MA3E1 Groups and Representations

Daan Krammer

October 28, 2013

Abstract

Lecture notes for third year maths students at Warwick University, on finite groups, mostly their complex representations. I have shamelessly stolen from Yuri Bazlov's excellent Warwick lecture notes and Martin Isaacs' excellent book *Character theory of finite groups*.

Contents

1 Groups

1.1 Groups

Definition 1. A **group** consists of a set G and a binary operation $G \times G \to G : (x, y) \mapsto xy$ such that:

- Associativity: We have $x(yz) = (xy)z$ for all $x, y, z \in G$.
- Identity: There exists an element $1 \in G$ such that $1x = x = x1$ for all $x \in G$. We call 1 the **identity element** or **neutral element** of G.
- Inverses: For all $x \in G$ there exists y (usually written $y = x^{-1}$) such that $xy = 1 = yx$. We call x^{-1} the **inverse** of x.

Example 2. (a). Let $G = \{1\}$ and necessarily $11 = 1$. This is a group called the **trivial group** and we simply write $G = 1$.

(b). Each of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ forms a group with addition for group operation.

(c). The set $\mathbb{Q}^\times := \mathbb{Q} \setminus \{0\}$ is a group with multiplication for group operation but $\mathbb{Z} \setminus \{0\}$ is not. In general, if R is a ring then $R^\times$ denotes the set of invertible elements in R and is a group.

Exercise (1.1) The product of n elements of a group is independent of the bracketing; for example $(ab)(cd) = (a(bc))d$. State more precisely what this means and prove it.

Let G be a group. For $x \in G$ and $n \geq 0$ we write x^n instead of $xx \cdots x$ (n factors) and $x^{-n} := (x^n)^{-1}$.

The number of elements of a set A is written $\#A$ or $|A|$. It is a nonnegative integer or infinite. It is also known as the **cardinality** of A. The number of elements of a group is traditionally called its **order**.

Definition 3. Let x be an element of a group G. The **order** of x is the least positive integer n such that $x^n = 1$, or ∞ if such n doesn't exist.

Definition 4. Two elements x, y of a group are said to **commute** if $xy = yx$. A group in which every pair of elements commute is called **commutative** or **abelian**.

Definition 5. A **subgroup** of a group G is a nonempty subset $H \subset G$ such that:

- Closed under multiplication: For all $x, y \in H$ we have $xy \in H$.
- Closed under inverses: For all $x \in H$ we have $x^{-1} \in H$.

Every subgroup of a group is a group in its own right. We write $H \leq G$ if H is a subgroup of a group G.

1.2 Groups of matrices

The set of $n \times n$ matrices with entries in $\mathbb{C}$ is written $M(n, \mathbb{C})$. Two such matrices can be multiplied, for example

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p & q \\ r & z \end{pmatrix} = \begin{pmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{pmatrix}.$$

We say that $A, B \in M(n, \mathbb{C})$ are inverses of each other if $AB = 1_n = BA$ where 1_n is the $n \times n$ identity matrix. If A has an inverse then A is called **invertible** or regular. Now $M(n, \mathbb{C})$ is not a group under multiplication because inverses don't always exist. The set of invertible elements of $M(n, \mathbb{C})$ is written $\mathrm{GL}(n, \mathbb{C})$ and is a group.

Fact 6. *A matrix A in $M(n, \mathbb{C})$ is invertible if and only if $\det(A) \neq 0$. That is, $\mathrm{GL}(n, \mathbb{C}) = \{A \in M(n, \mathbb{C}) \mid \det(A) \neq 0\}$.*

If $n \geq 2$ then $\mathrm{GL}(n, \mathbb{C})$ is not abelian. However $\mathrm{GL}(1, \mathbb{C})$ is abelian; it is "the same" as $\mathbb{C}^\times$.

1.3 Cyclic groups

Definition 7. A group G is **cyclic** if there exists $g \in G$ such that $G = \{g^n \mid n \in \mathbb{Z}\}$. We say that g is a **generator** of the cyclic group.

Much more on generators of groups will follow later. A generator of a cyclic group may not be unique. For example, 1 is a generator of the cyclic group $(\mathbb{Z}, +)$ but so is -1.

Proposition 8: Classification of cyclic groups. *Let G be a cyclic group with generator g.*

(a) *Suppose $\#G = \infty$. Then $g^k \neq g^\ell$ whenever $k \neq \ell$ and $k, \ell \in \mathbb{Z}$. Moreover $g^k g^\ell = g^{k+\ell}$ for all $k, \ell \in \mathbb{Z}$.*

(b) *Suppose $\#G = n < \infty$. Then $g^0, \ldots, g^{n-1}$ are distinct and therefore are all elements of G. Moreover if $k, \ell \in \{0, \ldots, n-1\}$ then $g^k g^\ell = g^m$ where $m = (k + \ell) \bmod n$, that is, m is the unique element of $\{0, \ldots, n-1\}$ such that $n \mid k + \ell - m$.*

Proof. Proof of (a). Suppose $g^k = g^\ell$ for some distinct $k, \ell \in \mathbb{Z}$, say $k > \ell$. Write $m = k - \ell$. Multiplying both sides with $g^{-\ell}$ we find $g^m = 1$.

We claim $G = \{g^r \mid 0 \leq r < m\}$. Choose any element of G, say, g^s. Then there exist $q, r \in \mathbb{Z}$ such that $s = qm + r$ and $0 \leq r < m$. It follows that

$$g^s = g^{qm+r} = (g^m)^q g^r = 1^q g^r = g^r$$

which proves our claim that $G = \{g^r \mid 0 \leq r < m\}$.

The remaining statement in (a) is obvious.

Proof of (b). Suppose $g^0, g^1, \ldots, g^{n-1}$ are not distinct, say, $g^k = g^\ell$ with $0 \leq \ell < k \leq n-1$. Put $m = k - \ell$. As in (a) it follows that $G = \{g^r \mid 0 \leq r < m\}$. In particular $\#G \leq m < n$, a contradiction. Therefore $g^0, g^1, \ldots, g^{n-1}$ are distinct. The remaining statement in (b) is obvious. □

In particular, any two cyclic groups of the same order are isomorphic (isomorphic will soon be defined). It also follows that if G is a cyclic group with generator g then the order of g equals the order of G.

Definition 9. Let C_∞ denote a cyclic group of order ∞ and C_n a cyclic group of order n.

Notice that cyclic groups are abelian.

1.4 Symmetric groups and alternating groups

Definition 10. A **permutation** of a set A is just a bijective map from A to itself. The **symmetric group** S_n is the set of permutations of $\{1, \dots, n\}$, with composition for multiplication.

If $a_1, \dots, a_k \in \{1, \dots, n\}$ are distinct then $(a_1, \dots, a_k)$ or simply $(a_1 \cdots a_k)$ is defined to be the element $g \in S_n$ known as a ***k*-cycle** such that $g(a_i) = a_{i+1}$ for all i (indices modulo k) and $g(x) = x$ whenever $x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$.

The above choice of $\{1, \dots, n\}$ is standard but any other set of n elements is also good. The group of permutations of a set A is called the symmetric group on A.

For $n \geq 2$ there is a unique subgroup of S_n containing all 3-cycles and different from S_n. It is known as the **alternating group** and written A_n.

1.5 Dihedral groups

The set of integers modulo n is denoted $\mathbb{Z}/n$. It is a commutative ring.

Lemma/Definition 11. *We define D_{2n} to be the set of mappings from $\mathbb{Z}/n$ to itself of the form $x \mapsto ax + b$ where $a \in \{-1, 1\} \subset \mathbb{Z}/n$ and $b \in \mathbb{Z}/n$. Then D_{2n} is a subgroup of the symmetric group on $\mathbb{Z}/n$. It is called the* **dihedral group**.

Proof. It is clear that D_{2n} is nonempty. Prove yourself that every element of D_{2n} is a permutation of $\mathbb{Z}/n$ and that its inverse is also in D_{2n}. It remains to prove that D_{2n} is closed under multiplication. Let $p, q \in D_{2n}$, say, $p(x) = ax + b$ and $q(x) = cx + d$ for all x. Then for all x

$$pq(x) = p(cx + d) = a(cx + d) + b = (ac)x + (ad + b)$$

which is again of the required form so $pq \in D_{2n}$. □

Definition 12. We define $r, s \in D_{2n}$ by $r(x) = x + 1$ and $s(x) = -x$.

Lemma 13. *We have $D_{2n} = \{r^k, s\,r^k \mid 0 \leq k < n\}$.*

Note that D_{2n} has $2n$ elements. Therefore the above lemma lists the elements of the dihedral group without repeats.

Proof. Since $\#D_{2n} = 2n$ it is enough to prove $\subset$ in the statement. Well, $r^b(x) = x + b$ and $s\,r^{-b}(x) = -x + b$. □

We call r^k a **rotation** and $s\,r^k$ a **reflection**. Therefore every element of the dihedral group is a rotation or a reflection but not both.

These names come from the following geometric definition of the dihedral group which we mention as an aside. The **standard regular *n*-gon** is the convex hull of $\{z \in \mathbb{C} \mid z^n = 1\}$. Then D_{2n} can be regarded as the group of bijective $\mathbb{R}$-linear maps $\mathbb{C} \to \mathbb{C}$ preserving the standard regular n-gon.

1.6 Homomorphisms and isomorphisms

Definition 14. Let G, H be groups. A **homomorphism** is a map $f\colon G \to H$ such that $f(xy) = f(x)\,f(y)$ for all $x, y \in G$.

Exercise (1.2) Let $f\colon G \to H$ be a group homomorphism. Prove:

(a) $f(1) = 1$.

(b) $f(x^{-1}) = f(x)^{-1}$ for all $x \in G$.

(c) $f(x^n) = f(x)^n$ for all $x \in G$, $n \in \mathbb{Z}$.

Definition/Exercise 15. The **direct product** of two groups G, H is $G \times H$ on which multiplication is defined to be entry-wise: $(a,b)(c,d) = (ac, bd)$. Prove that this makes $G \times H$ into a group.

Definition 16. Let G, H be groups. An **isomorphism** $G \to H$ is a bijective homomorphism. If there exists at least one isomorphism $G \to H$ then we write $G \cong H$ and we say that G, H are **isomorphic**.

The idea is that isomorphic groups are the same for most purposes. Note that $G \cong H$ implies $H \cong G$. Also, $G \cong H$ and $H \cong K$ imply $G \cong K$.

Example 17.

(a) Any two cyclic groups of the same order are isomorphic.

(b) $\mathbb{C}^\times \cong \mathrm{GL}(1, \mathbb{C})$.

(c) $C_6 \not\cong D_6$.

(d) $C_6 \cong C_2 \times C_3$.

(e) $S_3 \cong D_6$.

Here is the classification of groups of small order. For example, the classification of the groups of order 4 means finding a list of groups of order 4, such that every group of order 4 is isomorphic to just one group on the list.

$\#G$	1	2	3	4	5	6	7
G	1	C_2	C_3	$C_4,\ C_2 \times C_2$	C_5	$C_6,\ D_6$	C_7

1.7 Exercises

(1.3) True or false? Prove or disprove each statement.

(a) Let a be an element of a group G and m, n integers. Then $(a^m)^n = a^{mn}$.

(b) Let G, H be nontrivial cyclic groups (nontrivial means having more than one element). Then $G \times H$ is not cyclic.

(1.4) Consider the group $\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z})$, the group of invertible 2×2 matrices over $\mathbb{Z}/2\mathbb{Z}$. How many elements does it have? Is it isomorphic to a group you have seen before?

(1.5) Let G be a set. Let $G \times G \to G$: $(x, y) \mapsto xy$ be an associative binary operation. Let $1 \in G$ be such that $1x = x1 = x$ for all $x \in G$. (These define precisely what is known as a **monoid**). Prove or disprove each of the following.

(a) Let $e \in G$ be such that $ex = xe = x$ for all $x \in G$. Then $1 = e$.

(b) Suppose that for all $x \in G$ there exists $y \in G$ such that $xy = 1$. Then for all $x \in G$ there exists $z \in G$ such that $zx = 1$.

(c) Suppose that for all $x \in G$ there exist $y, z \in G$ such that $zx = 1 = xy$. Then G is a group.

(1.6) Let G, H be groups. An **anti-homomorphism** f: $G \to H$ is a map satisfying $f(xy) = f(y)f(x)$ for all $x, y \in G$.

(a) Give an example of an anti-homomorphism that is not a homomorphism and vice versa.

(b) Let $f\colon G \to H$ be a group homomorphism. Prove that f is also an anti-homomorphism if and only if $f(G)$ is abelian.

(c) Let G be a group. Prove that there exists a bijective anti-homomorphism $f\colon G \to G$ (a so-called anti-automorphism).

(1.7) Show that every group of even order contains an element of order 2.

(1.8) Show that the set of non-zero complex numbers under the usual multiplication is a group. Prove that every finite subgroup of this group is cyclic.

(1.9) Prove that s and rs are conjugate elements of D_{2m} (that is, $gsg^{-1} = rs$ for some $g \in D_{2m}$) if and only if m is odd.

(1.10) Prove that $D_{4m} \cong D_{2m} \times C_2$ if m is odd.

(1.11) We say that a square matrix X is upper triangular, if all entries below the main diagonal in X are zero. For example $\left(\begin{smallmatrix} 2i & 1 \\ 0 & -3 \end{smallmatrix}\right)$ is upper triangular. Let B_n be the set of upper triangular matrices in $\mathrm{GL}(n, \mathbb{C})$. Prove that B_n is a subgroup of $\mathrm{GL}(n, \mathbb{C})$.

2 Representations

2.1 Representations

Definition 18. A **representation** of a group G is a homomorphism $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ with $n \geq 0$ (by definition, $\mathrm{GL}(0, \mathbb{C})$ is a trivial group). We call n the **dimension** or **degree** of the representation.

Example 19. (a). For a group G and $n \geq 0$ there is the **trivial n-dimensional representation** $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ defined by $\rho(g) = 1$ for all $g \in G$.

(b). There is a representation $\rho\colon C_2 = \{1, g\} \to \mathrm{GL}(2, \mathbb{C})$ defined by $\rho(g) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Lemma 20. *Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation. Let $T \in \mathrm{GL}(n, \mathbb{C})$ and define $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ by $\sigma(x) = T\,\rho(x)\,T^{-1}$ for all $x \in G$. Then σ is also a representation.*

Proof. For all $x, y \in G$

$$\begin{aligned} \sigma(x)\,\sigma(y) &= (T\,\rho(x)\,T^{-1})(T\,\rho(y)\,T^{-1}) \\ &= T\,\rho(x)\,\rho(y)\,T^{-1} = T\,\rho(xy)\,T^{-1} = \sigma(xy). \end{aligned}$$

□

Definition 21. Let G be a group. Two n-dimensional representations ρ, σ of G are **equivalent**, and we write $\rho \sim \sigma$, if there exists $T \in \mathrm{GL}(n, \mathbb{C})$ such that $\sigma(x) = T\,\rho(x)\,T^{-1}$ for all $x \in G$.

Lemma 22. *Equivalence of representations is an equivalence relation.*

Proof. Prove yourself that $\sim$ is reflexive ($\rho \sim \rho$ for all ρ) and symmetric ($\rho \sim \sigma \Leftrightarrow \sigma \sim \rho$ for all ρ, σ).

We now prove that it is transitive. Assume that $\rho \sim \sigma \sim \tau$, say, $T, U \in \mathrm{GL}(n, \mathbb{C})$ are such that

$$\rho(x) = T\,\sigma(x)\,T^{-1}, \qquad \sigma(x) = U\,\tau(x)\,U^{-1} \qquad \text{for all } x \in G.$$

It follows that $\rho(x) = T\,\sigma(x)\,T^{-1} = T(U\,\tau(x)\,U^{-1})T^{-1} = (TU)\,\tau(x)\,(TU)^{-1}$ for all $x \in G$. This proves that $\rho \sim \tau$ and therefore $\sim$ is transitive. □

Reminder from set theory. Let $\sim$ be an equivalence relation on a set S. A **$\sim$-class** or **equivalence class with respect to $\sim$** or just **equivalence class** is a subset of S of the form $\{x \in S \mid x \sim y\}$ where $y \in S$. Then S is the disjoint union of the $\sim$-classes. We write $S/\sim$ for the set of $\sim$-classes and if $y \in S$ we write $y/\sim$ for the $\sim$-class containing y.

Definition 23. For a group G we define

$$\begin{aligned}\mathrm{Rep}_n(G) &= \{\text{representations } G \to \mathrm{GL}(n, \mathbb{C})\}/\sim \\ \mathrm{Rep}(G) &= \bigsqcup_{n \geq 0} \mathrm{Rep}_n(G)\end{aligned}$$

($\sqcup$ denotes disjoint union).

A fixed group G may have infinitely many n-dimensional representations. Later in exercise 5.7 we shall see that if G is finite then $\mathrm{Rep}_n(G)$ is finite. Most of these notes are about understanding $\mathrm{Rep}_n(G)$.

2.2 Representations of cyclic groups

Let $r \in \mathbb{Z}_{>0}$ and consider a cyclic group $C_r = \{1, g, g^2, \ldots, g^{r-1}\}$ of order r and generator g. We aim to classify the representations of C_r up to equivalence. This means listing the elements of $\mathrm{Rep}(C_r)$.

Lemma/Definition 24.

(a) *Let $A \in \mathrm{GL}(n, \mathbb{C})$ satisfy $A^r = 1$. Then there exists a unique representation $\rho_A \colon C_r \to \mathrm{GL}(n, \mathbb{C})$ such that $\rho_A(g) = A$. It satisfies $\rho_A(g^k) = A^k$ for all k.*

(b) *Every representation of C_r is equivalent to a representation of the form ρ_A.*

(c) *Let $A, B \in \mathrm{GL}(n, \mathbb{C})$. Then $\rho_A \sim \rho_B$ if and only if A, B are conjugate in $\mathrm{GL}(n, \mathbb{C})$.*

Proof. Prove (a) and (b) yourself. Proof of (c). $\Rightarrow$ is obvious. Proof of $\Leftarrow$. Let A, B be conjugate, say, $A = TBT^{-1}$ where $T \in \mathrm{GL}(n, \mathbb{C})$. Let $x \in C_r$. Then there exists $k \in \mathbb{Z}$ such that $x = g^k$. It follows that

$$\rho_A(x) = \rho_A(g^k) = A^k = (TBT^{-1})^k = TB^kT^{-1} = T\,\rho_B(g^k)\,T^{-1} = T\,\rho_B(x)\,T^{-1}.$$

This proves $\rho_A(x) = T\,\rho_B(x)\,T^{-1}$ for all $x \in C_r$ and therefore $\rho_A \sim \rho_B$. $\square$

Lemma 25. *Let $A \in \mathrm{GL}(n, \mathbb{C})$ be of finite order. Then A is diagonalisable.*

Proof. From linear algebra we know that it is enough to show that there exists a nonzero polynomial $f \in \mathbb{C}[t]$ such that $f(A) = 0$ and f has no multiple roots in $\mathbb{C}$.

Let $r > 0$ be such that $A^r = 1$ and put $f := t^r - 1$. Then $f(A) = 0$. In order to prove that f has no multiple roots, assume $\alpha \in \mathbb{C}$ is. Then $0 = f'(\alpha) = r\alpha^{r-1}$ so $\alpha = 0$ so $0 = f(\alpha) = -1$, a contradiction. This proves that f has the required properties. $\square$

Exercise (2.1) Let $a_1, \ldots, a_n \in \mathbb{C}^\times$ and $s \in S_n$. Let A be the diagonal $n \times n$ matrix whose diagonal reads $(a_1, \ldots, a_n)$. Let B be the diagonal $n \times n$ matrix whose diagonal reads $(a_{s1}, \ldots, a_{sn})$. Prove that A, B are conjugate in $\mathrm{GL}(n, \mathbb{C})$.

Let $\omega = \exp(2\pi i/r)$. Then a complex number z satisfies $z^r = 1$ if and only if it is a power of ω.

If $K = (k_0, \ldots, k_{r-1}) \in (\mathbb{Z}_{\geq 0})^r$, let $M(K)$ be the unique diagonal matrix such that:

- Its characteristic polynomial is $\prod_{i=0}^{r-1}(t - \omega^i)^{k_i}$. Thus ω^i appears on the diagonal k_i times, and no other numbers appear on the diagonal.
- If $M(K)_{ii} = \omega^s$, $M(K)_{jj} = \omega^t$ (these are two diagonal entries of M) and $0 \leq s < t \leq r - 1$ then $i < j$.

For example, if $r = 4$ then

$$M(1,2,0,1) = \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \omega & \cdot & \cdot \\ \cdot & \cdot & \omega & \cdot \\ \cdot & \cdot & \cdot & \omega^3 \end{pmatrix}.$$

We can now prove:

Proposition 26: Representations of finite cyclic groups.

(a) *There exists a bijection* $f \colon \mathbb{Z}^r_{\geq 0} \to \mathrm{Rep}(C_r)$ *taking* K *to* $\rho_{M(K)}/\!\sim$*, the equivalence class of* $\rho_{M(K)}$*.*

(b) *If* $K = (k_0, \ldots, k_{r-1}) \in (\mathbb{Z}_{\geq 0})^r$ *then the degree of* $\rho_{M(K)}$ *is* $k_0 + \cdots + k_{r-1}$*.*

Proof. Proof of (a).

Proof that f is well-defined. Let $K \in \mathbb{Z}^r_{\geq 0}$. Then $M(K)^r = 1$ and therefore the representation $\rho_{M(K)}$ of C_r is defined by lemma 24. Therefore f is well-defined.

It remains to prove that f is injective and surjective.

