality $N = \bigcap \ker \psi^*$, where the intersection is taken over all characters of $H$, which obviously impkmes the theorem. First, by definition, it holds that $\psi^*(g) = \psi^*(1) = \psi(1)$ whenever $g$ belongs to $N$; so $N \subseteq \bigcap \ker \psi^*$. Next, there is for every element $g \in H$ a character $\psi$ such that $g$ does not belong to $\ker \psi$; i.e., such that $\psi(g) \neq \psi(1)$, hence neither $g$ nor any of its conjugates lie in $\ker \psi^*$.

The Frobenius complement acts by conjugation on the kernel $N$, and the group $G$ is isomorphic to the semi-direct product of $N$ by $H$.

The $|H|$ is congruent 1 mod $|N|$:  

**Problem 7.3.** Show that $H$ acts on $N$ fixing no other element than 1. Show that $G$ is the semi-direct product $H \times N$. 

*
**Problem 7.4.** Show that \(|N| \equiv 1 \mod |H|\). Hint: compute \((\theta, \theta)\) and use that it is an integer since \(\theta\) is a virtual character.

**Problem 7.5.** Show that the quaternion group \(Q\) acts without fixedpoints on \(F_{13} \times F_{15}\); hence there is a Frobenius group of order \(1352 = 2^3 \cdot 13^2\) with kernel \(F_{13}^2\) and complement \(Q\). Hint: The two matrices in \(\text{Sl}(2, 13)\) below generates a group isomorphic to \(Q\):

\[
\sigma = \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
\]

**Problem 7.6.** Generalizing the previous problem, show that for any prime \(p > 3\) and \(F_q\) a field of characteristic \(p\) containing \(i = \sqrt{-1}\), there is a Frobenius group \(G\) of order \(8q^2\) with complement \(Q\) and kernel \(F_q^2\). Hint: there is a complex representation of \(Q\) in \(\text{Sl}(2, \mathbb{C})\) given generated by the matrices

\[
\sigma = \frac{i}{3} \begin{pmatrix} 3 & 4 \\ 4 & -3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}
\]

**Problem 7.7.** Let \(H\) be the *Heisenberg group* of rank three over the finite field \(F_q\); that is the group consisting of matrices shaped like

\[
\sigma = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.
\]

Show that \(H\) is a \(p\)-group of order \(q^3\). Let \(\alpha\) be a generator for the cyclic group \(F_q^*\) and let \(n\) and \(m\) be two numbers with \(n - 1\) and \(m - 1\) invertible mod \(q - 1\). Let \(A\) be the cyclic group generated by the diagonal matrix

\[
\begin{pmatrix}
\alpha & 0 & 0 \\
0 & \alpha^n & 0 \\
0 & 0 & \alpha^m
\end{pmatrix}.
\]

Show that \(A\) acts on \(H\) without essential fixed points and hence that the semi-direct product \(H \rtimes A\) is a Frobenius group of order \(q^3(q - 1)\).

**Problem 7.8.** Show that if \(H\) acts without fixed points on a \(p\)-group \(S\), then any abelian subgroup of \(H\) is cyclic.
8

Some algebra

The aim of this chapter is a quick and dirty introduction to or recapitualtion of the elementary thery of finite dimesional algebras over a field. At a few oc-
cations during this course we shall meet algebras that are not group algebras,
and this is the only motivation for this appendix. The algebras will still be
closely related to groups algebras. n A will be an algebra over a field $k$ of finite
dimension.

**Lemma 8.1** An element $a \in A$ is a left non-zero divisor if and only if it is right
invertible. An element $x \in A$ is a right (respectively a left) inverse for $a \in A$ if and
only it is a two-sided inverse

**Proof:** When $ax = 0$ only if $x = 0$, the multiplication map $A \to A$ that sends $x$
to $ax$ is injective. Hence it is surjective as well, $A$ being of finite dimension over
$k$. It follows that $1$ lies in the image, that is $ax = 1$ for some $x$.

Assume that $ax = 1$. Then clearly $x$ is a left-non-zero-divisor, and hence has
a right inverse $y$. It follows that $xax = x$ and thus $xa = xaxy = xy = 1$. $\square$

8.1 Semi-simple modules

A module $V$ is simple or irreducible if $0$ and $V$ are the only submodules and $V$
is semi-simple if $V$ is a diret sum of simple modules.