Proof of injectivity. Let $K, L \in \mathbb{Z}^r_{\geq 0}$ be such that $f(K) = f(L)$. Then $\rho_{M(K)} \sim \rho_{M(L)}$. By lemma 24 it follows that $M(K)$ and $M(L)$ are conjugate in $\mathrm{GL}(n, \mathbb{C})$. In linear algebra you have learned that then $M(K)$ and $M(L)$ have the same characteristic polynomial:

$$\prod_{i=0}^{r-1}(t - \omega^i)^{k_i} = \prod_{i=0}^{r-1}(t - \omega^i)^{\ell_i}$$

where we write $K = (k_0, \ldots, k_{r-1})$ and $L = (\ell_0, \ldots, \ell_{r-1})$. It follows that $k_i = \ell_i$ for all i, and therefore $K = L$. This proves that f is injective.

Proof of surjectivity. Let ρ be an n-dimensional representation of C_r. We must prove that ρ is equivalent to a representation of the form $\rho_{M(K)}$ for some $K \in \mathbb{Z}^r_{\geq 0}$.

By lemma 24 we have $\rho \sim \rho_A$ for some $A \in \mathrm{GL}(n, \mathbb{C})$ such that $A^r = 1$. By lemma 25 A is conjugate to a diagonal matrix B.

Note $B^r = 1$. Therefore the entries on the diagonal of B are rth roots of unity. Let $K \in \mathbb{Z}^r_{\geq 0}$ be the unique choice such that $M(K)$ and B have the same entries on the main diagonal but possibly in different order.

By exercise 2.1 $M(K)$ and B are conjugate. Therefore $M(K)$ is conjugate to A. It follows that $\rho_{M(K)} \sim \rho_A \sim \rho$.

Finally part (b) is easy and left to you. □

The method of proof of proposition 26 is rather ad hoc and entirely inadequate, for example, for nonabelian groups. Most of the notes are about a more organised approach to determine the representations of a finite group.

Example 27. Define $A \in \mathrm{GL}(r, \mathbb{C})$ by $A\, e_i = e_{i+1}$ for all i (indices modulo r). Then $A^r = 1$ so ρ_A is a representation of C_r. In the notation of proposition 26, what is $f^{-1}(\rho_A/\!\sim)$?

Solution. Let $v_k = \sum_{i=1}^{r} \omega^{ik} e_i$. Then

$$A\,v_k = A \sum_{i=1}^{r} \omega^{ik} e_i = \sum_{i=1}^{r} \omega^{ik} e_{i+1} = \sum_{i=1}^{r} \omega^{(i-1)k} e_i = \omega^{-k} \sum_{i=1}^{r} \omega^{ik} e_i = \omega^{-k} v_k.$$

This proves that v_k is an eigenvector of A with eigenvalue ω^{-k}. This is true whenever $0 \le k \le r-1$, providing r distinct eigenvalues of A. Due to the size of A the characteristic polynomial of A is $t^r - 1 = \prod_{i=0}^{r-1}(t - \omega^i)$ so $\rho_A/\!\sim\, = f(1, \ldots, 1)$ (r ones). □

2.3 *Exercises*

(2.2) Let G be a group. Let $\rho\colon G \to M(n, \mathbb{C})$ be a map such that $\rho(xy) = \rho(x)\,\rho(y)$ for all $x, y \in G$ and $\rho(1) = 1$ (the identity matrix). Prove that ρ is a representation.

(2.3) Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation. Let $a \in G$ and define $\sigma, \tau\colon G \to \mathrm{GL}(n, \mathbb{C})$ by $\sigma(g) = \rho(aga^{-1})$ and $\tau(g) = \rho(ag)$. Prove that σ is a representation, and that it is equivalent to ρ. Prove that τ is not necessarily a representation by giving a counterexample.

(2.4)

(a) Prove that there exists a unique representation ρ of $C_4 = \{1, g, g^2, g^3\}$ such that $\rho(g) = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

(b) To which tuple $(k_0, \ldots, k_{r-1})$ does ρ correspond as defined in our classification of representations of C_r?

(2.5) Let G be a finite group.

(a) Prove that every element of G has finite order.

(b) Let $A = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. What is A^n for $n \in \mathbb{Z}$? Prove your answer.

(c) Is it possible that G has a representation ρ such that $\rho(x) = A$ for some element $x \in G$?

(2.6) Classify the representations of C_∞ by mimicking our method for C_r, giving all details. You may use anything you know about Jordan normal forms and other linear algebra if you state it.

(2.7) Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation of a group G, and let $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ be given by $\sigma(x) = \rho(x)^2$ for all $x \in G$.

(a) Prove that σ is again a representation if G is abelian.

(b) Prove that σ is again a representation if $n = 1$.

(c) Give an example showing that, in general, σ is not again a representation.

(d) Give an example where σ is again a representation but not equivalent to ρ.

3 Generators and relations

3.1 *Generating sets*

Exercise (3.1) Let G be a group. If $\{H_i \mid i \in I\}$ are subgroups of G then so is their intersection $\bigcap_{i \in I} H_i$.

Definition 28. Let A be a subset of a group G. We define $\langle A\rangle$ to be the intersection of the subgroups of G containing A:

$$\langle A\rangle = \bigcap_{A\subset H\le G} H. \qquad \square$$

For this definition to makes sense there must be at least one H such that $A\subset H\le G$; it exists because one can take $H=G$.

Note that $\langle A\rangle$ is a group by exercise 3.1. It is called the **subgroup of G generated by A**. We also say that A is a **generating set** of the group $\langle A\rangle$. Every group G has a generating set because $G=\langle G\rangle$ but we try to find fewer generators. We say that a group is **finitely generated** if it is has a finite generating set.

Instead of $\langle\{a_1,\dots,a_n\}\rangle$ we write $\langle a_1,\dots,a_n\rangle$. Note $\langle\varnothing\rangle=1$.

Note that $\langle A\rangle$ is the smallest subgroup of G containing A. This can be taken as a second definition of $\langle A\rangle$. Here is a third definition:

Proposition 29. *Let A be a subset of a group G. Then*

$$\langle A\rangle = \{a_1^{d_1}\cdots a_k^{d_k} \mid k\ge 0 \text{ and } a_i\in A,\ d_i\in\{-1,1\} \text{ for all } i\}. \tag{30}$$

Proof. Let B be the right-hand side of (30). We now prove that B is a subgroup of G. Clearly $1\in B$. Let $x,y\in B$, say, $x=a_1^{d_1}\cdots a_k^{d_k}$, $y=b_1^{e_1}\cdots b_\ell^{e_\ell}$ where $a_i,b_j\in A$, $d_i,e_j\in\{-1,1\}$. Then $xy^{-1}=a_1^{d_1}\cdots a_k^{d_k}b_\ell^{-e_\ell}\cdots b_1^{-e_1}\in B$, proving that $B\le G$. It follows that $\langle A\rangle\subset B$.

Conversely, let $x\in B$, say, $x=a_1^{d_1}\cdots a_k^{d_k}$ where $a_i\in A$ and $d_i\in\{-1,1\}$. Since $\langle A\rangle\le G$ it follows that $x=a_1^{d_1}\cdots a_k^{d_k}\in\langle A\rangle$. Therefore $B\subset\langle A\rangle$. $\square$

It is now clear that a cyclic group is just a group generated by only one element g. The language, introduced in definition 7, of calling g a generator, agrees with what we have learned in the present section.

For another example, the dihedral group of section 1.5 is generated by $\{r,s\}$.

3.2 Normal subgroups

Notation 31. If A,B are subsets of a group G then we write $AB=\{ab \mid a\in A,\ b\in B\}$. We also write $aB:=\{a\}B$ and $Ab:=A\{b\}$.

Definition 32. Let H be a subgroup of a group G. A set of the form Hx (with $x\in G$) is called a **left coset (with respect to H)** and xH a **right coset**. Let $H\backslash G$ be the set of left cosets and G/H the set of right cosets.

Exercise (3.2) Let $H\le G$.

(a) Prove that G is the disjoint union of the left cosets with respect to H.

(b) Prove that G/H and $H\backslash G$ have equal cardinalities. It is called the **index** of H in G and written $[G:H]$. It is a positive integer or ∞. Note that $[G:H]$ may be finite even if G is infinite.

Definition 33. A **normal subgroup** of a group G is a subgroup $N\subset G$ such that $Nx=xN$ for all $x\in G$. Notation: $N\trianglelefteq G$.

Let N be a subgroup of a group G. Another way of saying $N\trianglelefteq G$ is $xNx^{-1}=N$ for all x. Again equivalent is that every left coset is a right coset and vice versa.

Exercise (3.3) Let G be a group. If $\{H_i \mid i \in I\}$ are normal subgroups of G then so is their intersection $\bigcap_{i\in I} H_i$.

Definition 34. Let A be a subset of a group G. We define $\langle\!\langle A\rangle\!\rangle_G = \langle\!\langle A\rangle\!\rangle$ to be the intersection of the normal subgroups of G containing A:

$$\langle\!\langle A\rangle\!\rangle = \bigcap_{A\subset H\trianglelefteq G} H. \qquad \square$$

Note that $\langle\!\langle A\rangle\!\rangle \trianglelefteq G$ by exercise 3.3. It is called the subgroup of G **normally generated by A** or the **normal closure in G of A**.

Sometimes $\langle\!\langle A\rangle\!\rangle_G$ is a better notation because of the way it depends on G; see exercise 3.20.

A second characterisation of $\langle\!\langle A\rangle\!\rangle$ is as the smallest normal subgroup of G containing A. See exercise 3.30 for a third characterisation.

A group G is said to be **simple** if it has no other normal subgroup than 1 and G. One of the greatest achievements of mathematics is the classification of finite simple groups. Originally this took 15,000 pages and it's beyond our scope.

3.3 Quotient groups

Assume $N \trianglelefteq G$. Recall that then $N\backslash G = G/N$. In words: every left coset is a right coset and vice versa. Recall our definition $AB := \{ab \mid a \in A,\ b \in B\}$ for subsets $A, B \in G$.

We claim that if $A, B \in G/N$ then $AB \in G/N$. Indeed, writing $A = Nx$, $B = Ny$ we have $AB = NxNy = NNxy = Nxy \in G/N$. Prove yourself that this multiplication makes G/N into a group.

Definition 35. Let $N \trianglelefteq G$. We call G/N with the above multiplication the **quotient group** of G by N.

Example 36. (a). $G/1 \cong G$.

(b) $G/G \cong 1$.

(c) Let $C_\infty = \langle g\rangle$ and $N = \langle g^r\rangle$ $(r \geq 1)$. Then N is a normal subgroup of C_∞ and $C_\infty/N \cong C_r$.

Exercise (3.4) Prove that $\langle r\rangle$ is a normal subgroup of the dihedral group D_{2n}.

Definition 37. Let $f\colon G \to H$ be a homomorphism of groups. The **kernel** of f is $\ker(f) = \{x \in G \mid f(x) = 1\}$ and the **image** of f is $\mathrm{im}(f) = \{f(x) \mid x \in G\}$.

An important observation is now:

Exercise (3.5) Let $f\colon G \to H$ be a homomorphism of groups.

(a) The kernel of f is a normal subgroup of G.

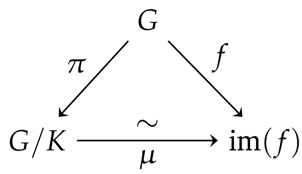
(b) The image of f is a subgroup of H.

Proposition/Definition 38. *Let $N \trianglelefteq G$. The* **natural map** $\pi\colon G \to G/N$ *is defined by $\pi(x) = Nx$. It is a surjective homomorphism of groups and its kernel is N.*

Proof. For all $x \in G$ we have $Nx = xN$ because N is a normal subgroup. For all $x, y \in G$ we have $\pi(x)\,\pi(y) = NxNy = NNxy = Nxy = \pi(xy)$ so π is a homomorphism. It is surjective by definition.

For all $x \in G$ we have $x \in \ker(\pi) \Leftrightarrow \pi(x) = 1 \Leftrightarrow Nx = N \Leftrightarrow x \in N$ which proves that $\ker(\pi) = N$. $\square$

Theorem 39: First isomorphism theorem for groups. *Let $f\colon N \to G$ be a homomorphism of groups with kernel K. Then there exists a unique isomorphism $\mu\colon G/N \to \mathrm{im}(f)$ such that $f = \mu \circ \pi$:*



Proof. See any textbook on group theory. $\square$

The diagram in theorem 39 is said to commute if $f = \mu \circ \pi$. In general, a **diagram** has a bunch of **objects** which could be sets, groups, vector spaces, and so on.

Further there are **arrows**. Each arrow points from its **source object** to its **target object**. Every arrow is labelled by a **map** from its source object to its target object. The source (respectively, target) object of an arrow are also called the source (respectively, target) object of the associated map.

If the objects are groups, the maps are often homomorphisms; for vector spaces they are often linear maps, and so on; but these are by no means necessary.

A diagram is said to **commute** or to be **commutative** if $f_1 \cdots f_k = g_1 \cdots g_\ell$ whenever there are arrow labels f_i, g_j such that:

- The source of f_i is the target of f_{i+1} for all i.
- The source of g_j is the target of g_{j+1} for all j.
- f_k and g_ℓ have equal sources.
- f_1 and g_1 have equal targets.

3.4 Orderings

Let S be a set and R a subset of the Cartesian product $S \times S$. We say that R is a **(binary) relation on S**. Instead of $(x, y) \in R$ we often write xRy; moreover $xRyRz$ means xRy and yRz.

Here are some properties R may or may not have:

- R is said to be **reflexive** if xRx for all $x \in S$.
- R is said to be **transitive** if $(xRyRz \Rightarrow xRz)$ for all $x, y, z \in S$.
- R is said to be **symmetric** if $(xRy \Rightarrow yRx)$ for all $x, y \in S$.
- R is said to be **anti-symmetric** if $(xRyRx \Rightarrow x = y)$ for all $x, y \in S$.

You already know that R is defined to be an equivalence relation if it is reflexive, transitive and symmetric. Equivalence relations are often written $\sim$ instead of R.

We call R an **ordering** (some people say partial ordering) if it is reflexive, transitive and anti-symmetric. Orderings are often written $\leq$ instead of R (or $\geq$ of course). By an **ordered set** we mean a pair $(S, \leq)$ of a set S and an ordering $\leq$ on it.

Example 40. Let X be a set. The **power set $P(X)$** is the set of subsets of X. So if $\#X = n$ then $\#P(X) = 2^n$. Let $R \subset P(X) \times P(X)$ be the **relation of inclusion**, that is, aRb if and only if $a \subset b$. Then R is an ordering.

A **total ordering** or **linear ordering** on a set S is an ordering $\leq$ such that for all $x, y \in S$ one has $(x \leq y$ or $y \leq x)$. There are two clashing terminologies:

our terminology:	ordering	total ordering
old-fashioned terminology:	partial ordering	ordering

.

Not all orderings are total, as is shown by the above example of the power set $P(X)$ when it is ordered by inclusion. An example of a total ordering is the usual ordering on $\mathbb{R}$.

Let $\leq$ be an ordering on a set S. We introduce three more relations $\geq$, $<$ and $>$ by the following well-known rules:

$$x \geq y \Leftrightarrow y \leq x$$
$$x < y \Leftrightarrow (x \leq y \text{ and } x \neq y)$$
$$x > y \Leftrightarrow y < x.$$

This neat trick is of course not possible if you use R instead of $\leq$.

Note that $<$ is not an ordering; it is a special kind of binary relation which one may call strict ordering. But $\geq$ is again an ordering known as the opposite of $\leq$.

3.5 Free groups

Let A be a set. In this setting, A is often called an **alphabet** and its elements **letters** or **generators**. A **word** over A is a sequence of pairs

$$(\binom{e_1}{a_1}, \ldots, \binom{e_k}{a_k}) \tag{41}$$

such that $k \geq 0$ and $a_i \in A$ and $e_i \in \{-1, 1\}$ for all i. The above word is said to have length k. We write $\ell(u)$ for the length of a word u. There is precisely one word of length 0; it is called the empty word and written 1. The set of words over A will be written A^*.

If A is a subset of a group G then a word (41) gives rise to an element

$$a_1^{e_1} \cdots a_k^{e_k} \tag{42}$$

of G. Confusingly, people usually write (42) when they mean (41). This is a great cause of confusion! But everybody does it and we don't want to get left behind. So from now on we may write (42) when we mean (41). If in doubt, try reverting to the earlier notation.

The **product** uv of two words

$$u = (\binom{d_1}{a_1}, \ldots, \binom{d_k}{a_k}), \qquad v = (\binom{e_1}{b_1}, \ldots, \binom{e_\ell}{b_\ell})$$

is defined by concatenation:

$$uv = (\binom{d_1}{a_1}, \ldots, \binom{d_k}{a_k}, \binom{e_1}{b_1}, \ldots, \binom{e_\ell}{b_\ell}).$$

Note that $\ell(uv) = \ell(u) + \ell(v)$ for all $u, v \in A^*$.

We define the **inverse** of the above word u by

$$u^{-1} = (\binom{-d_k}{a_k}, \ldots, \binom{-d_1}{a_1}).$$

Note that this doesn't make A^* into a group, because uu^{-1} is not the empty word unless u is empty. Instead we have

$$uu^{-1} = (\binom{d_1}{a_1}, \dots, \binom{d_k}{a_k}, \binom{-d_k}{a_k}, \dots, \binom{-d_1}{a_1}).$$

Associativity ($(uv)w = u(vw)$ for all $u, v, w \in A^*$) is true though and trivial.

Definition 43.

(a) Let u, v be words over A and $a \in A$ a letter. We say that uv is a **one-step reduction** of both $uaa^{-1}v$ and $ua^{-1}av$. We also write $u \to v$ if v is a one-step reduction of u.

(b) Let $\geq$ be the reflexive-transitive closure of $\to$. Equivalently, $u \geq v$ if and only if there exists a sequence of words $u = w_0 \to w_1 \to \cdots \to w_k = v$ with $k \geq 0$.

(c) Associated with $\geq$ are three more relations $\leq$, $>$, $<$ in the usual way. For example $u > v$ is equivalent to $u \geq v$ and $u \neq v$. □

If $u > v$ then $\ell(u) > \ell(v)$. The converse is not true of course. It follows that $\geq$ is an ordering.

Definition 44. A word u over A is said to be **reduced** if there is no smaller word, that is, no word v over A such that $u > v$. The set of reduced words over A is written $F(A)$. □

Thus a word is reduced if and only if it is not of the form $uaa^{-1}v$ or $ua^{-1}av$ for words u, v over A and $a \in A$.

By a **lower bound** for u we mean any v such that $u \geq v$. So a reduced lower bound of a word u is a reduced word v such that $u \geq v$.

Example 45. Let $a, b, c, d \in A$ be distinct and $w = a\,b^{-1}\,c\,c^{-1}\,b\,d\,a^{-1}$. Then

$$w = a\,b^{-1}\,c\,c^{-1}\,b\,d\,a^{-1} \to a\,b^{-1}\,b\,d\,a^{-1} \to a\,d\,a^{-1},$$

and the latter is reduced. Thus $a\,d\,a^{-1}$ is a reduced lower bound of w.

The following lemma is the key to understanding free groups.

Lemma/Definition 46: Reduced lower bound. *Let u be a word over A. Then u has a unique reduced lower bound. It is denoted* $\mathrm{R}(u)$.

Proof. Existence is an easy exercise.

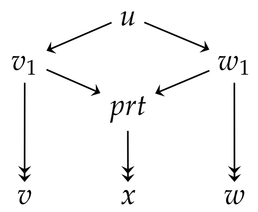
We prove uniqueness by induction on the length of u. It is true if $\ell(u) \leq 1$ because then the only possible value for v is $v = u$. Supposing that uniqueness is known if $\ell(u) \leq k$ we prove it if $\ell(u) \leq k + 2$. We may clearly suppose that u is not itself reduced.

Let v, w be reduced lower bounds of u. We must show that $v = w$. By definition of the ordering there are words v_1, w_1 such that $u \to v_1 \geq v$ and $u \to w_1 \geq w$ (since u is not reduced).

Some letters in u are removed in the one-step reduction from u to v_1 and some are from u to w_1. Let us say that there is **overlap** if there is a letter that is removed both times.

Suppose first that there is no overlap. After interchanging v and w if necessary there are words p, q, r, s, t over A such that $u = pqrst$ and $v_1 = prst$ and $w_1 = pqrt$ (of course, q and s are nonreduced words of length 2). Then $v_1 \to prt$ and $w_1 \to prt$.

Let x be any reduced lower bound of prt. Writing $\twoheadrightarrow$ instead of $\geq$ the situation is summarized by the following diagram.



Then v, x are two reduced lower bounds of v_1. But there is only one, by the inductive hypothesis and because $\ell(v_1) < \ell(v)$. So $v = x$. For the same reason $w = x$ and so $v = w$ as required.

Finally suppose that there is overlap. After interchanging v and w if necessary there are words p, q, a over A with $\ell(a) = 1$ (that is, a is a letter or the inverse of a letter) such that $u = p\,a\,a^{-1}\,a\,q$ and v_1 (respectively, w_1) is obtained from u by removing the shown $a\,a^{-1}$ (respectively, $a^{-1}\,a$). This implies $v_1 = paq = w_1$. Now $\ell(v_1) < \ell(v)$ so by the induction hypothesis v_1 has a unique reduced lower bound. But v and w are reduced lower bounds of v_1. Therefore $v = w$ as required.

This proves the induction step and thereby the lemma. □

Exercise (3.6) Prove:

(a) Let $u, v \in A^*$ and $u \leq v$. Then $\mathrm{R}(u) = \mathrm{R}(v)$.

(b) Let $u, v, w, x \in A^*$ be such that $u \leq v$ and $w \leq x$. Then $uw \leq vx$.

(c) Let $u, v \in A^*$. Then

$$\mathrm{R}(\mathrm{R}(u)\,v) = \mathrm{R}(uv) = \mathrm{R}(u\,\mathrm{R}(v)). \tag{47}$$

Definition 48. Let u, v be reduced words over A. We define $u * v := \mathrm{R}(uv)$.

Example 49. Continuing from example 45 we find

$$a\,b^{-1}\,c * c^{-1}\,b\,d\,a^{-1} = \mathrm{R}(a\,b^{-1}\,c\,c^{-1}\,b\,d\,a^{-1}) = a\,d\,a^{-1}.$$

Theorem/Definition 50. *The pair* $(F(A), *)$ *is a group, called the* **free group on** $\boldsymbol{A}$. *(Any group isomorphic to it is also called a free group.)*

Proof. Firstly, $F(A)$ contains the empty word (written 1) and is hence not empty, even if A is empty. Secondly, it is clear that $u * 1 = 1 * u = u$ for all $u \in F(A)$. Prove yourself $u * u^{-1} = u^{-1} * u = 1$ for all $u \in F(A)$ (even though $uu^{-1} \neq 1$!). It remains to prove that the star product is associative. Let $u, v, w \in A^*$. Using (47) twice we find

$$\begin{aligned}(u * v) * w &= \mathrm{R}((u * v)w) = \mathrm{R}(\mathrm{R}(uv)w) = \mathrm{R}((uv)w) \\ &= \mathrm{R}(u(vw)) = \mathrm{R}(u\,\mathrm{R}(vw)) = \mathrm{R}(u(v * w)) = u * (v * w).\end{aligned}$$

□

Remark 51. (a). The group operation in $F(A)$ is often written uv instead of $u * v$. Watch out not to confuse this with the concatenation of words.

(b). It is common to consider A as a subset of $F(A)$. Then $F(A)$ is generated by A.

Example 52. (a). $F(\varnothing) = 1$.

(b). We claim that a free group on one letter is an infinite cyclic group. To prove this, write $F = F(\{a\})$. A sequence $aa \cdots a$ of n copies of a is a reduced word. All of these are elements of F and therefore F is infinite. Moreover F is generated by a so $F \cong C_\infty$.

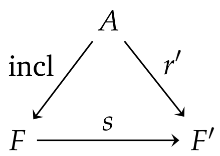
We write $F(a_1, \ldots, a_n)$ instead of $F(\{a_1, \ldots, a_n\})$.

For sets A, B we claim $F(A) \cong F(B) \iff \#A = \#B$. The implication $\Leftarrow$ is trivial. We shall not prove $\Rightarrow$.

It follows that up to isomorphism $F(a_1, \ldots a_n)$ depends only on n. It is often written F_n.

The famous Nielsen-Schreier theorem (outside our scope) states that every subgroup of a free group is again (isomorphic to) a free group. There exists a wieldy algebraic proof. A different topological proof is based on the observation that free groups are the same as fundamental groups of connected graphs.

Theorem 53: Universal property for free groups. *Let A be a set and write $F = F(A) \supset A$. Let F' be a group and $r' \colon A \to F'$ be a map. Then there exists a unique homomorphism $s \colon F \to F'$ such that $s(a) = r'(a)$ for all $a \in A$.*



Proof. Unicity is an **exercise**.

Proof of existence. We shall find it convenient to define $s(u)$ for every word u over A, not just the reduced ones. For $u \in A^*$, we define $s(u)$ the obvious way, that is, by replacing each letter $a \in A$ by $r'(a)$. Explicitly:

$$s(a_1^{d_1} \cdots a_k^{d_k}) = \big(r'(a_1)\big)^{d_1} \cdots \big(r'(a_k)\big)^{d_k}.$$

It is clear that $s(a) = r'(a)$ for all $a \in A$.

It remains to prove that the restriction $s|_F$ is a group homomorphism $F \to F'$. First notice that if v is a one-step reduction of u then $s(v) = s(u)$. It follows that $s(\mathrm{R}(u)) = s(u)$ for all u. Finally we find

$$s(u * v) = s(\mathrm{R}(uv)) = s(uv) = s(u)\, s(v). \qquad \square$$

Remark 54. The universal property as stated in theorem 53 **characterises** the free group on A, that is, up to isomorphism the free group on A is the only gadget satisfying the universal property. See exercise 3.27.

Proving this is even easier than understanding the free group! What's more, it still works for silly more complicated identities like $(ab)c = (cb)(ac)$ instead of associativity.

In this module we hardly ever use any understanding of the free group on A other than that it is essentially the only gadget satisfying the universal property. You often see this if there is a universal property around. We won't use the stuff on reduced words but in other areas people do.

3.6 Presentations of groups

Definition 55. (a). A **group presentation** is a pair (A, R) where A is a set of **generators** and $R \subset F(A)$ a subset of **relations**.

(b). Associated with a group presentation (A, R) is a group $\langle A \mid R \rangle := F(A)/\langle\!\langle R \rangle\!\rangle$. We say that (A, R) is a presentation of $\langle A \mid R \rangle$ and any group isomorphic to it. We also say that $\langle A \mid R \rangle$ is **defined by generators A and relations R.**

(c). We allow various equivalent ways to write relations. For example $xyx^{-1}y^{-1}$ and $xyx^{-1}y^{-1} = 1$ and $xy = yx$ are three different ways to write the same relation.

Let (A, R) be a group presentation. There is a natural map $A \to \langle A \mid R \rangle$ which is the composition of the maps $A \to F(A) \to \langle A \mid R \rangle$. It is common to identify A with its image in $\langle A \mid R \rangle$. Also, one writes down a word over A and considers it an element of $\langle A \mid R \rangle$. This is a great cause of confusion, so watch out!

The natural map $A \to \langle A \mid R \rangle$ may not be injective as is shown by the example $\langle a, b \mid aa = ab \rangle$.

Corollary 56. *Let G be a group.*

(a) *There exists a surjective homomorphism from some free group to G.*

(b) *There exists a presentation of G.*

Proof. Proof of (a). Let $A \subset G$ be any generating subset for G (for example, $A = G$). By the universal property theorem 53 (with $F' = G$ and $r'(a) = a$ for all a) there exists a unique homomorphism $s \colon F(A) \to G$ such that $s(a) = a$ for all a. Then the image of s contains A and therefore $\langle A \rangle$. Therefore s is surjective.

Proof of (b). Let R be the kernel of s. By the first isomorphism theorem (theorem 39) we have $F(A)/R \cong G$. Also $\langle\langle R \rangle\rangle = R$ so $\langle A \mid R \rangle = F(A)/\langle\langle R \rangle\rangle = F(A)/R \cong G$. □

Example 57. For $r \geq 1$ we have $C_r \cong \langle a \mid a^r \rangle$. Indeed, by example 52b and example 36c we have $\langle a \mid a^r \rangle = F(a)/\langle\langle a^r \rangle\rangle = F(a)/a^r \cong C_r$.

Definition 58. Let (A, R) be a group presentation and write $A = \{a(i) \mid i \in I\}$. Let H be a group and let $\{h(i) \mid i \in I\}$ be elements of H indexed by the same index set I. We say that $\{h(i) \mid i \in I\}$ **satisfy** R if

$$h(i_1)^{d_1} \cdots h(i_n)^{d_n} = 1 \tag{59}$$

whenever

$$a(i_1)^{d_1} \cdots a(i_n)^{d_n} \in R, \qquad i_k \in I \text{ and } d_k \in \{-1, 1\} \text{ for all } k. \tag{60}$$

We now come to a very useful result generalising the universal property for free groups.

Theorem 61. *Let (A, R) be a group presentation and write $A = \{a(i) \mid i \in I\}$. Let H be a group and let $\{h(i) \mid i \in I\}$ be elements of H indexed by the same index set I. Then the following are equivalent.*

(1) *There exists a homomorphism $f \colon \langle A \mid R \rangle \to H$ such that $f(a(i)) = h(i)$ for all $i \in I$.*

(2) *The elements $\{h(i) \mid i \in I\}$ satisfy R.*

If these are satisfied then f is unique.

Proof. Unicity of f follows immediate from the fact that G is generated by A.

Write $N = \langle\langle R \rangle\rangle$ and $G = \langle A \mid R \rangle = F(A)/N$. Let p denote the natural map $F(A) \to G$. By theorem 53 there exists a unique homomorphism $s \colon F(A) \to H$ such that $s(a(i)) = h(i)$ for all i. Then

$$\begin{aligned} (2) &\iff s(r) = 1 && \text{for all } r \in R \\ &\iff s(r) = 1 && \text{for all } r \in N \\ &\iff s(x) = s(y) && \text{whenever } p(x) = p(y). \end{aligned} \tag{62}$$

In this notation we should write $f(pa(i))$ instead of $f(a(i))$.

Proof of (1) $\Rightarrow$ (2). We have $f(px) = sx$ for all $x \in A$ and therefore for all $x \in F(A)$. Write r instead of x where $r \in R$. Then $p(r) = 1$ so $s(r) = 1$ as required.

Proof of (2) $\Rightarrow$ (1). Define $f(px) := s(x)$ for all $x \in F(A)$. For this to be well-defined we need two observations:

- $p\colon F(A) \to G$ is surjective.
- $s(x) = s(y)$ whenever $p(x) = p(y)$.

The first is clearly true and the second is true by (62).

It is clear that $f(px) = s(x)$ for all $x \in A$. We prove that f is a homomorphism as follows: for all $x, y \in F(A)$ we have

$$f(p(x)\, p(y)) = f(p(xy)) = s(xy) = s(x)\, s(y) = f(px)\, f(py). \qquad \square$$

Example 63. Prove that $D_{2n} \cong \langle x, y \mid x^n, y^2, (xy)^2 \rangle$.

Solution. Let G be the group on the right-hand side. It is straightforward to prove that r, s satisfy the relations $x^n, y^2, (xy)^2$, that is, $r^n = 1$ and so on. By theorem 61 there is a unique homomorphism $f\colon G \to D_{2n}$ such that $f(x) = r$ and $f(y) = s$. Also f is surjective because D_{2n} is generated by r, s by lemma 13. We are left to prove that f is injective.

Let $g \in G$. Then g can be represented by a word in $\{x, y\}$. We aim to replace the word by simpler words also representing g.

We have

$$yx = x^{-1}y, \quad yx^{-1} = xy, \quad y^{-1}x = x^{-1}y^{-1}, \quad y^{-1}x^{-1} = xy^{-1}.$$

We use these repeatedly to push the y's to the right until we can't do this any longer. Then we repeatedly remove any occurrence of xx^{-1}, $x^{-1}x$, yy^{-1} or $y^{-1}y$. We end up with a word of the form $x^k\, y^\ell$. So g can be represented by a word of the form $x^k\, y^\ell$.

But $x^n = 1$ and $y^2 = 1$ so $G = \{x^k,\ x^k\, y \mid 0 \le k < n\}$. Therefore $\#G \le 2n = \#D_{2n}$. It follows that f is an isomorphism. $\square$

Example 64. There exists a unique representation $\rho\colon D_8 \to \mathrm{GL}(2, \mathbb{C})$ such that $\rho(r) = A$, $\rho(s) = B$ where $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Solution. By example 63 $D_8 = \langle r, s \mid r^4, s^2, (rs)^2 \rangle$. The result now follows from theorem 61 and the observation (do this yourself) that A, B satisfy the relations r^4, s^2, $(rs)^2$. $\square$

For integers $p, q, r \ge 2$ let us define the **triangle groups**

$$T(p, q, r) = \langle x, y \mid x^p, y^q, (xy)^r \rangle.$$

It is known that:

- $T(p, q, r)$ is finite if and only if $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$.
- $T(p, q, r)$ contains a finite index subgroup isomorphic to $\mathbb{Z}^2$ if and only if $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$.

There is a beautiful geometric proof of these which is outside our scope. For example,

$$\begin{aligned} T(n, 2, 2) &\cong D_{2n}, \\ T(2, 3, 3) &\cong A_4 \qquad \text{(see exercise 3.32)}, \\ T(2, 3, 5) &\cong A_5. \end{aligned}$$

3.7 Exercises

(3.7) Let S_4 denote the symmetric group on $\{1,2,3,4\}$. Consider the elements $a = (12)(34)$, $b = (13)(24)$, $c = (14)(23)$ of S_4 and write $V = \{1, a, b, c\} \subset S_4$.

(a) Prove that V is a normal subgroup of S_4. You may reduce the amount of calculations by using the following observations which you don't need to prove:

(1) If $x, y \in \{a, b, c\}$ and $x \neq y$ then there exists $g \in S_4$ such that $gxg^{-1} = a$ and $gyg^{-1} = b$.

(2) If $x \in V$ and $g \in S_4$ then $gxg^{-1} \in V$.

(b) Which well-known groups are isomorphic to V and S_4/V? In your proof you may assume the classification of groups of small order. Give explicit isomorphisms without proof.

(3.8) Show that if G is an abelian group which is simple, then G is cyclic of prime order.

(3.9) Suppose that G is a subgroup of S_n and that G is not contained in A_n. Prove that $G \cap A_n$ is a normal subgroup of G and that $G/(G \cap A_n) \cong C_2$.

(3.10) Prove existence in the proof of lemma 46: Every word has a unique reduced lower bound.

(3.11) Prove unicity in the proof of theorem 53: Universal property for free groups.

(3.12) True or false? Prove or disprove each statement.

(a) Let a be an element of a group G. Then the order of a is the order of $\langle a \rangle$.

(b) $\mathbb{Z} \setminus \{17\}$ is a subgroup of $\mathbb{Z}$.

(c) Every subgroup of a cyclic group is cyclic.

(d) Let A, B be two subgroups of a group G. Then $A \cap B$ is also a subgroup of G.

(e) Let A, B be two subgroups of a group G. Then $A \cup B$ is also a subgroup of G.

(f) Let A, B be two subgroups of an abelian group G. Then $\{ab \mid a \in A,\ b \in B\}$ is also a subgroup of G.

(g) Let A, B be two subgroups of a group G. Then $\{ab \mid a \in A,\ b \in B\}$ is also a subgroup of G.

(h) Let a be an element of a group G such that $\langle\!\langle a \rangle\!\rangle = G$. Then G is cyclic.

(3.13) Let G be a group and H a subgroup such that $\#G/H = 2$, that is, there are precisely 2 cosets xH in G. Prove that H is normal in G.

(3.14) Prove that D_{2m} is presented by $\langle x, y \mid x^2, y^2, (xy)^m \rangle$.

(3.15) Find all subgroups of S_3. Which are normal subgroups? For all normal subgroups N of S_3, find a standard group which is isomorphic to S_3/N.

(3.16) Write $G = \langle x, y \mid x^2, y^2, (xy)^2 \rangle$.

(a) Prove that $G \cong C_2 \times C_2$.

(b) Prove that there are unique representations ρ, σ, τ of G such that

$$\rho(x) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \rho(y) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \sigma(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\sigma(y) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \tau(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \tau(y) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

(c) Which among ρ, σ, τ are equivalent?

(3.17) Find an example of a nontrivial cyclic group G, a generating subset A of G, and two inequivalent representations $\rho, \sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ of G such that for all $a \in A$ there exists $T_a \in \mathrm{GL}(n, \mathbb{C})$ with $\sigma(a) = T_a\, \rho(a)\, T_a^{-1}$.

(3.18) True or false?

(a) Let Q, N be groups. Then there exists a surjective homomorphism $f\colon Q \times N \to Q$ whose kernel is isomorphic to N.

(b) Let $f\colon G \to Q$ be a surjective group homomorphism and let N denote its kernel. Then $G \cong Q \times N$.

(3.19) Let ρ be a representation of a group G of degree 1. Prove that $G/\ker \rho$ is abelian.

(3.20) Let A be a subset of G. The subgroup of G generated by A will be denoted $\langle A \rangle_G$, and the normal subgroup $\langle\!\langle A \rangle\!\rangle_G$. This more informative notation is necessary in this exercise.

Let $H \subset G$ be groups and A a subset of H.

(a) Prove that $\langle A \rangle_H = \langle A \rangle_G$.

(b) Give an example where $\langle\!\langle A \rangle\!\rangle_G \neq \langle\!\langle A \rangle\!\rangle_H$.

(c) Prove or disprove the following. Suppose that H is a normal subgroup of G. Then $\langle\!\langle A \rangle\!\rangle_G = \langle\!\langle A \rangle\!\rangle_H$.

(3.21) Prove that $\langle a, b, c, d \mid ab = c,\ bc = d,\ cd = a,\ da = b \rangle$ is cyclic and find its order.

(3.22) Prove that $\langle x, y \mid y^{-1}x^n y = x^{n+1},\ x^{-1}y^n x = y^{n+1} \rangle$ is a trivial group, for all $n \in \mathbb{Z}$.

(3.23) Prove that $\langle x, y \mid xyx = y,\ yxy = x \rangle$ and $\langle a, b \mid a^2 = b^2,\ a^{-1}ba = b^{-1} \rangle$ are isomorphic groups. You're not supposed to use anything about group presentations that we didn't learn in the lectures.

(3.24) Let A be a generating subset of a group G. Suppose that every two elements of A commute. Prove that G is abelian.

(3.25) Classify the representations of D_{2n} of degree 1.

(3.26) Let G be the group presented by $\langle a, b \mid aba = bab \rangle$.

(a) Find all homomorphisms $G \to S_3$.

(b) Find all 1-dimensional representations of G.

(3.27) Let A be a set. A **universally free group** on A is a pair (F, r) of a group F and a map $r\colon A \to F$ with the following property. Let F' be a group and $r'\colon A \to F'$ be a map. Then there exists a unique homomorphism $s\colon F \to F'$ such that $s(r(a)) = r'(a)$ for all $a \in A$.

(a) Prove directly from the definition that universally free groups are unique. More precisely, if (F_1, r_1) and (F_2, r_2) are universally free groups then there exists a homomorphism $s\colon F_1 \to F_2$ such that $r_2 = s\, r_1$.

(b) Prove that universally free groups exist directly from the definition. The group $F(A)$ is one of them by theorem 53 but you're not supposed to use that here.

(3.28) In this exercise, you should prove things directly from the definition of universally free group as defined in exercise 3.27.

(a) The universally free group on 2 generators is not abelian.

(b) If $\#A = \#B$ then the universally free group on A is isomorphic to the universally free group on B.

(3.29) Let A be an alphabet of k elements. How many words u of length $2n$ over A are there such that $\mathrm{R}(u) = 1$?

(3.30) Let A be a subset of a group G and $B = \{gag^{-1} \mid g \in G,\ a \in A\}$. Prove that $\langle\!\langle A \rangle\!\rangle = \langle B \rangle$.

(3.31) Let G, H be groups. Suppose we have a map $H \times G \to H\colon (x, a) \mapsto x^a$ which is an **action** (that is, $x^{ab} = (x^a)^b$ and $x^1 = x$ for all $x \in H, a, b \in G$) by **group automorphisms** (that is, $(xy)^a = x^a y^a$ for all $x, y \in H$, $a \in G$). On the set $G \times H$ we define the binary operation

$$(a, x)(b, y) := (ab, x^b y).$$

(a) Prove that this binary operation makes $G \times H$ into a group. It is called an **external semi-direct product** and written $G \ltimes H$.

Let G, H be subgroups of a group P and write $GH := \{gh \mid g \in G,\ h \in H\}$. We say that P is an **internal semi-direct product** of G, H if $H \trianglelefteq P$, $G \cap H = 1$, $P = GH$. We also say that (P, G, H) is an internal semi-direct product.

(b) Prove that an external semi-direct product $G \ltimes H$ is an internal semi-direct product of two subgroups, one isomorphic to G, one to H.

(c) (Not for credit). Prove the following converse. Let (P, G, H) be an internal semi-direct product. Then there exists an action by automorphisms $H \times G \to H\colon (x, a) \mapsto x^a$ such that $G \ltimes H \cong P$.

(d) Let G, H be subgroups of a finite group P. Suppose $H \trianglelefteq P$ and $G \cap H = 1$. Prove that (P, G, H) is an internal semi-direct product if and only if $\#P = \#G \cdot \#H$.

(e) Give an example where the group $G \ltimes H$ (internal or external as you prefer) is not isomorphic to $G \times H$.

(f) (Not for credit). Let G be a group. We define an action by automorphisms $G \times G \to G\colon (x, a) \mapsto x^a := a^{-1} x a$. Prove that $G \ltimes G \cong G \times G$ as groups.

(3.32) (Adopted from the 2011 exam.) Put $G = \langle x, y \mid x^2, y^3, (xy)^3 \rangle$ and consider the elements $a = (12)(34)$ and $b = (123)$ of the alternating group A_4.

(a) Prove that there exists a unique homomorphism $f\colon G \to A_4$ such that $f(x) = a$, $f(y) = b$.

(b) Consider the subgroup $H = \langle y \rangle$ of G and the set of cosets

$$A = \{H,\ xH,\ yxH,\ y^2xH\}.$$

Prove $xyxH \in A$.

(c) Justify that $zC \in A$ for all $z \in \{x, y\}$ and $C \in A$ by writing down, without proof, a table which for all $z \in \{x, y\}$ and $C \in A$ gives an element $g \in \{1, x, yx, y^2 x\}$ such that $zC = gH$.

(d) Prove $gH \in A$ for all $g \in G$.

(e) Prove that $f\colon G \to A_4$ is an isomorphism. You may assume that it is surjective.

4 Modules

4.1 Modules

Throughout these notes, a vector space is always over $\mathbb{C}$.

Definition 65. Let G be a group and V a complex vector space. An **action** of G on V (by linear maps) is a map

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, v) &\longmapsto gv \end{aligned}$$

such that:

(1) $g(hv) = (gh)v$ for all $g, h \in G$, $v \in V$.

(2) $1v = v$ for all $v \in V$.

(3) $g(au + bv) = a(gu) + b(gv)$ for all $u, v \in V$, $a, b \in \mathbb{C}$, $g \in G$.

Note that (1) and (2) say that G acts on V as a set; (3) says that $v \mapsto gv$ is a linear map, for all $g \in G$.