One says that $V$ is completely decomposable if any submodule $W \subseteq V$ has a
complement, which is a submodule $W'$ such that $W \cap W' = 0$ and $V = W + W'$;
in other words, $V = W \oplus W'$.

**Lemma 8.2** Given a simple non-zero $A$-module $V$.

Then $V$ is monogenic and generated by any non-zero vector $v \in V$. 
The annihilator \( \text{ann} \ v \) is a maximal left ideal and The annihilator \( \text{ann} \ V \) is an intersection of maximal left ideals.

**Proof:** Pick a vector \( v \in V \) which is different from zero. Clearly \( \{ av \mid a \in A \} \) is a submodule that is non-zero as \( v \) lies there. Because \( V \) is simple, it follows that \( V \) is generated by \( v \).

The annihilator \( \text{ann} V = \{ a \in A \mid aV = 0 \} \) is the intersection of \( \text{ann} v = \{ a \mid av = 0 \} \) that is maximal.

The Jacobson radical, or simply the radical, of \( A \) is the intersection of all annihilators of irreducible modules:

\[
J(A) = \bigcap_{V \text{ irreducible}} \text{ann} V
\]

**Lemma 8.3** Let \( A \) be an algebra over a field \( k \) of finite dimension. Every nilpotent ideal is contained in the radical. The radical is nilpotent.

**Proof:** Let \( I \) be a nilpotent ideal, say \( I^n = 0 \), and assume that \( I \) is not contained in the radical which means that there is an irreducible module \( V \) not killed by \( I \). Now, since \( V \) is irreducible and \( IV \) is a submodule, it follows that \( IV = V \). But then \( 0 = I^n V = V \), which is absurd.

The second statement will follow from the following: For any finite \( A \)-module \( V \) of dimension \( n \) it holds true that \( J^n V = 0 \), the proof of which goes by induction. Let \( W \subseteq V \) be a minimal non-zero submodule. Then \( W \) is irreducible and consequently \( JW = 0 \). By induction \( J^{n-1} \) kills \( V/W \), which means that \( J^{n-1} V \subseteq W \), hence \( I^n V = 0 \).

**Proposition 8.1** The following are equivalent

1. \( M \) is completely reducible;
2. \( M = \sum_{j \in J} M_j \) where the \( M_j \)'s are simple submodules
3. \( M = \bigoplus_{i \in I} M_i \) where the \( M_i \)'s are simple submodules.

**Proof:** 2 implies 1: Assume that \( M' \subseteq M \) is a submodule. Let \( M'' \) be a maximal submodule intersecting \( M' \) trivially. Such a module exists trivially if \( M \) is noetherian, and it follows with the help of Zorn’s lemma in general. We claim that \( M' + M'' = M \), and this will finish the argument as \( M' \cap M'' = 0 \) by construction. Assume that \( M' + M'' \neq M \). For at least one \( j \) it would then hold that \( M_j \) was not contained in \( M' + M'' \), and as \( M_j \) is simple, the intersection
$M_i \cap M' = 0$. But then $M'' + M_j$ would properly contain $M''$ and meet $M'$ trivially which contradicts the maximality of $M''$.

1 implies 3: Consider the set of sets submodules $\{M_i\}$ such that the sum $\sum_i M_i$ is direct¹. This has a maximal element by Zorn’s lemma; indeed the union of a ascending series of direct sums is a direct. Let $I$ indect a maximal set and let $M_0 = \sum_{i \in I} M_i$ be the sum of the submodules in maximal elemenet, then $M = M_0$, since if not $M = M_0 \oplus M'$, $\{M_i\} \cup \{M'\}$ would be larger than $\{M_i\}$.

Induction on the length of $M$. Let $M'$ be simple non-zero submodule. One has $M = M' \oplus M''$ because $M$ is completely reducible, but $M'$ and $M'$ are both of length less that $M$ and the induction hypothesis applies to both.

3 implies 2 is trivial.