Example 66. Let $C_r = \langle g \mid g^r \rangle$. Let $\{v_i \mid i \in \mathbb{Z}/r\}$ be a basis of a vector space V. We define a C_r-action on V by $g^k v_i = v_{i+k}$ (extended by linearity). We claim that this is a C_r-action on V. Axioms (2) an (3) are clearly satisfied. Furthermore $g^k(g^\ell v_i) = g^k v_{i+\ell} = v_{i+k+\ell} = g^{k+\ell} v_i = (g^k g^\ell) v_i$ for all v_i and hence by linearity $g^k(g^\ell v) = (g^k g^\ell)v$ for all $v \in V$, thus proving axiom (1).

Definition 67. Let G be a group. A $\mathbb{C}$***G*-module** is a vector space V together with a G-action on it.

Remark 68. Throughout the notes we ignore the connection between $\mathbb{C}G$-modules and modules over rings, to keep things simple. But here it is in a nutshell. There is a ring $\mathbb{C}G$ known as the group algebra of G. Its modules in the sense of ring theory are essentially the same as what we call $\mathbb{C}G$-modules. For us however, "$\mathbb{C}G$" has no meaning, only "$\mathbb{C}G$-module" has.

Definition 69. Let V, W be $\mathbb{C}G$-modules. A $\mathbb{C}$***G*-homomorphism** $V \to W$ is a linear map $f\colon V \to W$ such that $f(gv) = g(fv)$ for all $v \in V$ and $g \in G$. A $\mathbb{C}$***G*-isomorphism** is a bijective $\mathbb{C}G$-homomorphism. We write $V \cong W$ if there exists a $\mathbb{C}G$-isomorphism $V \to W$.

Example 70. Let $G = \{1, g\} \cong C_2$. Prove yourself that the following defines two $\mathbb{C}G$-modules V, W: $V = \mathbb{C}^2$, $g(x, y) = (y, x)$, $W = \mathbb{C}$, $g(x) = -x$.

Define $f\colon V \to W$ by $f(x, y) = x - y$. We claim that f is a $\mathbb{C}G$-homomorphism $V \to W$. First of all, f is linear. Moreover,

$$fg(x, y) = f(y, x) = y - x = g(x - y) = gf(x, y)$$

for all $x, y \in \mathbb{C}$ and therefore f is a $\mathbb{C}G$-homomorphism $V \to W$.

4.2 Representations afforded by modules

First a reminder on linear algebra. Let $A = (v_1, \dots, v_p)$ be a basis of a vector space V and $B = (w_1, \dots, w_q)$ a basis of a vector space W. Let $f\colon W \to V$ be a linear map.

We define $\langle A, f, B\rangle$ to be the matrix of f with respect to bases A, B, that is, (c_{ij}) where

$$f(w_j) = \sum_i c_{ij}\, v_i \qquad \text{for all } j.$$

In linear algebra you have learned:

(a) The map $f \mapsto \langle A, f, B\rangle$ is a bijection from $\mathrm{Hom}(W, V) := \{\text{linear maps } W \to V\}$ to the set of $p \times q$ matrices.

(b) $\langle A, f, B\rangle\langle B, g, C\rangle = \langle A, fg, C\rangle$ whenever this makes sense.

(c) If A is the standard basis of $\mathbb{C}^n$ then $\langle A, f, A\rangle v = f(v)$ for all linear maps $f\colon \mathbb{C}^n \to \mathbb{C}^n$ and all $v \in \mathbb{C}^n$.

Exercise (4.1) Deduce from this that $\langle A, f^{-1}, B\rangle = \langle B, f, A\rangle^{-1}$ if f is bijective.

Notation 71. If V is a $\mathbb{C}G$-module and $g \in G$ we write t_g^V or just t_g for the linear map $V \to V\colon v \mapsto gv$.

Lemma 72. *Let V be an n-dimensional $\mathbb{C}G$-module and A a basis for V. Then the map $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ defined by*

$$\rho(g) = \langle A, t_g, A\rangle$$

is a representation.

Proof. Let $g, h \in G$. We have $t_g t_h = t_{gh}$ because for all $v \in V$

$$(t_g t_h)v = t_g(hv) = g(hv) = (gh)v = t_{gh}v.$$

We have $\rho(g)\rho(h) = \rho(gh)$ because

$$\rho(g)\rho(h) = \langle A, t_g, A\rangle\langle A, t_h, A\rangle = \langle A, t_g t_h, A\rangle = \langle A, t_{gh}, A\rangle = \rho(gh).$$

Note that $t_1 = \mathrm{id}_V$ and therefore $\rho(1) = 1$ (the identity matrix). It follows that $\rho(g)\rho(g^{-1}) = \rho(gg^{-1}) = \rho(1) = 1$. Therefore $\rho(g)$ is invertible, and $\rho(g) \in \mathrm{GL}(n, \mathbb{C})$. The proof is finished. ☐

Definition 73. In the notation of lemma 72, we call ρ the representation **afforded by (V, A)**.

Lemma 74. *Every representation is afforded by some (V, A).*

Proof. Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation. Put $V = \mathbb{C}^n$. At this point, V is just a vector space; we turn it into a $\mathbb{C}G$-module by putting $gv = (\rho(g))v$ for all $g \in G$, $v \in V = \mathbb{C}^n$. Note that $(\rho(g))v$ is the product of a square matrix with a column vector.

In order to prove that this makes V into a $\mathbb{C}G$-module we need to prove:

(a) For all $g \in G$, the map $v \mapsto gv$ is linear.

(b) We have $g(hv) = (gh)v$ for all $g, h \in G$, $v \in V$.

(c) $1v = v$ for all $v \in V$.

As to (a), this is a well-known property of multiplication of matrices of any sizes: $(\rho g)(v + bw) = (\rho g)v + b(\rho g)w$. We prove (b) by

$$g(hv) = (\rho g)\big((\rho h)v\big) = \big((\rho g)(\rho h)\big)v = \big(\rho(gh)\big)v = (gh)v.$$

Part (c) is obvious. This proves that V with the above structure is a $\mathbb{C}G$-module.

Define A to be the standard basis $(e_1, \dots, e_n)$. Our definition $gv = (\rho g)v$ for all $v \in V$ is equivalent to $\rho(g) = \langle A, t_g, A\rangle$ as we know from linear algebra. Therefore ρ is afforded by (V, A). □

Lemma 75. *The representations afforded by* (V, A) *and* (V, B) *are equivalent.*

Proof. Let ρ, σ be the representations afforded by (V, A) and (V, B). Put $T = \langle A, \mathrm{id}_V, B\rangle$, the matrix of the identity with respect to A and B. For all $g, h \in G$ we have

$$T\,\sigma(g)\,T^{-1} = \langle A, \mathrm{id}_V, B\rangle\langle B, t_g, B\rangle\langle B, \mathrm{id}_V, A\rangle = \langle A, t_g, A\rangle = \rho(g)$$

so ρ and σ are equivalent. □

Lemma 76. *The representations afforded by* (V, A) *and* (W, B) *are equivalent if and only if* $V \cong W$.

Proof. Proof of $\Rightarrow$. Let ρ be the representation afforded by (V, A) and σ by (W, B). We know they are equivalent; let $T \in \mathrm{GL}(n, \mathbb{C})$ be such that $\sigma(g) = T\rho(g)T^{-1}$ for all $g \in G$. There exists a linear map $f\colon V \to W$ such that $T = \langle B, f, A\rangle$. Note that f is bijective because T is invertible. Then for all $g \in G$

$$\langle B, t_g^W, B\rangle = \sigma(g) = T\rho(g)T^{-1} = \langle B, f, A\rangle\langle A, t_g^V, A\rangle\langle A, f^{-1}, B\rangle = \langle B, f\,t_g^V\,f^{-1}, B\rangle,$$

that is, $t_g^W f = f\,t_g^V$. Thus $g(fv) = f(gv)$ for all $v \in V$. This shows that f is a homomorphism of $\mathbb{C}G$-modules. It is an isomorphism because f is bijective.

Proof of $\Leftarrow$. This is essentially the proof of $\Rightarrow$ read backwards; do this yourself. Note also that the case $V = W$ is just lemma 75. □

Exercise (4.2) Let ρ be afforded by (V, A) and σ by (W, B). Let $f\colon W \to V$ be a linear map and $T = \langle A, f, B\rangle$. Prove that f is a homomorphism of $\mathbb{C}G$-modules if and only if

$$\rho(x)\,T = T\,\sigma(x) \quad \text{for all } x \in G. \tag{77}$$

Definition 78. Let ρ and σ be representations of G. Let T be a $p \times q$ matrix where $p = \deg(\rho)$ and $q = \deg(\sigma)$. We call T an **intertwining matrix** or **intertwiner** from σ to ρ if (77) holds.

This section can be summarised as follows: representations of G and finite-dimensional $\mathbb{C}G$-modules are essentially the same thing. There is a bijection between $\mathrm{Rep}(G)$ and the set of isomorphism classes of finite-dimensional $\mathbb{C}G$-modules. The one language is more suited for calculations, the other for abstract mathematics. See (84) for a dictionary between the two languages.

4.3 Submodules

Definition 79. Let G be a group. A **submodule** of a $\mathbb{C}G$-module V is a linear subspace $W \subset V$ such that $gW \subset W$ for all $g \in G$.

Exercise (4.3) Prove that then $gW = W$ for all $g \in G$. Therefore W is a $\mathbb{C}G$-module in its own right.

Example 80. Let $G = C_\infty = \langle g \mid -\rangle$ act on $\mathbb{C}^2$ by $g(x, y) = (x + y, y)$. We shall prove that $\mathbb{C} \cdot (1, 0)$ is the only 1-dimensional $\mathbb{C}G$-submodule of $\mathbb{C}^2$.

We have $g(1,0) = (1,0)$ so that $\mathbb{C} \cdot (1,0)$ is a $\mathbb{C}G$-submodule of $\mathbb{C}^2$.

Suppose there is another 1-dimensional $\mathbb{C}G$-submodule. It is necessarily of the form $\mathbb{C} \cdot (a,1)$. But $g(a,1) = (a+1,1)$ so that $\mathbb{C} \cdot (a,1)$ is not a $\mathbb{C}G$-submodule. This proves our claim.

Definition 81. A $\mathbb{C}G$-module is said to be **simple** if it is nonzero and it has no submodules other than 0 and itself.

Every 1-dimensional $\mathbb{C}G$-module is simple.

Internal direct sums. Let V be a vector space and $X, Y \subset V$ linear subspaces. We say that V is the **(internal) direct sum** of X and Y, and write $V = X \oplus_i Y$, if the following equivalent properties hold:

- Every element of V can uniquely be written $x + y$ with $x \in X$ and $y \in Y$.
- We have $X \cap Y = 0$ and $V = X + Y := \{x + y \mid x \in X,\ y \in Y\}$.
- There exist a basis A of X and a basis B of Y such that $A \cap B = \varnothing$ and such that $A \cup B$ is a basis of V.

If V is finite-dimensional then the following are also equivalent:

- $V = X + Y$ and $\dim(V) = \dim(X) + \dim(Y)$.
- $X \cap Y = 0$ and $\dim(V) = \dim(X) + \dim(Y)$.

More generally, we write $V = X_1 \oplus_i \cdots \oplus_i X_n$ and say that V is an **(internal) direct sum** of the subspaces $X_1, \ldots, X_n$ if every element of V can uniquely be written $x_1 + \cdots + x_n$ where $x_i \in X_i$ for all i.

External direct sums. Let two vector spaces X, Y be given. It may well happen for formal reasons that an internal direct sum of X and Y doesn't exist, for example because $0_X \neq 0_Y$.

However the Cartesian product $X \times Y$ is an internal direct sum of $X \times \{0\}$ and $\{0\} \times Y$ which are isomorphic to (respectively) X and Y. Abusing notation we identify X with $X \times \{0\}$ and Y with $\{0\} \times Y$ whenever it seems convenient. We call $X \times Y$ the **(external) direct sum** of X and Y and it is written $X \oplus_e Y$. Note that it is an internal direct sum as well.

It is common to write $\oplus$ instead of $\oplus_i$, $\oplus_e$. Wherever you read $\oplus$ find out if they mean internal or external!

Definition 82. Let ρ, σ be representations of a group G and write $k = \deg \rho$, $\ell = \deg \sigma$. The **diagonal sum** $\rho \oplus \sigma$ is the $(k+\ell)$-dimensional representation of G defined by the block matrices

$$(\rho \oplus \sigma)(g) = \begin{array}{|c|c|} \hline \rho(g) & 0 \\ \hline 0 & \sigma(g) \\ \hline \end{array}\ .$$

Note that if $(V, (a_1, \ldots, a_k))$ affords ρ and $(W, (a_{k+1}, \ldots, a_\ell))$ affords σ then $(V \oplus W, (a_1, \ldots, a_\ell))$ affords $\rho \oplus \sigma$.

Definition 83. A representation is said to be **irreducible** if it is afforded by some (V, A) where V is simple. It is called reducible if it is not irreducible.

Exercise (4.4) Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation of a group G with $n > 0$. Prove that the following are equivalent:

(1) ρ is reducible.

(2) There are $k, \ell \in \mathbb{Z}_{>0}$ with $k + \ell = n$, and a representation σ of G, equivalent to ρ, such that the following holds for all $x \in G$. No nonzero entry of the matrix $\sigma(x)$ is both in one of the first k columns and in one of the last ℓ rows.

We can now give the dictionary between the languages of $\mathbb{C}G$-modules and representations:

$\mathbb{C}G$-module	representation
$\mathbb{C}G$-homomorphism	intertwiner
simple	irreducible
direct sum of $\mathbb{C}G$-modules	diagonal sum of representations

(84)

Theorem 85: Maschke's theorem. *Let G be a* finite *group and V a $\mathbb{C}G$-module of finite dimension. For every submodule $W \subset V$ there is a submodule $X \subset V$ such that $V = W \oplus X$.*

We will prove Maschke's theorem later on (page 27). We shall also deduce later on (corollary 92) that every representation of a finite group is equivalent to a diagonal sum of a number of irreducible representations.

4.4 Inner products

Definition 86. Let V be a vector space over $\mathbb{C}$. An **inner product** on V is a map

$$\begin{aligned} V \times V &\longrightarrow \mathbb{C} \\ (v, w) &\longmapsto \langle v, w \rangle \end{aligned}$$

such that

(1) Linear in first argument: $\langle au + bv, w \rangle = a\langle u, w \rangle + b\langle v, w \rangle$ for all $u, v, w \in V$, $a, b \in \mathbb{C}$.

(2) Hermitian: $\langle v, w \rangle = \overline{\langle w, v \rangle}$ for all $v, w \in V$.

(3) Positive definite: $\langle v, v \rangle > 0$ if $v \neq 0$.

Remark 87. (a). Axiom (2) implies that $\langle v, v \rangle \in \mathbb{R}$ for all $v \in V$. This is why axiom (3) makes sense.

(b). Axioms (1) and (2) imply that $\langle w, au + bv \rangle = \bar{a}\langle w, u \rangle + \bar{b}\langle w, v \rangle$ for all $u, v, w \in V$, $a, b \in \mathbb{C}$.

Every finite-dimensional vector space can be equipped with an inner product as follows. Let $(v_1, \ldots, v_n)$ be a basis and put

$$\left\langle \textstyle\sum a_i v_i, \sum b_i v_i \right\rangle = \textstyle\sum a_i \bar{b}_i.$$

It can be shown that every inner product on a finite-dimensional vector space is of this form; we won't need or prove this.

Definition 88. Let $\langle \cdot, \cdot \rangle$ be an inner product on a vector space V. Let W be a subspace of V. The **orthogonal complement** of W is

$$W^{\perp} := \{ v \in V \mid \langle v, w \rangle = 0 \text{ for all } w \in W \}.$$

Lemma 89. *Let $\langle\cdot,\cdot\rangle$ be an inner product on a finite-dimensional vector space V and let W be a subspace of V. Then $V = W \oplus W^{\perp}$.*

Proof. Firstly, $W \cap W^{\perp} = 0$ because if $v \in W \cap W^{\perp}$ then $\langle v, v\rangle = 0$ whence $v = 0$. It remains to prove $\dim W + \dim W^{\perp} \geq \dim V$.

Let $(w_1, \ldots, w_k)$ be a basis for of W and define a linear map $L\colon V \to \mathbb{C}$ by

$$L(v) = (\langle v, w_1\rangle, \ldots, \langle v, w_k\rangle).$$

Then $\ker L = W^{\perp}$ so

$$\begin{aligned}\dim W + \dim W^{\perp} &= k + \dim W^{\perp} \geq \dim \operatorname{im} L + \dim W^{\perp} \\ &= \dim \operatorname{im} L + \dim \ker L = \dim V.\end{aligned}$$

□

Definition 90. Let V be a $\mathbb{C}G$-module. An inner product $\langle\cdot,\cdot\rangle$ is said to be ***G*-invariant** if $\langle gv, gw\rangle = \langle v, w\rangle$ for all $g \in G$, $v, w \in V$.

Proposition 91. *Let G be a finite group and V a finite-dimensional $\mathbb{C}G$-module. Then there exists a G-invariant inner product on V.*

Proof. We know that an inner product $\langle\cdot,\cdot\rangle_0$ on V exists. Define

$$\langle v, w\rangle = \sum_{h\in G} \langle hu, hv\rangle_0.$$

Prove yourself that $\langle\cdot,\cdot\rangle$ is also an inner product on V. To finish we shall prove that it is G-invariant. Let $g \in G$ and $v, w \in V$. Then

$$\langle gv, gw\rangle = \sum_{h\in G} \langle hgv, hgw\rangle_0 \stackrel{*}{=} \sum_{h\in G} \langle hv, hw\rangle_0 = \langle v, w\rangle$$

where the starred equality follows from the bijection $G \to G\colon h \mapsto hg$. □

In the above proof we see two arguments that we shall often meet again: a sum over a finite group G; and a change of index in such a sum according to a permutation of G such as $h \mapsto hg$.

Proof of Maschke's theorem (theorem 85). Let G be a finite group. Let V be a $\mathbb{C}G$-module and $W \subset V$ a submodule. We must show that $V = W \oplus X$ for some submodule X.

By proposition 91 there exists a G-invariant inner product $\langle\cdot,\cdot\rangle$ on V. Put $X = W^{\perp}$. By lemma 89 $V = W \oplus X$. We will be done if we prove that X is a submodule of V. It is clearly a linear subspace.

Let $x \in X$, $w \in W$ and $g \in G$. Then $g^{-1}w \in W$ because W is a submodule and so

$$\begin{aligned}\langle w, gx\rangle &= \langle g^{-1}w, x\rangle && \text{because } \langle\cdot,\cdot\rangle \text{ is } G\text{-invariant} \\ &= 0 && \text{because } g^{-1}w \in W \text{ and } x \in X = W^{\perp}.\end{aligned}$$

This holds for all $w \in W$ so $gx \in W^{\perp} = X$. This is true for all $g \in G$, $x \in X$ so X is a submodule as promised. □

See exercise 4.23 for a different proof of Maschke's theorem.

Corollary 92. *Let G be a finite group. Then every finite-dimensional $\mathbb{C}G$-module is a direct sum of simple submodules.*

Proof. Let V be a $\mathbb{C}G$-module of dimension n. By induction on n we shall prove that V is a direct sum of simple submodules. If $n \leq 1$ then the result is clear. Let $n > 1$.

If V is simple, there is nothing to prove, so assume otherwise; let $W \subset V$ be a submodule different from 0 and V. By theorem 85 (Maschke) there exists a submodule $X \subset V$ such that $V = W \oplus X$.

Now W and X have smaller dimensions than V. By the induction hypothesis we can write

$$W = W_1 \oplus \cdots \oplus W_k, \qquad X = X_1 \oplus \cdots \oplus X_\ell$$

for some simple submodules W_i and X_j. Then

$$V = W \oplus X = W_1 \oplus \cdots \oplus W_k \oplus X_1 \oplus \cdots \oplus X_\ell$$

which is the desired decomposition. □

4.5 Exercises

(4.5) Let V, W be $\mathbb{C}G$-modules. Let L be the set of linear maps $V \to W$; it is a vector space by putting $(af + bg)(x) = a \cdot f(x) + b \cdot g(x)$ ($a, b \in \mathbb{C}$, $f, g \in L$, $x \in V$). Let H be the set of homomorphisms $V \to W$ of $\mathbb{C}G$-homomorphisms. Prove that H is a linear subspace of L.

(4.6) Let V and W be $\mathbb{C}G$-modules. Prove that $V \times W$ equipped with the map $G \times (V \times W) \to (V \times W)$: $(g, (v, w)) \mapsto (gv, gw)$ is also a $\mathbb{C}G$-module.

(4.7) Let V be a $\mathbb{C}G$-module and W a $\mathbb{C}H$-module. Prove that $V \times W$ equipped with the map $(G \times H) \times (V \times W)$: $((g, h), (v, w)) \mapsto (gv, hw)$ is a $\mathbb{C}(G \times H)$-module.

(4.8) Let V be a $\mathbb{C}G$-module. Let $W = \mathrm{End}(V)$ be the set of linear maps $V \to V$ with the obvious structure of vector space. Prove that W equipped with the map $G \times W \to W$: $(g, f) \mapsto g \circ f \circ g^{-1}$ is also a $\mathbb{C}G$-module.

(4.9) Let U, V, W be $\mathbb{C}G$-modules. Let p: $U \to V$ and q: $V \to W$ be homomorphisms of $\mathbb{C}G$-modules. Prove that $q \circ p$: $U \to W$ is also a homomorphism.

(4.10) Write $C_\infty = \langle x \mid - \rangle$ and define ρ: $C_\infty \to \mathrm{GL}(3, \mathbb{C})$ by

$$\rho(x) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Find all submodules of ρ or, more precisely, of a $\mathbb{C}G$-module V where ρ is afforded by (V, A).

(4.11) Let V be a $\mathbb{C}G$-module. Prove that if A, B are submodules of V then so are $A + B$ and $A \cap B$.

(4.12) Let $G \times A \to A$: $(g, a) \mapsto g(a)$ be an action of a group G on a set A. Let $\mathbb{C}^A$ be the set of functions $A \to \mathbb{C}$. It is a vector space with pointwise vector space operations.

(a) Prove that $\mathbb{C}^A$ becomes a $\mathbb{C}G$-module by putting $(gf)a = f(g^{-1}a)$ for all $f \in \mathbb{C}^A$, $g \in G$, $a \in A$.

(b) If $2 \leq \#A < \infty$, prove that $\mathbb{C}^A$ is not simple as $\mathbb{C}G$-module.

(c) If A is infinite, prove again that $\mathbb{C}^A$ is not simple.

(4.13) Prove that $\mathbb{C}^2$ is simple as $\mathbb{C}G$-module where $G = \mathrm{GL}(2, \mathbb{C})$.

(4.14) Let V be a complex vector space. True or false?

(a) If $\langle\cdot,\cdot\rangle$ is an inner product on V then so is $(v,w)\mapsto\langle iv,iw\rangle$.

(b) If $\langle\cdot,\cdot\rangle$ is an inner product on V then so is $(v,w)\mapsto\langle v,-w\rangle$.

(c) If $\langle\cdot,\cdot\rangle$ is an inner product on V then so is $(v,w)\mapsto\overline{\langle v,w\rangle}$.

(d) If $\langle\cdot,\cdot\rangle_1,\langle\cdot,\cdot\rangle_2$ are inner products on V then so is $(v,w)\mapsto\langle v,w\rangle_1+\langle v,w\rangle_2$.

(e) If $\langle\cdot,\cdot\rangle_1,\langle\cdot,\cdot\rangle_2$ are inner products on V then so is $(v,w)\mapsto\langle v,w\rangle_1\langle v,w\rangle_2$.

(4.15) For all $i\in\{1,2\}$, let $\langle\cdot,\cdot\rangle_i$ be an inner product on a complex vector space V_i. True or false?

(a) Then $((u,v),(w,x))\mapsto\langle u,v\rangle_1+\langle w,x\rangle_2$ is an inner product on $V_1\times V_2$.

(b) Then $((u,v),(w,x))\mapsto\langle u,w\rangle_1+\langle v,3x\rangle_2$ is an inner product on $V_1\times V_2$.

(c) Then $((u,v),(w,x))\mapsto\langle u,w\rangle_1$ is an inner product on $V_1\times V_2$.

(4.16) Let $\langle\cdot,\cdot\rangle$ be an inner product on a complex vector space V. Let $W\subset V$ be a subspace. Prove that the orthogonal complement $W^\perp$ is also a subspace of V.

(4.17) Prove $\Leftarrow$ in lemma 76: if $V\cong W$ then the representations afforded by (V,A) and (W,B) are equivalent.

(4.18) Let G be a finite group and V a nonzero finite-dimensional $\mathbb{C}G$-module. We know that V is a direct sum of simple submodules. In this exercise, we find all such decompositions.

(a) Prove that the following are equivalent: (1) Any two simple submodules of V are isomorphic; (2) There exists a simple $\mathbb{C}G$-module U and an integer $k\geq 0$ such that V is isomorphic to $kU:=U\times\cdots\times U$ (k factors).

If these hold then V is called **isotypical** of k factors.

Prove also that U (up to isomorphism) and k depend only on V.

(b) Suppose that V is isotypical of k factors. Let $\mathrm{End}(V)$ be the set of homomorphisms $V\to V$ of $\mathbb{C}G$-modules. Prove that if $e,f\in\mathrm{End}(V)$ and $a,b\in\mathbb{C}$ then $ae+bf\colon u\mapsto a\cdot e(u)+b\cdot f(u)$ and $ef\colon u\mapsto e(f(u))$ are also in $\mathrm{End}(V)$. Prove that this makes $\mathrm{End}(V)$ into a ring isomorphic to $M_k(\mathbb{C})$.

(c) Prove that there are nonzero isotypical submodules $U_1,\ldots,U_k\subset V$ such that $V=U_1\oplus\cdots\oplus U_k$ and $U_i\oplus U_j$ is not isotypical if $i\neq j$. Moreover, the U_i are unique up to permutation.

The U_i are called the **isotypical components** of V.

(4.19) Let G be a group, not necessarily finite. Let V be a $\mathbb{C}G$-module with the property that for every submodule $X\subset V$ there exists a submodule $Y\subset V$ such that $V=X\oplus Y$.

(a) If V is finite-dimensional, prove that V is semi-simple (that is, a direct sum of simple modules).

(b) Give an example showing that this fails if V is not finite-dimensional.

(4.20) Show that Maschke's theorem for finite-dimensional $\mathbb{C}G$-modules is false if the group G is not assumed to be finite.

(4.21) Consider the permutation representation ρ of S_3 which we shall write as follows:

$$\rho((12))=\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix},\quad\rho((23))=\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}.$$

Find all intertwiners from ρ to itself in explicit form.

(4.22) Let $(v_1, \dots, v_n)$ be a basis of a complex vector space V with $n \geq 2$. For $s \in S_n$ (the symmetric group) and $a_1, \dots, a_n \in \mathbb{C}$ we define

$$s\Big(\sum_{i=1}^{n} a_i\, v_i\Big) := \sum_{i=1}^{n} a_i\, v_{s(i)}.$$

(a) Prove that this makes V into a $\mathbb{C}S_n$-module. It is called the **permutation module**.

(b) Let $X = \big\{ \sum_{i=1}^{n} a_i\, v_i \in V \bigm| \sum_{i=1}^{n} a_i = 0 \big\}$. Prove that X is a submodule of V.

(c) In order to prove that X is simple, assume from now on that Y is a nonzero submodule of X. Prove that there exists $y \in Y$ of the form

$$y = \sum a_i\, v_i, \qquad a_n = 1.$$

(d) Put $w = v_1 + \cdots + v_n$ and $S_{n-1} = \big\{ g \in S_n \bigm| g(n) = n \big\}$. Define

$$z = \frac{1}{(n-2)!} \sum_{g \in S_{n-1}} gy.$$

Prove $gz = z$ for all $g \in S_{n-1}$. Prove $z = n\, v_n - w$.

(e) Prove $n\, v_i - w \in Y$ for all i.

(f) Prove $v_n - v_i \in Y$ for all i. Prove $Y = X$, that is, X is simple.

(g) Find an explicit submodule W of V such that $V = W \oplus X$. Prove that W is simple.

(4.23) An alternative proof of Maschke's theorem. Let G be a finite group and U a $\mathbb{C}G$-module. Let $V \subset U$ be a submodule and $p\colon U \to V$ any linear map such that $p(v) = v$ for all $v \in V$.

(a) (Not for credit). Why does such a p exist? Show by an example that p is not necessarily a homomorphism of $\mathbb{C}G$-modules (if p is chosen as above).

(b) Define $q\colon U \to V$ by

$$q(v) = \frac{1}{\#G} \sum_{g \in G} g^{-1}\, p\, g(v).$$

Prove that $q\colon U \to V$ is a homomorphism of $\mathbb{C}G$-modules.

(c) Prove that $q(v) = v$ for all $v \in V$.

(d) Let H be a group and $f\colon A \to B$ a homomorphism of $\mathbb{C}H$-modules. Prove that $\ker(f)$ is a submodule of A.

(e) Prove that there exists a submodule $W \subset U$ such that $U = V \oplus W$.

(f) (Not for credit). The present proof has many advantages over the proof from the lectures. List as many as you can think of.

5 Characters

5.1 Characters

Reminder on the trace. The **trace** of a square matrix $A = (a_{ij})_{ij} \in M_n(\mathbb{C})$ is defined to be $\mathrm{tr}(A) = a_{11} + \cdots + a_{nn}$, the sum of the elements on the diagonal. It is not hard to show that

$$\mathrm{tr}(AB) = \mathrm{tr}(BA), \qquad \mathrm{tr}(TAT^{-1}) = \mathrm{tr}(A) \tag{93}$$

for all $A, B \in M(n, \mathbb{C})$, $T \in \mathrm{GL}(n, \mathbb{C})$.

If V is a finite-dimensional vector space with basis C and $f\colon V \to V$ is a linear map, we define $\mathrm{tr}(f)$, the **trace** of f, to be the trace of $\langle C, f, C\rangle$, the matrix of f with respect to a basis C. This doesn't depend on C by (93) and the fact from linear algebra that if D is another basis then

$$\langle D, f, D\rangle = \langle D, 1, C\rangle\langle C, f, C\rangle\langle D, 1, C\rangle^{-1}.$$

Definition 94: Characters. Let G be a group.

(a) Let ρ be a representation of G. Its **character** $\chi_\rho\colon G \to \mathbb{C}$ (χ is the Greek letter chi) is defined by $\chi_\rho(g) = \mathrm{tr}\,\rho(g)$ for all $g \in G$.

(b) A **character of G** is by definition a character of some representation of G.

(c) Let V be a finite-dimensional $\mathbb{C}G$-module. Its **character** $\chi_V\colon G \to \mathbb{C}$ is defined by $\chi_V(g) = \mathrm{tr}(t_g^V)$ for all $g \in G$.

Note that if ρ is afforded by (V, A) then $\chi_V = \chi_\rho$.

Proposition 95. *Let ρ, σ be representations of a group G. If $\rho \sim \sigma$ then $\chi_\rho = \chi_\sigma$.*

Proof. Write $n = \deg \rho$. The assumption $\rho \sim \sigma$ means that there exists $T \in \mathrm{GL}(n, \mathbb{C})$ such that $\sigma(g) = T\,\rho(g)\,T^{-1}$ for all $g \in G$. It follows that

$$\chi_\sigma(g) = \mathrm{tr}\,\sigma(g) = \mathrm{tr}(T\,\rho(g)\,T^{-1}) = \mathrm{tr}\,\rho(g) = \chi_\rho(g)$$

for all $g \in G$ as required. □

If the group in proposition 95 is finite then the converse also holds: if $\chi_\rho = \chi_\sigma$ then $\rho \sim \sigma$. This is much harder and will be proved in theorem 113.

Recall the diagonal sum $\rho \oplus \sigma$ of two representations ρ, σ of G. It is clear that

$$\chi_{\rho\oplus\sigma} = \chi_\rho + \chi_\sigma.$$

Therefore, the sum of two characters of G is again a character.

Remark 96. The following is beyond our scope (exercise 7.14 and chapter 10). For any two representations ρ, σ of a group G there is another written $\rho \otimes \sigma$ and known as the **tensor product** or **Kronecker product** of ρ and σ. It has the property that $\chi_{\rho\otimes\sigma}(g) = \chi_\rho(g)\,\chi_\sigma(g)$ for all $g \in G$. □

Proposition 97. *Let $\chi\colon G \to \mathbb{C}$ be a character. Then $\chi(gxg^{-1}) = \chi(x)$ for all $g, x \in G$.*

Proof. By definition there exists a representation ρ such that $\chi = \chi_\rho$. Then

$$\begin{aligned}
\chi(gxg^{-1}) &= \mathrm{tr}\,\rho(gxg^{-1}) && \text{by definition of } \chi_\rho\\
&= \mathrm{tr}(\rho(g)\,\rho(x)\,\rho(g)^{-1}) && \text{because } \rho \text{ is a representation}\\
&= \mathrm{tr}\ \rho(x) && \text{by (93)}\\
&= \chi(x) && \text{by definition of } \chi_\rho.
\end{aligned}$$

□

Reminder on conjugacy classes. Two elements x, y of a group G are said to be **conjugate** in G if there exists $g \in G$ such that $x = gyg^{-1}$.

Being conjugate is an equivalence relation, or more precisely, the binary relation $\{(x, gxg^{-1}) \mid x, g \in G\}$ is an equivalence relation. The corresponding equivalence classes are called **conjugacy classes**. Let $K(G)$ denote the set of conjugacy classes of a group G and $k(G) = \#K(G)$.

For $g, x \in G$ we write

$$x^g := g^{-1}xg, \qquad x^G = \{g^{-1}xg \mid g \in G\}.$$

Note that x^G is just the conjugacy class of x.

Exercise (5.1) Let g, h, x, y be elements of a group G.

(a) Then $(xy)^g = x^g y^g$. Equivalently, the map $G \to G$: $a \mapsto a^g$ is a homomorphism.

(b) Also $(x^g)^h = x^{gh}$. Why would this be false if x^g were defined to be gxg^{-1} instead?

Exercise (5.2) Let G be a group and $m \in \mathbb{Z}$.

(a) Prove that $(x^g)^m = (x^m)^g$ for all $g, x \in G$.

(b) Let C be a conjugacy class of G and write $C^m = \{x^m \mid x \in C\}$. Prove that C^m is also a conjugacy class of G.

Exercise (5.3) The results of this exercise are often useful when you're looking for the conjugacy classes of a group.

Let G be a group generated by a set A. Let $C \subset G$ be any subset.

(a) Prove that the following are equivalent:

(1) $\{aca^{-1}, a^{-1}ca\} \subset C$ for all $c \in C$, $a \in A$.

(2) $gcg^{-1} \in C$ for all $c \in C$, $g \in G$.

(3) Let D be a conjugacy class of G. Then $D \subset C$ or $D \cap C = \varnothing$.

(4) C is a union of conjugacy classes of G.

(In fact (3) $\Leftrightarrow$ (4) is trivial.)

(b) State and prove an analogous result where condition (4) is replaced by ***C* is a conjugacy class of *G*.**

The **centre** of a group G is

$$Z(G) = \{g \in G \mid ga = ag \text{ for all } a \in G\}$$

and its elements are said to be **central** in G. In words: an element of a group G is central if and only if it commutes with all other elements of G. Note that if $a \in G$ then ($a^G = \{a\} \Leftrightarrow a$ is central in G).

Example 98. Recall the presentation $\langle r, s \mid r^n,\ s^2,\ (rs)^2\rangle$ of the dihedral group D_{2n}. Prove that if n is odd then the conjugacy classes of D_{2n} are

$$\{1\}, \quad \{r^m, r^{-m}\} \text{ for } m \in \{1, \dots, \tfrac{n-1}{2}\}, \quad \{r^k s \mid k \in \mathbb{Z}\}.$$

Solution. Firstly $\{1\}$ is a conjugacy class in any group.

Next r is conjugate to r^{-1} because $r^s = r^{-1}$. In order to prove that $C := \{r, r^{-1}\}$ is a conjugacy class, it is enough to prove that $x^r, x^s \in C$ for all $x \in C$ (by exercise 5.3 and because $\{r, s\}$ generate D_{2n}). This is indeed true:

$$r^r = r, \quad r^s = r^{-1}, \quad (r^{-1})^r = r^{-1}, \quad (r^{-1})^s = r.$$

This proves that $\{r, r^{-1}\}$ is a conjugacy class. By exercise (5.2b) it follows that $\{r^m, r^{-m}\}$ is a conjugacy class for all $m \in \mathbb{Z}$.

It remains to prove that $D := \{r^k s \mid k \in \mathbb{Z}\}$ is a conjugacy class. It is enough to prove that the elements of D are pairwise conjugate because we already proved that $G \setminus D$ is a union of conjugacy classes. For all $k \in \mathbb{Z}$

$$(r^k s)^r = r^{-1} r^k s r = r^{-1} r^k r^{-1} s = r^{k-2} s.$$

It follows that $r^k s$ is conjugate to $r^{k-2m} s$ for all $m \in \mathbb{Z}$. But $r^n = 1$ and n is odd so $r^k s$ is conjugate to $r^\ell s$ for all $k, \ell \in \mathbb{Z}$ and the proof is finished. □

Example 99. As an example we calculate the character of a certain representation. Prove yourself that their exists a unique representation $\rho\colon D_6 \to \mathrm{GL}(2, \mathbb{C})$ such that

$$\rho(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \rho(r) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

We aim to calculate the character of ρ.

As every character, it is constant on conjugacy classes by proposition 97. We found the conjugacy classes of D_6 in example 98: they are $\{1\}$, $\{s, rs, r^2 s\}$ and $\{r, r^2\}$. So it is enough to calculate the values of χ_ρ at $1, s, r$ (one element from each conjugacy class). The character of ρ is now immediate from the definition of ρ:

g	1	s	r
$\chi_\rho(g)$	2	0	-1

.

Definition 100. For a group G, the set of functions $G \to \mathbb{C}$ is written $\mathbb{C}(G)$. We make it into a vector space by the pointwise operations

$$(ap + bq)(x) = a\,p(x) + b\,q(x)$$

for all $a, b \in \mathbb{C}$, $p, q \in \mathbb{C}(G)$, $x \in G$. (Prove yourself that this indeed makes $\mathbb{C}(G)$ into a vector space.) For $p, q \in \mathbb{C}(G)$ we define

$$(p, q)_G = \frac{1}{\#G} \sum_{x \in G} p(x)\,\overline{q(x)}.$$

Lemma 101. *The map $(\cdot, \cdot)_G$ is an inner product on $\mathbb{C}(G)$.*

Proof. For all $a, b \in \mathbb{C}$, $p, q, r \in \mathbb{C}(G)$ we have

$$\begin{aligned} \#G \cdot (ap + bq, r)_G &= \sum_{x \in G} (ap + bq)(x)\,\overline{r(x)} = \sum_{x \in G} (a\,p(x) + b\,q(x))\,\overline{r(x)} \\ &= a \sum_{x \in G} p(x)\,\overline{r(x)} + b \sum_{x \in G} q(x)\,\overline{r(x)} = \#G\big(a(p, r)_G + b(q, r)_G\big) \end{aligned}$$

which proves that $(\cdot, \cdot)_G$ is linear in the first argument. For all $p, q \in \mathbb{C}(G)$ we have

$$\overline{(p, q)_G} = \frac{1}{\#G} \sum_{x \in G} \overline{p(x)\,\overline{q(x)}} = \frac{1}{\#G} \sum_{x \in G} \overline{p(x)}\,q(x) = (q, p)_G$$

which proves it's Hermitian. Finally if $p \in \mathbb{C}(G)$ is nonzero, say $p(y) \neq 0$ ($y \in G$), then

$$(p, p)_G = \frac{1}{\#G} \sum_{x \in G} p(x)\,\overline{p(x)} \geq \frac{1}{\#G} p(y)\,\overline{p(y)} > 0$$

which proves that $(\cdot, \cdot)_G$ is positive definite. □

Definition 102. Let G be a group. A function $f \in \mathbb{C}(G)$ is called a **class function** if $f(gxg^{-1}) = f(x)$ for all $g, x \in G$. In words: f is constant on conjugacy classes. We write $\mathrm{CF}(G)$ for the set of class functions on G.

So proposition 97 says that every character is a class function.

Exercise (5.4) Prove that the set $\mathrm{CF}(G)$ is a linear subspace of $\mathbb{C}(G)$ and its dimension is $k(G)$ (the number of conjugacy classes of G).

Lemma 103. *Let ρ be a representation of a finite group G and let $g \in G$.*

(a) $\chi_\rho(1) = \deg \rho$.

(b) $\chi_\rho(g)$ *is a sum of roots of unity.*

(c) $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

Proof. Proof of (a). Write $n = \deg \rho$ and let I_n denote the identity matrix in $\mathrm{GL}(n, \mathbb{C})$. Then $\chi_\rho(1) = \operatorname{tr} \rho(1) = \operatorname{tr} I_n = n = \deg \rho$.

Before we prove (b) and (c) some observations are in order. Let $g \in G$. Let $\omega_1, \ldots, \omega_n$ be the eigenvalues of $\rho(g)$.

Note that g is of finite order, because G is finite. Say $g^r = 1$ with $r > 0$. Then $\rho(g)^r = 1$. By lemma 25 $\rho(g)$ is conjugate to a diagonal matrix B. The diagonal entries of B are $\omega_1, \ldots, \omega_n$ though not necessarily in this order.

Note $B^r = 1$ and therefore $\omega_i^r = 1$ for all i.

Proof of (b). We find $\chi_\rho(g) = \operatorname{tr} \rho(g) = \omega_1 + \cdots + \omega_n$ which is a sum of roots of unity.

Proof of (c). Note that $\rho(g^{-1})$ is conjugate to B^{-1} which is a diagonal matrix whose diagonal entries are $\omega_1^{-1}, \ldots, \omega_n^{-1}$ in some order.

Also $\omega_i^{-1} = \overline{\omega_i}$ because ω_i is a root of unity. Therefore

$$\begin{aligned}\chi_\rho(g^{-1}) &= \operatorname{tr} \rho(g^{-1}) = \operatorname{tr} B = \omega_1^{-1} + \cdots + \omega_n^{-1} \\ &= \overline{\omega}_1 + \cdots + \overline{\omega}_n = \overline{\omega_1 + \cdots + \omega_n} = \overline{\chi_\rho(g)}.\end{aligned}$$ □

The **degree** of a character χ is $\deg \chi := \chi(1)$. Note that the degree of χ_ρ is just the degree of ρ by lemma 103(a).

A character is said to be **irreducible** if it is of the form χ_ρ for some irreducible representation ρ. Let $I(G)$ denote the set of irreducible characters of G.

5.2 Schur's lemma and orthogonality

Exercise (5.5) Let $L\colon V \to W$ be a homomorphism of $\mathbb{C}G$-modules. Prove that $\ker L$ is a submodule of V and $\operatorname{im} L$ is a submodule of W.

Recall that a $\mathbb{C}G$-module is said to be simple if it has no other submodules than 0 and itself.