¹ This is equivalent to the sums of $\sum_{i \in I'} M_i$ and $\sum_{i \in I''} M_i$ of any two disjoint subsets of $I$ intersecting in zero.
9

The symmetric groups

Very preliminary version 0.0 as of 14th November, 2017
Not even a sketch and will change

9.1 Fundamental properties

We let $X$ be a finite set. The symmetric group on $X$ has by definition the set of bijections $\sigma: X \to X$ as underlying set and the group law is composition. The elements of $\text{Sym}(X)$ are called permutations of $X$. It If $X$ has $n$ elements, te order of $\text{Sym}(X)$ will be $n!$.

In the case $X = X_n = \{1, 2, \ldots, n\}$; that is $X_n$ is the set of integers between 1 and $n$, one writes $S_n$ for $\text{Sym}(X_n)$. Any numbering of the elements of $X$ gives rise to an isomorphism between $\text{Sym}(X)$ and $S_n$: Indeed, if $\beta: X \to X_n$ is a numbering (which by assumption is bijective, no to members of $X$ are given the same number), the isomorphism is given as $\sigma \mapsto \beta \sigma \beta^{-1}$.

In particular, any renumbering of the elements in $X_n$, which is effectuated by a permutation $\beta: X_n \to X_n$, gives rise to the conjugation map, (or the inner automorphism as one frequently says) $\sigma \mapsto \beta \sigma \beta^{-1}$.

9.1.1 Conjugacy classes

A cycle is a permutation that has one orbit with more than one element. Any orbit $Y$ of a permutation $\sigma$ is finite of course, and for any element $y \in Y$ it holds that $Y = \{ y, \sigma y, \sigma^2 y, \ldots, \sigma^{r-1} y \}$ where $r$ is the order of $\sigma$. When $\sigma$ is a cycle, this is the only non-trivial orbit of of $\sigma$ all other elements are fixed points. Hence a cycle $\sigma$ is completely determined by its action on its non-trivial
orbit $Y_\sigma$. This permits the notation

$$\sigma = (y_0, y_1, \ldots, y_{r-1}).$$

Notice that this representation depends on the choice of an element $y_0$ from the non-trivial orbit, so it is not unique. One can use any of the $y_i$'s as the initial point, in other words it holds true that

$$\sigma = (y_i, y_{i+1}, \ldots, y_{r-1}, y_0, \ldots, y_{i-1});$$

that is, any cyclic permutation of the $y_i$'s gives the same $\sigma$. For instance one has

$$(1, 2, 3, 4) = (3, 4, 2, 1)$$

in $S_4$ for any $0 \leq i \leq r - 1$.

In our definition of a cycle, we have excluded the identity by requiring that there should be one orbit with more than one element.

Two cycles are said to be disjoint when their non-trivial orbits are disjoint.

For instance $(1, 2, 3)$ and $(4, 5, 6)$ are disjoint, whereas as $(1, n)$ and $(1, 2, \ldots, n)$ are not. It is a fundamental fact that disjoint cycles commute. The orbits of $\sigma$ on $X$ play a special role.

**Lemma 9.1** Every permutation $\sigma$ can be expressed as a product

$$\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r \quad \text{(9.1)}$$

of disjoint, hence commuting, cycles. The cycles $\sigma_i$ are uniquely determined by $\sigma$.

**Proof:** Let $Y_1, \ldots, Y_s$ be the distinct non-trivial orbits of $\sigma$. Define cycles $\sigma_i$ by

$$\sigma_i(x) = \begin{cases} x & \text{when } x \notin Y_i \\ \sigma(x) & \text{when } x \in Y_i \end{cases}$$

They are clearly disjoint and their product equals $\sigma$. 

The decomposition in (9.1) above is called the cycle decomposition of $\sigma$, and the set of the lengths of the intervening cycles $\sigma_i$ is said to be the type of the decomposition. The order does not matter, so it is often listed as a descending list. In the decomposition 9.1 only cycles (which correspond to non-trivial orbits of $\sigma$) appear, but it is common usage to include the fixed points as well in the type by appending an appropriate number of one’s to the list. So, for instance the type of $(1, 2)(3, 4, 5)(6, 7)$ will be 3, 2, 2 when regarded as an element in $S_7$, but as an element in $S_{10}$ it fixes 8, 9 and 10, so the type will be 3, 2, 2, 1, 1, 1.
Lemma 9.2 Let \( \pi \) be a permutation of \( S_n \) and let \( (a_0, \ldots, a_m) \) be a cycle. Then it holds true that

\[
(\pi(a_0), \ldots, \pi(a_{m-1})) = \pi \circ (a_0, \ldots, a_{m-1}) \circ \pi^{-1},
\]

(9.2)

Consequently any two cycles of the same length are conjugate.