Theorem 104: Schur's lemma. *Let G be a group and let V, W be simple $\mathbb{C}G$-modules.*

(a) *Every $\mathbb{C}G$-homomorphism $L\colon V \to W$ is 0 or an isomorphism.*

(b) *Every $\mathbb{C}G$-homomorphism $L\colon V \to V$ is scalar multiplication by some complex number.*

Proof. Proof of (a). Suppose $L \neq 0$. Then $\ker(L) \neq V$. By exercise 5.5, $\ker(L)$ is a submodule of V. But V is simple so $\ker(L) = 0$, that is, L is injective.

Likewise, $\operatorname{im}(L)$ is a nonzero submodule of W. But W is simple so $\operatorname{im}(L) = W$, that is, L is surjective. We have proved that L is bijective if it is nonzero, as required.

Proof of (b). Note that $V \neq 0$ because V is simple. Let v be an eigenvector of L with eigenvalue λ. Define $M\colon V \to V$ by $M(x) = L(x) - \lambda x$. Prove yourself that M is again a $\mathbb{C}G$-homomorphism.

Now $M(v) = 0$ so M is a non-injective $\mathbb{C}G$-homomorphism. By part (a) we must have $M = 0$, that is, $L(x) = \lambda x$ for all $x \in V$. □

The translation of Schur's lemma (theorem 104) in terms of representations looks as follows. Let ρ, σ be irreducible representations of a group G. Then every intertwining matrix $T\colon \rho \to \sigma$ is zero or invertible; moreover every intertwiner $T\colon \rho \to \rho$ is a scalar matrix.

Lemma 105. *Let ρ, σ be representations of a group G of degrees n, m, respectively. Let $A \in M_{m\times n}(\mathbb{C})$ and*

$$T = \sum_{h\in G} \sigma(h^{-1}) \cdot A \cdot \rho(h).$$

Then T is an intertwining matrix $\rho \to \sigma$.

Proof. We must prove $\sigma(x)\, T = T\, \rho(x)$ for all $x \in G$. We have

$$\begin{aligned} T\,\rho(x) &= \Big(\sum_{h\in G} \sigma(h^{-1})\, A\, \rho(h)\Big)\rho(x) = \sum_{h\in G} \sigma(h^{-1})\, A\, \rho(hx) \\ &\overset{*}{=} \sum_{g\in G} \sigma(xg^{-1})\, A\, \rho(g) = \sigma(x)\Big(\sum_{g\in G} \sigma(g^{-1})\, A\, \rho(g)\Big) = \sigma(x)\, T \end{aligned}$$

where the starred equality is because of the bijection $G \to G\colon h \mapsto hx$. □

Exercise (5.6) State the above lemma in terms of modules.

If A is a matrix, let A_{ij} denote its entry in position (i, j). If A, B are matrices such that the product AB is defined (that is, the number of rows in A is the number of columns in B) then

$$(AB)_{ij} = \sum_s A_{is}\, B_{sj}.$$

Here s ranges over $\{1, \ldots, n\}$ where n is the number of rows of A. Let's not bother specifying such ranges any longer. Likewise, if A, B, C are matrices such that the product ABC is defined then

$$(ABC)_{ij} = \sum_{s,t} A_{is}\, B_{st}\, C_{tj}. \tag{106}$$

Theorem 107: Orthogonality of characters. *Let ρ, σ be irreducible representations of a finite group G.*

(a) *If $\rho \not\sim \sigma$ then $(\chi_\rho, \chi_\sigma)_G = 0$.*

(b) *Also $(\chi_\rho, \chi_\rho)_G = 1$.*

Proof. Let $E(i, j)$ denote the $(\deg \sigma) \times (\deg \rho)$ matrix with 1 in position (i, j) and zeroes elsewhere. If A and B are matrices and $A\, E(i, j)\, B$ is defined then

$$(A \cdot E(i, j) \cdot B)_{ij} = A_{ii}\, B_{jj} \tag{108}$$

because $(A\, E(i, j)\, B)_{ij} = \sum_{s,t} A_{is}\, E(i, j)_{st}\, B_{tj}$ by (106) all of whose terms are 0 except the term with $(s, t) = (i, j)$ which is $A_{ii}\, B_{jj}$.

Put

$$T(i,j) := \sum_{g\in G} \sigma(g^{-1}) \cdot E(i,j) \cdot \rho(g).$$

Then $T(i,j)$ is an intertwiner $\rho \to \sigma$ by lemma 105. Moreover, using (108)

$$\begin{aligned}\sum_{i,j} T(i,j)_{ij} &= \sum_{i,j}\sum_{g\in G} \left[\sigma(g^{-1}) \cdot E(i,j) \cdot \rho(g)\right]_{ij} = \sum_{i,j}\sum_{g\in G} \sigma(g^{-1})_{ii} \cdot \rho(g)_{jj} \\ &= \sum_{g\in G} \operatorname{tr} \sigma(g^{-1}) \cdot \operatorname{tr} \rho(g) = \sum_{g\in G} \chi_\sigma(g^{-1})\, \chi_\rho(g) = \#G \cdot (\chi_\rho, \chi_\sigma)_G. \qquad (109)\end{aligned}$$

Proof of (a). Suppose $\rho \not\sim \sigma$. Then $T(i,j) = 0$ by Schur's lemma and the result follows by (109).

Proof of (b). Put $\rho = \sigma$ in the foregoing. By Schur's lemma there exists $\lambda_{ij} \in \mathbb{C}$ such that $T(i,j) = \lambda_{ij} I_n$ where $n = \deg \rho = \chi_\rho(1)$ and I_n is the $n \times n$ identity matrix. By (109)

$$\begin{aligned} n \cdot \#G \cdot (\chi_\rho, \chi_\rho)_G &= n \sum_{i,j} T(i,j)_{ij} = n \sum_i \lambda_{ii} = \operatorname{tr} \sum_i \lambda_{ii} I_n = \operatorname{tr} \sum_i T(i,i) \\ &= \operatorname{tr} \sum_i \sum_{g\in G} \rho(g^{-1})\, E(i,i)\, \rho(g) = \operatorname{tr} \sum_{g\in G} \rho(g^{-1}) \left[\sum_i E(i,i)\right] \rho(g) \\ &= \operatorname{tr} \sum_{g\in G} \rho(g^{-1})\, I_n\, \rho(g) = \sum_{g\in G} \operatorname{tr} \rho(1) = \#G \cdot \operatorname{tr} \rho(1) = \#G \cdot n. \end{aligned}$$

The result follows. □

Corollary 110. *Let G be a finite group. Then G has at most $k(G)$ inequivalent irreducible representations.*

Proof. Suppose not, say, $\rho_1, \dots, \rho_s$ are inequivalent irreducible representations with $s > k(G)$. Let χ_i be the character of ρ_i. Now $\chi_i \in \mathrm{CF}(G)$ for all i and $\mathrm{CF}(G)$ is of dimension $k(G) < s$ so the χ_i are linearly dependent; say $\sum_i a_i \chi_i = 0$ with $a_i \in \mathbb{C}$ for all i, not all zero, say $a_k \neq 0$. By theorem 107 (orthogonality) we have $(\chi_i, \chi_k)_G = \delta_{ik}$ for all i and therefore

$$0 = (0, \chi_k)_G = (\sum_i a_i \chi_i, \chi_k)_G = a_k.$$

This is a contradiction and finishes the proof. □

Later in theorem 120 we shall prove the reverse inequality: G has $k(G)$ inequivalent irreducible representations.

Theorem/Definition 111. *Let $\rho_1, \dots, \rho_s$ be a maximal set of non-equivalent irreducible characters of a finite group G. Let ρ be a representation of G. Then there are unique nonnegative integers n_i ($1 \le i \le s$) such that*

$$\rho \sim n_1 \rho_1 \oplus \cdots \oplus n_s \rho_s$$

where $n_i \rho_i$ means the diagonal sum of n_i copies of ρ_i. Indeed $n_i = (\chi_\rho, \chi_i)_G$ where χ_i denotes the character of ρ_i. We call n_i the **multiplicity** *of ρ_i in ρ.*

Proof. Existence was proved in corollary 92. We prove uniqueness. For all i

$$(\chi_\rho, \chi_i)_G = (\sum_j n_j \chi_j, \chi_i)_G = \sum_j n_j \delta_{ji} = n_i$$

so n_i is determined by ρ. □

Corollary 112. *Let ρ be a representation of a finite group G. Then ρ is irreducible if and only if $(\chi_\rho, \chi_\rho)_G = 1$.*

Proof. The implication $\Rightarrow$ was proved in theorem 107 (orthogonality). We prove $\Leftarrow$. By corollary 92 we can write $\rho \sim \bigoplus_i n_i \rho_i$ where ρ_i are irreducible and inequivalent. By theorem 107

$$1 = (\chi_\rho, \chi_\rho)_G = (\sum_i n_i \chi_i, \sum_i n_i \chi_i)_G = \sum_i n_i^2.$$

It follows that the n_i are zero except one of them, say $n_k = 1$. Then ρ is equivalent to ρ_k and therefore is irreducible. □

Theorem 113. *Let ρ, σ be representations of a finite group G. Then $\rho \sim \sigma \Leftrightarrow \chi_\rho = \chi_\sigma$.*

Proof. The implication $\Rightarrow$ is proposition 95. We prove $\Leftarrow$. Let $\rho_1, \ldots, \rho_s$ be a maximal set of inequivalent irreducible characters and let χ_i denote the character of ρ_i. Put $n_i = (\chi_\rho, \chi_i)_G$ so also $n_i = (\chi_\sigma, \chi_i)_G$. By theorem 111

$$\rho \sim \bigoplus_i n_i \rho_i \sim \sigma.$$

□

Exercise (5.7) Let G be a finite group. Recall that $\mathrm{Rep}_n(G)$ denotes the set of equivalence classes of n-dimensional representations of G. Prove that $\mathrm{Rep}_n(G)$ is finite.

5.3 Exercises

(5.8) Find an example of an infinite group G and two inequivalent representations $G \to \mathrm{GL}(n, \mathbb{C})$ with the same character.

(5.9) For $g \in S_n$ let $f(g)$ be the number of fixed points of g, that is, the number of $x \in \{1, \ldots, n\}$ such that $g(x) = x$. Prove that $\sum_{g \in S_n} f(g)^2 = 2\,n!$ if $n > 1$.

(5.10) Let $0 \le k \le n$ and write $A_n = \{1, \ldots, n\}$. Let V be an $\binom{n}{k}$-dimensional vector space with basis $\{v(I) \mid I \subset A_n,\ \#I = k\}$.

Let $G = S_n$ act on V by $g\,v(I) = v(gI)$ where $gI = \{gi \mid i \in I\}$. Let χ be the character of the $\mathbb{C}G$-module V. Prove

$$(\chi, \chi)_G = \min(k, n-k) + 1.$$

(5.11) An element of a group is said to be **real** if it is conjugate to its inverse.

(a) Let g be a real element of a finite group G. Prove $\chi(g) \in \mathbb{R}$ for all characters χ of G.

(b) Prove that all elements of the symmetric group S_n are real.

(c) Find all real elements in the alternating group A_n.

(5.12) Find the conjugacy classes and the centre of D_{2n} if n is even.

(5.13) Let $H \trianglelefteq G$ be groups such that $G = \{hz \mid h \in H,\ z \in Z(G)\}$. Let ρ be an irreducible representation of G. Prove that the restriction of ρ to H is also irreducible.

(5.14) (a) Let ρ be an irreducible representation of a finite group G. Prove that $\sum_{g \in G} \rho(g) = 0$ unless ρ is the trivial representation of degree 1.

(b) Let $H \leq G$ be groups and let $g \in G$ be such that all elements of Hg are conjugate. Let χ be a character of G such that $(\chi_H, 1_H)_H = 0$. Show that $\chi(g) = 0$. (Note: $\chi_H := \chi|_H$ and 1_H is the trivial linear character of H.)

(5.15) Restate and reprove lemma 105 in the language of $\mathbb{C}G$-modules.

(5.16) Let G be a finite group and V a finite-dimensional $\mathbb{C}G$-module. Let χ be an irreducible character of G. Define $p_\chi\colon V \to V$ by $p_\chi v = \sum_{g \in G} \chi(g)\, gv$. Prove that $p_\chi(V)$ is one of the isotypical components of V as defined in exercise 4.18 (or zero).

(5.17) Let G be a finite group. Recall that $\mathbb{C}(G)$ denotes the set of functions from G to $\mathbb{C}$. For $p, q \in \mathbb{C}(G)$ define the **convolution** $p * q \in \mathbb{C}(G)$ by

$$(p * q)(x) = \sum_{y \in G} p(y^{-1})\, q(yx).$$

(a) Prove that $*$ is associative.

(b) Prove that if $p, q \in \mathbb{C}(G)$ are class functions then so is $p * q$.

(c) Prove that $p * q = q * p$ for all $p \in \mathrm{CF}(G)$, $q \in \mathbb{C}(G)$.

(d) Let ρ, σ be irreducible representations of G. Prove:

$$\chi_\rho * \chi_\sigma = \begin{cases} 0 & \text{if } \rho \not\sim \sigma \\ \frac{\#G}{\deg \rho} \cdot \chi_\rho & \text{if } \rho \sim \sigma. \end{cases}$$

Hint: use the result of exercise (5.20) (generalised orthogonality).

(5.18) Let G be a finite group and $\chi_1, \ldots, \chi_s$ its irreducible characters. Let d_i be the degree of χ_i. Prove:

$$\sum_{n \geq 0} \#\mathrm{Rep}_n(G) \cdot t^n = \prod_{i=1}^{s} \frac{1}{1 - t^{d_i}}.$$

(5.19) (Adopted from the 2012 exam.) Let $n \geq 4$ and put $A = \{1, 2, \ldots, n\}$. Let V be a complex vector space of dimension $n(n-1)/2$ and with basis $\{v_{ab} \mid a, b \in A,\ a < b\}$. We also write $v_{ba} = v_{ab}$.

The symmetric group $G = S_n$ acts on V by putting $g\, v_{a,b} = v_{ga,gb}$ for all $g \in G$. This makes V into a $\mathbb{C}G$-module whose character will be written χ. The linear map $V \to V\colon v \mapsto gv$ is denoted by t_g.

For $a, b, c, d \in A$ with $a \neq b$, $c \neq d$ put

$$M(a,b,c,d) = \left\{ g \in S_n \;\middle|\; gv_{ab} = v_{ab},\ gv_{cd} = v_{cd} \right\}$$

and $m(a,b,c,d) = \#M(a,b,c,d)$.

(a) Calculate the trace of t_h if $n = 8$ and $h = (158)(24)$.

(b) Prove directly from the definitions

$$4 \cdot n! \cdot (\chi, \chi)_G = \sum_{\substack{a,b,c,d \in A \\ a \neq b,\ c \neq d}} m(a,b,c,d).$$

(c) Assume that $a, b, c, d \in A$ are distinct. Prove

$$m(a,b,c,d) = 4(n-4)!\,,$$
$$m(a,b,a,b) = 2(n-2)!\,,$$
$$m(a,b,a,c) = (n-3)!\,.$$

(d) Use the foregoing to prove $(\chi, \chi)_G = 3$.

(e) Prove that there are distinct irreducible characters χ_1, χ_2, χ_3 of S_n such that $\chi = \chi_1 + \chi_2 + \chi_3$.

(5.20) Let ρ, σ be irreducible representations of a finite group G and let $h \in G$. Prove the **generalised orthogonality**

$$\sum_{g \in G} \chi_\sigma(g^{-1})\, \chi_\rho(hg) = \begin{cases} 0 & \text{if } \rho \not\sim \sigma \\ \#G\, \dfrac{\chi_\rho(h)}{\chi_\rho(1)} & \text{if } \rho \sim \sigma. \end{cases}$$

Hint: modify the proof of theorem 107.

(5.21) Let ρ be an irreducible representation of a finite group G. Prove $\sum_{g \in G} \rho(g) = 0$ unless ρ is the trivial representation of degree 1.

6 The regular representation

For a group G, let $V^{\text{reg}} = V^{\text{reg}}(G)$ denote a complex vector space with basis $\{e_x \mid x \in G\}$ (this is any set in bijection with G). Then every element of V^{reg} can uniquely be written as a sum

$$\sum_{x \in G} a_x\, e_x$$

where $a_x \in \mathbb{C}$ are such that only finitely many a_x are nonzero.

We define an action of G on V^{reg} by

$$g\Big(\sum_{x \in G} a_x\, e_x \Big) = \sum_{x \in G} a_x\, e_{gx}$$

for all $g \in G$, $a_x \in \mathbb{C}$, only finitely many nonzero. Prove yourself that this defines an action.

The pair of V^{reg} together with this action is a $\mathbb{C}G$-module called the **regular module**.

Suppose from now on that G is finite. Then V^{reg} is finite-dimensional and $\dim V^{\text{reg}} = \#G$. The **regular representation** ρ^{reg} of G is the representation afforded by (V^{reg}, A) where A is the (ordered) basis of the e_x with any total ordering. The character χ^{reg} of the regular representation is called the **regular character**.

Example 114. Let $G = C_2 \times C_2$. Then the elements of G can be written $1, x, y, xy$ for appropriate generators x, y of G. Suppose that ρ^{reg} is afforded by (V^{reg}, A) where A is the basis $A = (e_1, e_x, e_y, e_{xy})$. Then

$$\rho^{\text{reg}}(x) = \begin{pmatrix} \cdot & 1 & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{pmatrix}, \qquad \rho^{\text{reg}}(y) = \begin{pmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \end{pmatrix}.$$

Remark 115. A **permutation matrix** is a square matrix in which every row or column has zeroes everywhere except for a 1 in one position. Then the $n \times n$ permutation matrices form a subgroup of $\mathrm{GL}(n, \mathbb{C})$ isomorphic to the symmetric group S_n. It is clear that the image of a regular representation consists of permutation matrices.

Lemma 116. *Let G be a finite group. Then*

$$\chi^{\text{reg}}(1) = \#G, \qquad \chi^{\text{reg}}(g) = 0 \textit{ for all } g \in G \setminus \{1\}.$$

Proof. Firstly $\chi^{\text{reg}}(1) = \dim V^{\text{reg}} = \#G$.

Let now $g \in G \smallsetminus \{1\}$. Any nonzero entry of $\rho^{\text{reg}}(g)$ is in position (gx, x) for some $x \in G$. This is not on the diagonal because $gx \neq x$. Thus the diagonal of $\rho^{\text{reg}}(g)$ consists of zeroes only and $\chi^{\text{reg}}(g) = \operatorname{tr} \rho^{\text{reg}}(g) = 0$. □

Proposition 117. *Let $\chi_1, \dots, \chi_s$ be the irreducible characters of G and put $d_i = \chi_i(1)$. Then*

$$\chi^{\text{reg}} = \sum_{i=1}^{s} d_i \, \chi_i. \tag{118}$$

Proof. Put $n_i = (\chi^{\text{reg}}, \chi_i)_G$. By theorem 111 we have $\chi^{\text{reg}} = \sum_i n_i \, \chi_i$. Using lemma 116 we find

$$n_i = (\chi^{\text{reg}}, \chi_i)_G = \frac{1}{\#G} \sum_{x \in G} \chi^{\text{reg}}(x) \, \overline{\chi_i(x)} = \frac{1}{\#G} \big(\#G \cdot \overline{\chi_i(1)}\big) = d_i$$

which finishes the proof. □

Corollary 119. *Let $\chi_1, \dots, \chi_s$ be the irreducible characters of G and put $d_i = \chi_i(1)$. Then*

$$\#G = d_1^2 + \cdots + d_s^2.$$

Proof. Evaluating both sides in (118) at $1 = 1_G$ we get

$$\#G = \chi^{\text{reg}}(1) = \sum_{i=1}^{s} d_i \, \chi_i(1) = \sum_{i=1}^{s} d_i^2.$$ □

Recall that $I(G)$ denotes the set of irreducible characters of G and $k(G)$ the number of conjugacy classes.

Theorem 120. $\#I(G) = k(G)$.

Proof. Let $k = k(G)$. By corollary 110 we have $\#I(G) \leq k$. It remains to prove $\#I(G) \geq k$.

Recall the vector space $\mathrm{CF}(G)$ of class functions on G. It is of dimension k and equipped with an inner product $(\cdot, \cdot)_G$. Also $I(G) \subset \mathrm{CF}(G)$. It remains to prove that if f is a class function on G orthogonal to $I(G)$ then $f = 0$.

For a representation ρ of G, put

$$\rho^f := \sum_{g \in G} f(g) \, \rho(g^{-1}).$$

We claim that ρ^f is an intertwiner from ρ to itself. Indeed, for all $x \in G$ we have

$$\begin{aligned} \rho(x) \, \rho^f \, \rho(x^{-1}) &= \rho(x) \Big(\sum_{g \in G} f(g) \, \rho(g^{-1}) \Big) \rho(x^{-1}) = \sum_{g \in G} f(g) \, \rho(x \, g^{-1} x^{-1}) \\ &\overset{*}{=} \sum_{h \in G} f(x^{-1} h \, x) \, \rho(h^{-1}) = \sum_{h \in G} f(h) \, \rho(h^{-1}) = \rho^f \end{aligned}$$

where the starred equality is because of the bijection $G \to G$: $g \mapsto x \, g \, x^{-1}$. This proves our claim that $\rho^f \colon \rho \to \rho$ is an intertwiner.

Let ρ be an irreducible representation of G. As ρ^f is an intertwiner from ρ to itself, Schur's lemma (theorem 104) implies that there exists $\alpha \in \mathbb{C}$ such that $\rho^f = \alpha \, I_n$ where $n = \deg \rho$ and I_n is the $n \times n$ identity matrix. We find the value of α as follows:

$$\begin{aligned} n \, \alpha = \operatorname{tr}(\alpha I_n) = \operatorname{tr} \rho^f &= \operatorname{tr} \sum_{g \in G} f(g) \, \rho(g^{-1}) = \sum_{g \in G} f(g) \, \operatorname{tr} \rho(g^{-1}) \\ &= \sum_{g \in G} f(g) \, \chi_\rho(g^{-1}) = \sum_{g \in G} f(g) \, \overline{\chi_\rho(g)} = \#G \cdot (f, \chi_\rho)_G = 0 \end{aligned}$$

by our assumption that f is orthogonal to $I(G)$. We have proved that $\rho^f = 0$ if ρ is irreducible.

It follows that also $\rho^f = 0$ if ρ is not irreducible because $T\,\rho\,T^{-1} = \rho_1 \oplus \cdots \oplus \rho_k$ for some irreducible representations ρ_i and some $T \in \mathrm{GL}(n, \mathbb{C})$ ($n = \deg \rho$) which implies

$$T\,\rho^f\,T^{-1} = \rho_1^f \oplus \cdots \oplus \rho_k^f = 0$$

whence $\rho^f = 0$.

Let us put $\rho = \rho^{\mathrm{reg}}$ in the equation $\rho^f = 0$. We find

$$\sum_{g \in G} f(g)\,\rho^{\mathrm{reg}}(g^{-1}) = 0.$$

Note that the elements of the image of ρ^{reg} are linearly independent; indeed their first columns are. It follows that $f = 0$ which finishes the proof. □

A character is said to be **linear** if it is of degree 1.

Theorem 121. *A finite group G is abelian if and only if all its irreducible characters are linear.*

Proof. Write $k = k(G)$. By corollary 119 and theorem 120

$$\#G = d_1^2 + \cdots + d_k^2$$

and $d_i > 0$. So G is abelian $\Leftrightarrow k = \#G \Leftrightarrow (d_i = 1$ for all $i)$. □

6.1 Exercises

(6.1) Prove proposition 26 (representations of cyclic groups) by the more sophisticated methods of chapters 4, 5, 6.

(6.2) Let G be a finite group. Prove or disprove:

(a) There exists a representation $\rho\colon D_6 \to \mathrm{GL}(n, \mathbb{C})$ with $\det \rho(r) = \exp(2\pi i/3)$.

(b) $I(G)$ is a basis of $\mathrm{CF}(G)$.

(c) Let G be a group (not necessarily finite). Let V be a finite-dimensional $\mathbb{C}G$-module. Then V admits a G-invariant inner product.

(d) Let $f\colon V \to W$ be a homomorphism of $\mathbb{C}G$-modules. Then f is 0 or an isomorphism.

(e) Let G be a group (not necessarily finite). Let V be a finite-dimensional $\mathbb{C}G$-module and $\langle \cdot, \cdot \rangle$ a G-invariant inner product on V. Then V is a direct sum of simple $\mathbb{C}G$-submodules.

(f) Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation of a finite group G such that the elements of $\rho(G)$ are linearly independent and ρ is injective. Then $(\chi_\rho, \phi)_G > 0$ for all irreducible characters ϕ of G.

(g) Let $\rho\colon G \to \mathrm{GL}(n, \mathbb{C})$ be a representation of a finite group G. Then $|\det \rho(x)| = 1$ for all $x \in G$.

(h) Let $\rho_1, \ldots, \rho_k$ be irreducible representations of a finite group G and $\sigma = n_1\,\rho_1 \oplus \cdots \oplus n_k\,\rho_k$ where $n_i \in \mathbb{Z}_{\geq 0}$. Then $(\chi_\sigma, \chi_\sigma)_G = n_1^2 + \cdots + n_k^2$.

(6.3) Let G be a finite group and $K(G)$ the set of conjugacy classes of G. Fix conjugacy classes $C_1, \ldots, C_m \in K(G)$ and put

$$N(C_1, \ldots, C_m) := \#\{(g_1, \ldots, g_m) \in C_1 \times \cdots \times C_m \mid g_1 \cdots g_m = 1\}.$$

If χ is any class function on G and $C \in K(G)$, write $\chi(C) := \chi(g)$ for one (hence any) $g \in G$. Let I denote the set of irreducible characters of G. In this exercise you will prove the **Frobenius formula**:

$$N(C_1, \ldots, C_m) = \frac{\#C_1 \cdots \#C_m}{\#G} \sum_{\chi \in I} \frac{\chi(C_1) \cdots \chi(C_m)}{\chi(1)^{m-2}}. \tag{122}$$

If $C \in K(G)$ and ρ is a representation of G, define

$$\rho_C := \sum_{g \in C} \rho(g).$$

(a) Prove that ρ_C is an intertwiner $\rho \to \rho$.

(b) Suppose moreover that ρ is irreducible of degree n. Prove that there exists $\lambda_\rho \in \mathbb{C}$ such that $\rho_C = \lambda_C \cdot I_n$.

(c) Prove: $\lambda_\rho = \dfrac{\chi_\rho(C)}{\chi_\rho(1)} \cdot \#C$.

(d) Let us use $\sum_0$ as shorthand for $\sum_{g_1 \in C_1} \cdots \sum_{g_m \in C_m}$. Prove:

$$\textstyle\sum_0 \chi^{\text{reg}}(g_1 \cdots g_m) = \sum_0 \sum_{\chi \in I} \chi(1) \cdot \chi(g_1 \cdots g_m). \tag{123}$$

(e) Compute the right hand side of (123). Hint: if ρ is a representation of G, how can $\sum_0 \rho(g_1 \cdots g_m)$ be factorized?

(f) Compute the left hand side of (123) and deduce (122).

(6.4) Use the notation of exercise 6.3 and put

$$N_g(C_1, \ldots, C_m) := \#\left\{ \begin{matrix} (a_1, b_1, a_2, b_2, \ldots, a_g, b_g, g_1, \ldots, g_m) \\ \in G^{2g} \times C_1 \times \cdots \times C_m \end{matrix} \;\middle|\; \begin{matrix} [a_1, b_1] \cdots [a_g, b_g] \\ g_1 \cdots g_m = 1 \end{matrix} \right\}$$

where $[a, b] = aba^{-1}b^{-1}$. Prove:

$$N_g(C_1, \ldots, C_m) = (\#G)^{2g-1} \#C_1 \cdots \#C_m \sum_{\chi \in I} \frac{\chi(C_1) \cdots \chi(C_m)}{\chi(1)^{m+2g-2}}.$$

Hint: use Frobenius' formula from exercise 6.3.

Remark: This has the following topological interpretation. Let S be a compact connected oriented surface (real 1-manifold) with m boundary circles. Then $N_g(C_1, \ldots, C_m)$ is the number of homomorphisms $\pi_1 S \to G$ such that the image of the ith boundary circle is in C_i.

(6.5) Let G, H be finite groups. Let $I(G)$ denote the set of irreducible characters of G.

(a) Prove that $I(G) \times I(H)$ and $I(G \times H)$ have equal cardinalities.

(b) (Not for credit). You may assume that if χ, ϕ are characters of a group K then so is $\chi\phi$ defined by $(\chi\phi)(g) = \chi(g)\,\phi(g)$. This is true but beyond our scope. Prove that if p is a character of G and q a character of H then

$$\begin{aligned} p * q \colon G \times H &\longrightarrow \mathbb{C} \\ (g, h) &\longmapsto p(g)\,q(h) \end{aligned}$$

is a character of $G \times H$.

(c) Prove that the map $(p, q) \mapsto p * q$ defines a bijection $I(G) \times I(H) \to I(G \times H)$.

Hint: first prove $(p * q, r * s)_{G \times H} = (p, r)_G\,(q, s)_H$ for all $p, r \in I(G)$, $q, s \in I(H)$.

7 Character tables

7.1 Character tables

Let G be a finite group. If C is a conjugacy class of G and $g \in C$ and f is a class function on G we often write $f(C)$ instead of $f(g)$.

Let $C_1, \dots, C_k$ be the conjugacy classes of G and assume $C_1 = \{1\}$. Let $\chi_1, \dots, \chi_k$ be the irreducible characters of G and assume that χ_1 is the trivial linear character (that is, $\chi_1(g) = 1$ for all $g \in G$). The square matrix

$$\big(\chi_i(C_j)\big)_{ij}$$

is called the **character table** of G. More precisely, a permutation of the rows or columns or both (fixing the first row and first column) is not considered to change the character table.

The character table of a finite group contains a good deal of information about the group but not everything: there are non-isomorphic groups with the same character table (exercise 7.13).

The character table may be annotated with more useful information, for example $\#C_j$ for every j. The latter information can however be deduced from the body of the character table (exercise 7.8).

Example 124. Consider $C_4 = \langle c \mid c^4 \rangle$. Write $\varepsilon = \sqrt{-1}$. We know that all irreducible characters of C_4 are linear; we can write $\chi_i(c) = \varepsilon^{i-1}$. Also $c^{j-1} \in C_{j-1}$. It follows that $\chi_i(C_j) = \varepsilon^{(i-1)(j-1)}$ and the character table is

	1	c	c^2	c^3
χ_1	1	1	1	1
χ_2	1	ε	ε^2	ε^3
χ_3	1	ε^2	ε^4	ε^6
χ_4	1	ε^3	ε^6	ε^9

.

Example 125. Next we compute the character table of $G = D_6$. Recall that D_6 is $\langle r, s \mid r^3, s^2, (rs)^2 \rangle$ and that the conjugacy classes are 1^G, r^G, s^G.

First we find the linear characters. Recall that, for any group G, a linear character is just a homomorphism $G \to \mathbb{C}^\times$ and all linear characters are irreducible. By theorem 61, there exists a linear character χ_i with $\chi_i(r) = \alpha$ and $\chi_i(s) = \beta$ if and only if

$$1 = \alpha^3 = \beta^2 = (\alpha\beta)^2. \tag{126}$$

This is just a system of equations in complex numbers and can therefore be solved by any usual means. We find that (126) is equivalent to $\alpha = 1$ and $\beta \in \{-1, 1\}$. We thus find two linear characters:

	1	r	s
χ_1	1	1	1
χ_2	1	1	-1

.

Let χ_3 be the remaining irreducible character and d_i the degree of χ_i. Then $d_3 = 2$ because by corollary 119

$$6 = \#D_6 = d_1^2 + d_2^2 + d_3^2 = 1 + 1 + d_3^2.$$

One way to find χ_3 is by proposition 117 which says $\chi^{\text{reg}} = d_1\,\chi_1 + d_2\,\chi_2 + d_3\,\chi_3$. The result is:

	1	r	s
χ_1	1	1	1
χ_2	1	1	-1
χ_3	2	-1	0

.

7.2 *Properties of character tables*

We now look at some properties of characters, which are especially useful when calculating character tables.

Proposition/Definition 127: Duals and twists. *Let χ and μ be irreducible characters of G, with $\deg\mu = 1$.*

(a) *The function $\bar{\chi}\colon g \mapsto \overline{\chi(g)}$ is also an irreducible character called the* **dual** *of χ.*

(b) *The function $\chi\mu\colon g \mapsto \chi(g)\,\mu(g)$ is also an irreducible character called a* **twist** *of χ.*

Proof. Part (a). Suppose $\chi = \chi_\rho$ where ρ is a representation of degree n. There exists an automorphism c of $\mathrm{GL}(n,\mathbb{C})$ defined by $(cA)_{ij} = \overline{A}_{ij}$ for all i,j. It follows that $c \circ \rho$ is also a representation of G. It character is clearly $\bar{\chi}$ which is therefore a character.

It remains to prove that $\bar{\chi}$ is irreducible. This follows from corollary 112 and the following:

$$(\bar{\chi},\bar{\chi})_G = \frac{1}{\#G}\sum_{g\in G}\bar{\chi}(g)\,\overline{\bar{\chi}(g)} = \frac{1}{\#G}\sum_{g\in G}\bar{\chi}(g)\,\chi(g) = (\chi,\chi)_G = 1.$$

Part (b). Write $\chi = \chi_\rho$. Define $\sigma(g) = \rho(g)\,\mu(g)$ for all g in G. In order to prove that σ is again a representation of G, observe

$$\sigma(gh) = \rho(gh)\,\mu(gh) = \rho(g)\,\rho(h)\,\mu(g)\,\mu(h) = \rho(g)\,\mu(g)\,\rho(h)\,\mu(h) = \sigma(g)\,\sigma(h)$$

for all $g,h \in G$. Its character is clearly $\chi\mu$ which is therefore a character.

In order to prove that it is irreducible, note that $\mu(g)\,\mu(g^{-1}) = 1$ for all $g \in G$ so that

$$(\chi\mu,\chi\mu)_G = \frac{1}{\#G}\sum_{g\in G}\chi(g)\,\mu(g)\,\chi(g^{-1})\,\mu(g^{-1}) = \frac{1}{\#G}\sum_{g\in G}\chi(g)\,\chi(g^{-1}) = 1.$$

By corollary 112 again the twist $\chi\mu$ is irreducible. □

Exercise (7.1) Let $A \in M_n(\mathbb{C})$. Prove that the rows of A are orthonormal ($A\,\overline{A}^{\mathrm{T}} = 1$) if and only if the columns are ($\overline{A}^{\mathrm{T}}\,A = 1$).

Theorem 128: Orthogonality. *Let G be a finite group. Let $\chi_1,\ldots,\chi_k$ be the irreducible characters, $C_1,\ldots,C_k$ the conjugacy classes and $n_j = \#C_j$. Let $s,t \in \{1,\ldots,k\}$.*

(a) *Row orthogonality:* $\sum_{j=1}^{k} n_j\,\chi_s(C_j)\,\bar{\chi}_t(C_j) = \#G\cdot\delta_{st}$.

(b) *Column orthogonality:* $\sum_{i=1}^{k} \chi_i(C_s)\,\bar{\chi}_i(C_t) = \dfrac{\#G\cdot\delta_{st}}{n_s}$.

Proof. (a). Recall theorem 107 (orthogonality for characters): $\#G \cdot \delta_{st} = \sum_{g \in G} f(g)$ where we write $f(g) = \chi_s(g)\,\bar{\chi}_t(g)$. Now $f(g)$ depends only on the conjugacy class of g. Part (a) follows.

(b). Write

$$a_{st} = \left(\frac{n_t}{\#G}\right)^{1/2} \chi_s(C_t)$$

and let A denote the $k \times k$ matrix $(a_{st})_{st}$. Then part (a) states that the rows of A are orthonormal. By exercise 7.1 its columns are orthonormal. This proves part (b). □

Example 129: A mystery group. Suppose G is a group of order 12 with 4 conjugacy classes. Suppose that one of the rows of its character table is

$g_1 = 1$	g_2	g_3	g_4
1	1	ω	ω^2

where $\omega = \exp(2\pi i/3)$. Find the full character table.

Solution. The trivial character and the dual of the given row are also irreducible characters. So far we have:

	1	g_2	g_3	g_4
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω

The number of irreducible characters equals the number of conjugacy classes, which is 4. Let χ_4 denote the last unknown row. We find $\chi_4(1)$ by corollary 119:

$$12 = \#G = \chi_1(1)^2 + \chi_2(1)^2 + \chi_3(1)^2 + \chi_4(1)^2 = 1 + 1 + 1 + \chi_4(1)^2$$

so $\chi_4(1) = 3$. We find the remaining values of χ_4 by column orthogonality (theorem 128). We get:

	1	g_2	g_3	g_4
χ_1	1	1	1	1
χ_2	1	1	ω	ω^2
χ_3	1	1	ω^2	ω
χ_4	3	-1	0	0

□

Exercise (7.2) Use column orthogonality to find the sizes of the conjugacy classes in the above example.

7.3 Characters and normal subgroups

Definition 130. Let ρ be a representation of a group G. We define

$$\ker \chi_\rho := \ker \rho = \{g \in G \mid \rho(g) = 1\}.$$

Lemma 131. *Let χ be a character of a finite group G. Then*

$$\ker \chi = \{g \in G \mid \chi(g) = \chi(1)\}.$$

Proof. The inclusion $\subset$ is clear. We prove $\supset$. Write $\chi = \chi_\rho$ and $n = \chi(1)$. Let $g \in G$ be such that $\chi(g) = \chi(1)$. By lemma 103 there are roots of unity $\omega_1, \dots, \omega_n$ such that $\chi(g) = \omega_1 + \cdots + \omega_n$. Then $|\omega_i| = 1$ for all i and $n = \omega_1 + \cdots + \omega_n$ from which we deduce $\omega_i = 1$ for all i. By lemma 103 $\rho(g)$ is diagonalisable so $\rho(g) = 1$. This finishes the proof. □

Theorem/Definition 132: Lifting. *Let $f\colon G \to H$ be a homomorphism of finite groups with kernel N.*

(a) *There is a map*

$$p\colon \left\{ \begin{array}{l} \text{characters} \\ \text{of } H \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{characters } \lambda \text{ of } G \\ \text{with } N \subset \ker \lambda \end{array} \right\}$$

defined by $p(\chi) = \chi \circ f$. This is known as the **pull-back** *or* **lift***.*

(b) *Suppose that f is surjective (for example, $H = G/N$ and f is the natural map). Then p is bijective.*

Proof. (a). Let ρ be a representation of H and $\chi := \chi_\rho$. Then $\rho \circ f$ is a representations of G whose character is clearly $\chi \circ f = p(\chi)$. Therefore $p(\chi)$ is a character of G.

(b). Proof of surjectivity. Let σ be a representation of G whose kernel contains N. Let ρ be the representation of H defined by $\rho(f(x)) = \sigma(x)$. This is well-defined because f is surjective and because $f(x) = f(y) \Rightarrow xN = yN \Rightarrow \sigma(x) = \sigma(y)$. Then $\chi_\sigma = p(\chi_\rho)$.

Proof of injectivity. Let $p(\lambda) = p(\mu)$. Then $\lambda \circ f = \mu \circ f$. Since f is surjective, $\lambda = \mu$. Therefore p is injective. □

Theorem 133. *Let G be a finite group.*

(a) *For any irreducible characters $\lambda_1, \dots, \lambda_n$ of G, $\ker(\lambda_1) \cap \cdots \cap \ker(\lambda_n)$ is a normal subgroup of G.*

(b) *All normal subgroups of G arise this way.*

Proof. (a). It is immediate from the definition that $\ker \lambda_i$ is a normal subgroup of G. The result follows because every intersection of normal subgroups is again a normal subgroup (exercise 3.3).

(b). Let N be a normal subgroup of G. Let ρ be an injective representation of G/N (for example, the regular representation) and let $f\colon G \to G/N$ be the natural map. Then $\rho \circ f$ is a representation of G whose kernel is N. Let $\rho \circ f \sim \sigma_1 \oplus \cdots \oplus \sigma_n$ with σ_i irreducible for all i (such a decomposition exists). Let λ_i be the character of σ_i. Then $N = \ker(\lambda_1) \cap \cdots \cap \ker(\lambda_n)$. □

Exercise (7.3) Let G be the mystery group of example 129. Find all normal subgroups of G.

7.4 Linear characters and the derived subgroup

Definition 134. Let G be a group and $x, y \in G$. The **commutator** of x, y is

$$[x, y] := x\, y\, x^{-1}\, y^{-1}.$$

The **derived subgroup** or **commutator subgroup** of G is the subgroup of G generated by the set of all commutators:

$$G' = [G, G] = \Big\langle \{ [x, y] \mid x, y \in G \} \Big\rangle$$ □

Note that $[x, y] = 1$ if and only if $xy = yx$ (that is, x, y commute). Warning: some elements of G' may not be commutators.

Example 135. (a). It is clear that a group G is abelian if and only if $G' = 1$.
(b). We have $S_n' = A_n$. If $n \geq 4$ then $A_n' = A_n$.

Proposition 136. *Let G be a group.*

(a) *Then $G' \trianglelefteq G$.*
(b) *Let $N \trianglelefteq G$. Then G/N is abelian if and only if $G' \subset N$.*

Proof. (a). By exercise 3.30 it is enough to show that any conjugate of a commutator is again a commutator. Well, if $g \in G$ then $x \mapsto x^g = g^{-1}xg$ is an automorphism of G so for all x, y in G we have

$$[x, y]^g = (xyx^{-1}y^{-1})^g = (x^g)(y^g)(x^g)^{-1}(y^g)^{-1} = [x^g, y^g]$$

which is a commutator.
(b). We have

$$\begin{aligned} &G/N \text{ is abelian} \\ &\iff [xN, yN] = 1 \text{ for all } x, y \in G \\ &\iff (xN)(yN)(xN)^{-1}(yN)^{-1} = 1 \text{ for all } x, y \in G \\ &\iff xyx^{-1}y^{-1}N = N \text{ for all } x, y \in G \\ &\iff [x, y] \in N \text{ for all } x, y \in G \\ &\iff G' \subset N. \end{aligned}$$

□

Proposition 137. *Let G be a group.*

(a) *A linear character of G is the same as the lift to G of a linear character of G/G'.*
(b) *The number of linear characters of G is $\#(G/G')$.*

Proof. (a). It is clear that lifting a linear character of G/G' to G gives a linear character of G. In order to prove the converse, let $\chi = \chi_\rho$ be a linear character of G. Then $\rho(G) \subset \mathrm{GL}(1, \mathbb{C})$ so $\rho(G)$ is abelian. By proposition 136 $G' \subset \ker \rho$. So $G' \subset \ker \chi$. By theorem 132 χ is a lift of a character of G/G'.

(b). Write $Q = G/G'$. We know that Q is abelian so it has precisely $\#Q$ conjugacy classes. By theorem 120 it has $\#Q$ irreducible characters. But irreducible characters of Q are the same thing as linear characters of Q by theorem 121. So Q has precisely $\#Q$ linear characters. By (a) G has the same number of linear characters (noting that no two distinct characters of G/G' lift to the same character of G). □

Exercise (7.4) Use proposition 137 to prove that there is no finite group G such that if $\chi_1, \ldots, \chi_k$ are its irreducible characters in appropriate order then

$$(\chi_1(1), \ldots, \chi_k(1)) = (1, 1, 5).$$

7.5 More examples

Exercise (7.5) Let p, q be characters of a finite group G with q irreducible. Then $p - q$ is a character if and only if $(p, q)_G \geq 1$.