Proof: Feeding the right side by an element \( a \), we see that if \( a \) equals one of the \( \pi(a_i) \)'s, it undergoes the metamorphosis

\[
\pi(a_i) \xrightarrow{\pi^{-1}} a_i \xrightarrow{a_{i+1}} \pi(a_{i+1}),
\]

but if not, nothing happens to it. And this exactly the action of the cycle on the left side in (9.3). Assume that \( (b_0, \ldots, b_m) \) is another cycle of length \( m \). Let \( \pi \) be the permutation with \( \pi(a_i) = b_i \), and which on the complement \( X_n \setminus \{a_i\} \) equals any bijection between \( X_n \setminus \{a_i\} \) and \( X_n \setminus \{b_i\} \). Then (9.3) shows that \( (b_0, \ldots, b_m) = \pi \circ (a_0, \ldots, a_m) \circ \pi^{-1} \).

(9.1)—The Conjugacy Classes. Combining the two previous lemmas one proves the following result that gives a complete description of the conjugacy classes of the symmetric groups.

Proposition 9.1 Two permutations \( \pi \) and \( \pi' \) are conjugate in \( S_n \) if and only if they have cycle decompositions of the same type.

Proof: Two cycles \( \sigma_1 \) and \( \tau_1 \) of the same length are conjugate by lemma xxx, and they can be conjugated by any permutation \( \pi \) that sends \( Y_{\sigma_1} \) to \( Y_{\tau_1} \) in the appropriate way (that is \( \pi(\sigma_1 y_1) = \tau_1 z_1 \)), what it does to elements not lying in \( Y_{\sigma_1} \) does not matter. Now, given two other cycles \( \sigma_2 \) and \( \tau_2 \) with the same length and disjoint from respectively \( \sigma_1 \) and \( \tau_1 \). Then since \( Y_{\sigma_2} \) does not meet \( Y_{\sigma_1} \), we may chose \( \pi \) so that it maps \( Y_{\sigma_2} \) into \( Y_{\tau_2} \) in the way prescribed in lemma xxx. Then the product \( \sigma_1 \sigma_2 \) and \( \tau_1 \tau_2 \) are conjugate by \( \pi \).

9.1.2

Lemma 9.3 Every permutation \( \sigma \in S_n \) is conjugate to its inverse \( \sigma^{-1} \) by an element in \( S_{n-1} \) fixing 1.

Proof: It is enough to check the theorem for one full cycle, for instance \( \sigma = (1, 2, \ldots, n) \). Then the inverse \( \sigma^{-1} \) is the “backward” cycle \( \sigma^{-1} = (n, n-1, \ldots, 2, 1) \) which also can be presented as \( \sigma^{-1} = (1, n, n-1, \ldots, 3, 2) \). So the permutation \( c \) that interchanges \( n-i \) and \( 2+i \) for \( i \leq (n-2)/2 \) does the job.
9.2 Partitions and Young diagrams

Recall that a partition of a natural number \( n \) is a decreasing sequence \( \{ \lambda_i \} \) of non-negative integers whose sum equals \( n \), that is \( \sum \lambda_i = n \). This enforces \( \lambda_i \) to eventually vanish and we let \( \lambda_r \) be the last non-zero member of the sequence.

There is a suggestive geometric way of interpreting a partition called its Young diagram \( D_\lambda \). It is the region in the plane with \((x, y)\) satisfying \( 0 < x \leq i \) and \( 0 < y \leq \lambda_i \) for some natural number \( i \). It is staircase-like region depicting a configuration of adjacent pillars of boxes (each box being a 1 \( \times \) 1-box) resting on the \( x \)-axis and decreasing to the right, the \( i \)-th pillar being of height \( \lambda_i \). The figure in the margin illustrates the Young diagram of the partition 4, 2, 2, 1, 1, 1.

The boxes in the diagram shear the property that the neighbouring boxes to the left and below belong to diagram as well, as long as they lie in the first quadrant.

(9.1)—Corners. Some boxes are more prominent than others, and their prominence stems from their fundamental role in the omnipresent arguments based on induction on the integer being partitioned (or the number of boxes, if you prefer).

A box is an outer corner of the diagram \( D_\lambda \) if the configuration we obtain by removing leaves us with the diagram of a new partition (of \( n - 1 \)). They are characterized as those boxes such that neither the neighbour above nor the one to the right belongs to the diagram.

There are inner corners as well. They do not belong to the diagram, but have the property that adding them gives the diagram of a new partition (of \( n + 1 \)). Equivalently, the inner corners are boxes in the complement of \( D \) whose closest neighbours to the left and below are boxes in \( D \).

The set \( \mathcal{Y} \) of Young diagrams are ordered by inclusion; and this induces a partial order on the set of partition. Given two partitions \( \lambda \) and \( \mu \) one writes \( \lambda \leq \mu \) if \( D_\lambda \subseteq D_\mu \). Or equivalently, that \( \lambda_i \leq \mu_i \) for all \( i \).

Let \( Z_n \) be the sub algebra of \( k[S_n] \) of elements commuting with \( S_{n-1} \); that is the collection of \( \alpha \)'s such that \( g \alpha = \alpha g \) for all \( g \in S_{n-1} \).

**Lemma 9.4** The algebra \( Z_n \) is commutative.

**Proof:** Any element \( \alpha = \sum_\sigma \alpha_\sigma \sigma \) satisfies \( \alpha_\sigma = \alpha_{\sigma^{-1}} \); since \( \sigma \) and \( \sigma^{-1} \) are conjugate with elements \( S_{n-1} \).

Indeed, when \( \alpha = \sum_\sigma \alpha_\sigma \sigma \) lies in \( Z_n \) one has \( \tau \alpha \tau^{-1} = \sum_\sigma \alpha_\sigma \tau \sigma \tau^{-1} = \sum_\sigma \alpha_\sigma \sigma^{-1} \) and the \( \sigma \)'s forming a basis for \( k[S_n] \) it follows that \( \alpha_\sigma = \alpha_{\sigma^{-1}} \).
Lemma 9.5 Every permutation $\sigma \in S_n$ is conjugate to its inverse $\sigma^{-1}$ by an element in $S_{n-1}$ fixing 1.

Proof: It is enough to check the theorem for one full cycle, for instance $\sigma = (1,2,\ldots,n)$. Then the inverse $\sigma^{-1}$ is the “backward” cycle $\sigma^{-1} = (n,n-1,\ldots,2,1)$ which also can be presented as $\sigma^{-1} = (1,n,n-1,\ldots,3,2)$. So the permutation $c$ that interchanges $n-i$ and $2+i$ for $i \leq (n-2)/2$ does the job.

Lemma 9.6 Every element in $A_n$ is a commutator in $S_n$; $[S_n,S_n] = A_n$.

Proof: As $sts^{-1}t^{-1} = ab$ with $a$ and $b$ conjugate. If $a$ and $b$ are conjugate, the product $ab$ is a commutator. Indeed, $b = ca^{-1}c^{-1}$, so $ab = aca^{-1}c^{-1} = [a,c]$. Hence it suffices to check that any element from $A_n$ is the product of two conjugate element, and we may assume that $s$ is an odd cycle or the product of two even cycles.

9.3 Appendix: Basics properties of the symmetric group

Most of what we do in this appendix should be known to the well educated student, but for those who have not seen it yet and to refresh their memories, we give short of the fundamental properties of the symmetric group.

The symmetric group $S_n$ acts on the set $I_n = \{1,\ldots,n\}$. Let $\sigma$ be permutation of $I_n$ whose order is $m$. For $a \in I_n$, the orbit of $a$ equals $\{a,\sigma(a),\sigma^2(a),\ldots,\sigma^{m-1}(a)\}$.

So the action of $\sigma$ almost makes the orbit an ordered set with $\sigma(x)$ being the immediate successor of $x$. The initial point $a$, however, is matter of choice, and any point in the orbit will do. One may say that the orbit is cyclic ordered.

The permutation $\sigma$ is called a cycle if it has a single orbit with more than one element; that is, $\sigma$ has one orbit such that all points not belonging to that orbit are fixed points. Writing $a_i = \sigma^i(a)$ with $1 \leq i \leq m-1$ for the points belonging to the special orbit, one denotes the cycle $\sigma$ by

$$\sigma = (a_0,a_2,\ldots,a_{m-1}).$$

Be aware that this notation depends on the the choice of the initial point $a_0$, and one has $\sigma = (a_i,a_{i+1},\ldots,a_{m-1},a_0,\ldots,a_{i-1})$ as well. One has $\sigma^i(a_i) = a_{i+j}$ where the sum $i+j$ is interpreted modulo $m$.

A cycle with just two elements is called a transposition; the effect of the transposition $\sigma = (i,j)$ is to swap the numbers $i$ and $j$ leaving all others fixed.
Obviously any choice of \( m \) different numbers from \( I_n \) defines a unique a cycle. For instance \( \sigma = (1, 5, 7) \) is the permutation that sends 1 to 5, 5 to 7 and the 7 back to 1, and it does not move any other number.

(9.1)—**Factorization in disjoint cycles.** Now, let \( \pi \) be any permutation of \( I_n \), and let \( X \subseteq I_n \) be one of its orbits. With the orbit \( X \) one can associate a cycle \( \sigma_X \) in the following way:

\[
\sigma_X(a) = \begin{cases} 
\pi(a) & \text{if } a \in X \\
 a & \text{if not}
\end{cases}
\]

It is indeed a cycle having \( X \) as an orbit and all points off \( X \) being fixed points.

Let \( X_1, \ldots, X_r \) be all the orbits of \( \pi \) in \( I_n \) (including the one-point orbits, which are the fixed points). Then the set \( I_n \) is the disjoint union of \( X_i \)'s; that is, \( I_n = \bigcup_i X_i \). For each \( i \) one has the cycle \( \sigma_{X_i} \) whose restriction to \( X_i \) equals \( \pi|_{X_i} \) and which off \( X_i \) acts as the identity. This entails that one has the factorization

\[
\pi = \sigma_{X_1} \circ \sigma_{X_2} \circ \ldots \circ \sigma_{X_r}
\]

Indeed, if \( x \in I_n \) lies in the orbit \( X_i \), only the cycle \( \sigma_{X_i} \) affects \( x \).

Disjoint cycles commute; this is clear since

Hence \( \pi \) is any permutation, \( I_n \) decomposes into orbits, and the corresponding cycles is a factorization of \( \pi \).

(9.2)—**Conjugation class of cycles.** The conjugate of a cycle \( \sigma = (a_0, \ldots, a_{m-1}) \) by a permutation \( \pi \) of \( I_n \) has a nice description. One has

**Lemma 9.7** Let \( \pi \) be a permutation of \( S_n \) and let \( (a_0, \ldots, a_m) \) be a cycle. Then it holds true that

\[
(\pi(a_0), \ldots, \pi(a_{m-1})) = \pi \circ (a_0, \ldots, a_{m-1}) \circ \pi^{-1},
\]

(9.3)

Consequently any two cycles of the same length are conjugate.

**Proof:** Feeding the right side by a number \( a \), we see that if \( a \) equals one of the \( \pi(a_i)'s \), it undergoes the metamorphosis

\[
\pi(a_i) \xrightarrow{\pi^{-1}} a_i \rightarrow a_{i+1} \xrightarrow{\pi} \pi(a_{i+1}),
\]

but if not, nothing happens to it. And this exactly the action of the cycle on the left side in (9.3). Assume that \( (b_0, \ldots, b_m) \) is another cycle of length \( m \). Let \( \pi \) be the permutation with \( \pi(a_i) = b_i \), and which on the complement \( I_n \setminus \{a_i\} \) equals any bijection between \( I_n \setminus \{a_i\} \) and \( I_n \setminus \{b_i\} \). Then (9.3) shows that

\[
(b_0, \ldots, b_m) = \pi \circ (a_0, \ldots, a_m) \circ \pi^{-1}.
\]
Conjugacy classes

Generators and relations