Example 138. We shall calculate the character table of S_4.

First some generalities about S_n. The alternating group A_n is a normal subgroup of S_n of index 2. It follows that there is a 1-dimensional representation of S_n taking all elements of A_n to 1 and other elements to -1. This is known as the **sign representation** and its character is the **sign character**.

Recall the permutation representation $\rho^p \colon S_n \to \mathrm{GL}(n, \mathbb{C})$ defined by $(\rho^p s)e_i = e_{s(i)}$. Its character (denoted p) is called the **permutation character** (it is not irreducible). Note that $p(g) = \#\{x \in \{1, \dots, n\} \mid g(x) = x\}$, the number of fixed points of g for all $g \in S_n$.

Put now $n = 4$. We begin by calculating the conjugacy classes of S_4 and their sizes:

$C \ni x$	1	(12)	(123)	(1234)	(12)(34)
$\#C$	1	6	8	6	3

Let χ_1 be the trivial linear character. Let χ_2 be the sign character. Let p be the permutation character. We get the following table.

$\#C$	1	6	8	6	3
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
p	4	2	1	0	0

We have $24 \cdot (p, \chi_1)_G = 1 \cdot 1 \cdot 4 + 6 \cdot 1 \cdot 2 + 8 \cdot 1 \cdot 1 + 0 + 0 = 24$ so that $(p, \chi_1)_G = 1$ and $\chi_3 := p - \chi_1$ is a character by exercise 7.5. Let $\chi_4 := \chi_3\chi_2$ be its twist. We have

$\#C$	1	6	8	6	3
χ_3	3	1	0	-1	-1
χ_4	3	-1	0	1	-1

.

We find $24(\chi_3, \chi_3)_G = 1 \cdot 9 + 6 \cdot 1 + 0 + 6 \cdot 1 + 3 \cdot 1 = 24$ whence $(\chi_3, \chi_3)_G = 1$. Therefore χ_3 is irreducible and hence so is χ_4.

Let χ_5 be the remaining irreducible character. We find $\chi_5(1)$ by the formula $24 = \#G = \sum_{i=1}^{5} \chi_i(1)^2$. We find the remaining values of χ_5 by orthogonality of columns. Here is the full table:

$C \ni x$	1	(12)	(123)	(1234)	(12)(34)
$\#C$	1	6	8	6	3
p	4	2	1	0	0
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	3	1	0	-1	-1
χ_4	3	-1	0	1	-1
χ_5	2	0	-1	0	2

.

Example 139. Let G be the group of permutations of $\mathbb{Z}/5$ of the form $x \mapsto ax + b$ where $a, b \in \mathbb{Z}/5$ and a is invertible. Define $r, s \in G$ by $r(x) = x + 1$, $s(x) = 2x$.

(a) Prove $G = \langle r, s \rangle$.

(b) Prove that $r^5 = 1$, $s^4 = 1$, $srs^{-1} = r^2$. (We don't need to prove that these present G.)

(c) Prove that every element of G can be written uniquely as $r^k s^\ell$ where $0 \le k \le 4$ and $0 \le \ell \le 3$.

(d) Define a map $f\colon G \to (\mathbb{Z}/5)^\times$ by $(x \mapsto ax+b) \mapsto a$. Prove that f is a homomorphism. Deduce that there is a homomorphism $h\colon G \to C_4 = \langle c \mid c^4 \rangle$, $h(r) = 1$, $h(s) = c$.

(e) Prove that the conjugacy classes are

$$\{1\}, \quad \{r, r^2, r^3, r^4\}, \quad \{r^k s \mid k\}, \quad \{r^k s^2 \mid k\}, \quad \{r^k s^3 \mid k\}.$$

(f) Find the character table of G.

Solution. (a). We have $s(x) = 2x$, $s^2(x) = 4x$, $s^3 = 3x$. Therefore $x \mapsto ax$ is in $\langle s \rangle$ for all a. Finally $r^b(ax) = ax + b$.

(b). Straightforward. We just do the last one: $srs^{-1}(x) = sr(3x) = s(3x+1) = x + 2 = r^2(x)$.

(c). Existence follows easily from (a) and the relation $srs^{-1} = r^2$. Uniqueness follows by comparison with $\#G$.

(d). Define $u, v \in G$ by $u(x) = ax + b$, $v(x) = cx + d$. Then $uv(x) = u(cx + d) = a(cx+d) + b = acx + (ad+b)$. This proves that f is a homomorphism. But $(\mathbb{Z}/5)^\times \cong C_4$ which yields h.

(e). The image C_4 of h is abelian. Therefore, if two elements of G have different images in C_4 then they are not conjugate. Clearly $\{1\}$ is a conjugacy class. This proves that the given sets are each a union of conjugacy classes.

Now $srs^{-1} = r^2$ so conjugating by s yields the permutation $r \mapsto r^2 \mapsto r^4 \mapsto r^3$.

We have $sr = r^2 s$ so $r^{-1}(r^k s)r = (r^{-1} r^k r^2)s = r^{k+1}s$ so conjugating by r^{-1} cyclically permutes $\{r^k s \mid k\}$. Likewise for the remaining two classes.

(f). Pulling back the irreducible characters of C_4 gives 4 linear characters $\chi_1, \ldots, \chi_4$. Since G has precisely 5 conjugacy classes, there is one remaining character χ_5. Its degree is found by the condition $\#G = \sum_i \chi_i(1)^2$. Its remaining values are found by orthogonality of columns. We get:

	1	r	s	s^2	s^3
χ_1	1	1	1	1	1
χ_2	1	1	i	-1	$-i$
χ_3	1	1	-1	1	-1
χ_4	1	1	$-i$	-1	i
χ_5	4	-1	0	0	0

□

7.6 Exercises

(7.6) (a) Find the conjugacy classes of A_4.

(b) Prove that one of the rows in the character table of A_4 is

1	a	b	c
1	1	ω	ω^2

where $\omega = \exp(2\pi i/3)$.

(c) Briefly justify that the mystery group of example 129 and A_4 have the same character table.

(7.7) Let χ be a character of an infinite group G. Prove that $g \mapsto \overline{\chi(g^{-1})}$ and $g \mapsto \overline{\chi(g)}$ are again characters of G. Give an example where $\chi(g^{-1}) \neq \overline{\chi(g)}$.

(7.8) Let χ_i $(1 \leq i \leq k)$ be the irreducible characters of a finite group G. Let C_j $(1 \leq j \leq k)$ be the conjugacy classes of G and pick an element $g_j \in C_j$ for each j.

If one is only given the function $(i, j) \mapsto \chi_i(g_j)$, show that one can find the unique j such that $g_j = 1$, as well as the degree of χ_i and $\#C_i$.

(7.9) Calculate the conjugacy classes and character table for the group

$$\langle a, b, c \mid a^3,\ b^3,\ aba^{-1}b^{-1},\ c^2,\ cac^{-1}b^{-1} \rangle$$

(7.10) Find the character tables of the finite dihedral groups.

(7.11) (Adopted from the 2012 exam.) We define a group

$$G = \langle x, y, z \mid x^2 = z,\ y^2 = z,\ (xy)^2 = z,\ z^2 = 1 \rangle$$

and consider x, y, z as elements of G. We write $(g_1, \ldots, g_5) = (1, x, y, xy, z)$.

(a) Prove that there are precisely 4 linear characters of G, written $\chi_1, \ldots, \chi_4$. Give a table with the values $\chi_i(g_j)$ whenever $1 \leq i \leq 4,\ 1 \leq j \leq 5$.

(b) Prove that there exists a unique representation ρ of G such that $\rho(x) = A$, $\rho(y) = B$ where we write

$$A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

(c) Prove that ρ is irreducible.
Hint: Proceed directly from the definition of irreducibility (or simplicity of modules).

(d) Prove that $\langle z \rangle$ is a normal subgroup of G. Give an explicit presentation of the quotient group $G/\langle z \rangle$.

(e) Prove $\#G = 8$.

(f) Prove that $g_1, \ldots, g_5$ is a maximal set of pairwise non-conjugate elements of G. In other words, G is the disjoint union $g_1^G \sqcup \cdots \sqcup g_5^G$. Give the character table of G.

(7.12)

(a) Let $M(m, \mathbb{C})$ denote the set of complex $m \times m$ matrices. For $x \in M(m, \mathbb{C})$ write $x^* = \bar{x}^t$: the transpose of the complex conjugate. Prove that $\langle \cdot, \cdot \rangle \colon M(m, \mathbb{C}) \times M(m, \mathbb{C}) \to \mathbb{C}$ defined by $\langle x, y \rangle = \operatorname{tr}(xy^*)$ is an inner product on $M(m, \mathbb{C})$.

(b) Let G be a finite group. Write $n = \#G$ and $G = \{g_1, \ldots, g_n\}$. A class function f on G is said to be positive semi-definite (PSD) if $f(g^{-1}) = \overline{f(g)}$ for all $g \in G$ and the Hermitian matrix

$$\left(g_i g_j^{-1}\right)_{i,j}$$

is PSD. Prove that every character of G is PSD.

(c) Let f be a PSD class function on G. Does it follow that f is of the form $a_1 \chi_1 + \cdots + a_k \chi_k$ where $a_i \in \mathbb{R}_{\geq 0}$ and the χ_i are characters of G?

(7.13) Let Q_8 be the subgroup of $\mathrm{GL}(2, \mathbb{C})$ generated by $i = \left(\begin{smallmatrix} i & 0 \\ 0 & i \end{smallmatrix}\right)$ and $j = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Calculate the character tables of Q_8 and D_8. Prove that Q_8 and D_8 are nonisomorphic groups with the same character table.

(7.14) In this exercise you prove that the set of characters of a finite group G is closed under multiplication. See chapter 10 for a more thorough treatment.

Let G be a finite group and let U, V be finite-dimensional $\mathbb{C}G$-modules. Let W be the set of mappings $f\colon U \times V \to \mathbb{C}$ such that

$$f(au + bv, x) = a\, f(u, x) + b\, f(v, x),$$
$$f(u, ax + by) = a\, f(u, x) + b\, f(u, y)$$

for all $u, v \in U,\ x, y \in V,\ a, b \in \mathbb{C}$ (the bilinear mappings).

(a) Prove that W becomes a vector space by the pointwise operations

$$(af + bg)(x, y) = a\, f(x, y) + b\, g(x, y)$$

whenever $a, b \in \mathbb{C},\ f, g \in W,\ x \in U,\ y \in V$.

(b) For $g \in G$ and $f \in W$ define $g^{-1}f\colon U \times V \to \mathbb{C}$ by $(g^{-1}f)(x, y) = f(gx, gy)$. Prove that this makes W into a $\mathbb{C}G$-module.

(c) Let $(u_1, \ldots, u_m)$ be a basis for U and $(v_1, \ldots, v_n)$ for V. For $1 \le i \le m$ and $1 \le j \le n$ define $w_{ij} \in W$ by

$$w_{ij}(v_k, v_\ell) = \delta_{ik}\, \delta_{j\ell} = \begin{cases} 1 & \text{if } (i, j) = (k, \ell), \\ 0 & \text{otherwise.} \end{cases}$$

Prove that the w_{ij} are well-defined and form a basis for W.

(d) Prove that $\bar{\chi}_W = \chi_U\, \chi_V$, that is, $\chi_W(g^{-1}) = \chi_U(g)\, \chi_V(g)$ for all $g \in G$. Deduce that the product of any two characters of G is again a character of G.

Hint: Use the notation of (b) and (c) and suppose that $gu_i = \alpha_i\, u_i$, $gv_j = \beta_j\, v_j$ for all i, j. Find $g^{-1}w_{ij}$.

(7.15) Let

$$G = \langle a, b \mid a^3 = 1,\ b^4 = 1,\ bab^{-1} = a^{-1} \rangle$$
$$D_6 = \langle r, s \mid r^3,\ s^2,\ (rs)^2 \rangle, \qquad C_4 = \langle c \mid c^4 \rangle.$$

(a) Prove that there exist unique homomorphisms

$$f\colon G \to D_6: \quad f(a) = r, \quad f(b) = s,$$
$$h\colon G \to C_4: \quad h(a) = 1, \quad h(b) = c.$$

(b) Prove $\#G = 12$ and $G = \{a^k\, b^\ell \mid 0 \le k \le 2 \text{ and } 0 \le \ell \le 3\}$. Hint: Prove that h is surjective and find the size of its kernel by using f.

(c) Let us call two elements of G **weakly conjugate** if their images in D_6 as well as in C_4 are conjugate. Find all weak conjugacy classes. Then prove that the weak conjugacy classes are the conjugacy classes.

(d) Calculate the character table for G. Justify your answers and show the intermediate steps in filling the character table.

Hints: You may wish to use proposition 127. Also, if $u\colon A \to B$ is a homomorphism of groups and χ a character of B then $\chi \circ u$ is clearly a character of A.

(e) (Not for credit). Use the character table and a result from the lectures to find all normal subgroups of G.

8 Induction and Restriction

8.1 Induction and restriction for characters

Let $H \leq G$ be finite groups. We define two maps called **induction and restriction**

$$\mathrm{CF}(H) \underset{\mathrm{Res}}{\overset{\mathrm{Ind}}{\rightleftarrows}} \mathrm{CF}(G)$$

as follows. Let $p \in \mathrm{CF}(G)$ and $q \in \mathrm{CF}(H)$. We define $q^\circ \colon G \to \mathbb{C}$ by

$$q^\circ(x) = \begin{cases} q(x) & \text{if } x \in H, \\ 0 & \text{if } x \notin H. \end{cases}$$

Then

$$\begin{aligned} \mathrm{Res}^G_H(p) &= \mathrm{Res}(p) = p_H, & p_H(h) &:= p(h), \\ \mathrm{Ind}^G_H(q) &= \mathrm{Ind}(q) = q^G, & q^G(g) &:= \frac{1}{\#H} \sum_{x \in G} q^\circ(tgt^{-1}). \end{aligned}$$

Sometimes a more flexible notation is convenient. For any assertion P write

$$[P] = \begin{cases} 1 & \text{if } P \text{ is true}, \\ 0 & \text{if } P \text{ is false}. \end{cases}$$

In this notation the definition of induced characters looks like

$$q^G(g) := \frac{1}{\#H} \sum_{x \in G} [xgx^{-1} \in H]\, q(xgx^{-1})$$

where we abuse notation by writing $[x \in A]\, f(x) := 0$ if $x \notin A$, even though this may cause $f(x)$ to be undefined.

Proposition 140. *The functions p_H and q^G are class functions.*

Proof. For p_H this is obvious. For all $g, s \in G$ we have

$$q^G(sgs^{-1}) = \frac{1}{\#H} \sum_{t \in G} q^\circ(tsgs^{-1}t^{-1}) = \frac{1}{\#H} \sum_{u \in G} q^\circ(ugu^{-1}) = q^G(g)$$

where we replaced ts by u. □

Proposition 141: Frobenius reciprocity. *Let $H \leq G$ be finite groups. Let $p \in \mathrm{CF}(G)$ and $q \in \mathrm{CF}(H)$. Then*

$$(p_H, q)_H = (p, q^G)_G.$$

Proof.

$$\begin{aligned}
(q^G, p)_G &= \frac{1}{\#G} \sum_{g\in G} q^G(g)\, \overline{p(g)} && \text{by definition of inner product}\\
&= \frac{1}{\#G\cdot\#H} \sum_{g,x\in G} q^\circ(xgx^{-1})\, \overline{p(g)} && \text{by definition of induction}\\
&= \frac{1}{\#G\cdot\#H} \sum_{g,x\in G} q^\circ(xgx^{-1})\, \overline{p(xgx^{-1})} && \text{because } p \text{ is a class function}\\
&= \frac{1}{\#G\cdot\#H} \sum_{h,x\in G} q^\circ(h)\, \overline{p(h)} && \text{on writing } h = xgx^{-1}\\
&= \frac{1}{\#G\cdot\#H} \sum_{x\in G}\sum_{h\in H} q(h)\, \overline{p(h)} && \text{because the other terms are 0}\\
&= \frac{1}{\#H} \sum_{h\in H} q(h)\, \overline{p(h)} = (q, p_H)_H.
\end{aligned}$$

□

Exercise (8.1) Let G be a finite group, $I(G)$ the set of irreducible characters of G and let $p \in \mathrm{CF}(G)$. Prove that p is a character if and only if $(p,q)_G \in \mathbb{Z}_{\geq 0}$ for all $q \in I(G)$.

Corollary 142. *Let $H \leq G$ be finite groups and suppose that q is a character of H. Then q^G is a character of G.*

Proof. Let p be an irreducible character of G. Then p_H is a character of H so $(p_H, q)_H$ is a nonnegative integer. By Frobenius reciprocity, $(p, q^G)_G$ is a nonnegative integer. The result follows by exercise 8.1. □

8.2 *How to compute an induced character in practice*

The following is clear.

Proposition 143. $p^G(1) = [G : H] \cdot p(1)$. □

Let C be a conjugacy class in a group G and $g \in C$. We sometimes write $p(C) := p(g)$ if p is a class function on G.

The following result aims to speed up the calculation of induced characters in practice.

Proposition/Definition 144. *Let $H \leq G$ be finite groups and $p \in \mathrm{CF}(H)$. Let C be a conjugacy class in G. Let $D_1, \ldots, D_k$ be the conjugacy classes of H that are contained in C. Then*

$$p^G(C) = \frac{[G:H]}{\#C} \sum_{i=1}^{k} \#D_i \cdot p(D_i).$$

If $k > 1$ we say that C **splits**.

Proof. Let $g \in C$. In exercise 8.3 you will prove that

$$\frac{\#\{x \in G \mid xgx^{-1} \in D_i\}}{\#G} = \frac{\#D_i}{\#C}.$$

It follows that

$$p^G(C) = p^G(g) = \frac{1}{\#H} \sum_{x\in G} p(xgx^{-1})[xgx^{-1} \in H]$$
$$= \frac{1}{\#H} \sum_{i=1}^{k} \sum_{x\in G} p(xgx^{-1})[xgx^{-1} \in D_i] = \frac{1}{\#H} \sum_{i=1}^{k} p(D_i) \sum_{x\in G} [xgx^{-1} \in D_i]$$
$$= \frac{1}{\#H} \sum_{i=1}^{k} p(D_i) \cdot \#G \cdot \frac{\#D_i}{\#C} = \frac{[G:H]}{\#C} \sum_{i=1}^{k} \#D_i \cdot p(D_i).$$ □

Example 145. As an illustration how to calculate induced characters, we now calculate those characters of S_3 induced from the irreducible characters of S_2 and A_3. Our method uses proposition 144 and what we call induction tables.

The character tables of S_2, A_3 are:

S_2	1	(12)
χ_1	1	1
χ_2	1	-1

A_3	1	(123)	(321)
χ_3	1	1	1
χ_4	1	ω	ω^2
χ_5	1	ω^2	ω

where $\omega = \exp(2\pi i/3)$. Moreover, representatives of conjugacy classes of S_3 are 1, (12), (123).

Let us first consider S_2. For each conjugacy class C of S_3 we do the following. Firstly, we give the pair $C : \#C$ separated by a colon (or rather, we give a representative instead of C). If $D_1, \dots, D_k$ are the conjugacy classes of S_2 contained in C, we list the pairs $D_i : \#D_i$ in the same column as $C : \#C$:

S_3	1 : 1	(12) : 3	(123) : 2
S_2	1 : 1	(12) : 1	

In this case, no conjugacy class splits. (This is even true for $S_k \leq S_n$.) It is now easy to extend the table with the values of the induced characters to get the so-called induction table:

S_3	1 : 1	(12) : 3	(123) : 2
S_2	1 : 1	(12) : 1	
$(\chi_1)^{S_3}$	3	1	0
$(\chi_2)^{S_3}$	3	-1	0

For example by proposition 144

$$(\chi_2)^{S_3}(1) = [S_3 : S_2] \cdot \tfrac{1}{1} \cdot \chi_2(1) = 3,$$
$$(\chi_2)^{S_3}((12)) = [S_3 : S_2] \cdot \tfrac{1}{3} \cdot \chi_2((12)) = -1.$$

In the case of A_3 things get a bit more complicated, because (123) and (321) are conjugate in S_3 but not in A_3. This is the only splitting occurring:

S_3	1 : 1	(12) : 3	(123) : 2
A_3	1 : 1		(123) : 1, (321) : 1
$(\chi_3)^{S_3}$	2	0	2
$(\chi_4)^{S_3}$	2	0	$\omega + \omega^2 = -1$

For example

$$(\chi_4)^{S_3}((123)) = [S_3 : A_3]\Big(\tfrac{1}{2}\chi_4((123)) + \tfrac{1}{2}\chi_4((321))\Big) = \omega + \omega^2 = -1.$$

Note that χ_4 and χ_5 induce the same character of S_3.

The characters induced by χ_4 and χ_5 are irreducible but those induced by χ_1, χ_2, χ_3 are not. □

Notation 146. For a group G, let 1_G denote the trivial linear character of G.

Example 147. In this example we find the character table for A_5 using induction. Write $G = A_5$, $H = A_4$, $x = (12345)$ and let K be the subgroup of A_5 generated by x.

(a) Let C be a conjugacy class in S_n. Prove that at most 2 conjugacy classes of A_n are contained in C.

(b) For each conjugacy class in A_4 or A_5, find its cardinality and give one element.

(c) Let λ be the linear character of H defined by

	1	(123)	(321)	(12)(34)
λ	1	ω	ω^2	1

Compute $(1_H)^G$ and λ^G.

(d) Prove that $\chi_4 := (1_H)^G - 1_G$ is a character of G.

(e) Prove that χ_4 and $\chi_5 := \lambda^G$ are irreducible.

(f) Find $(12345)^G \cap K$ and $(12354)^G \cap K$.

(g) Let $\varepsilon = \exp(2\pi i/5)$. Let μ be the linear character of K such that $\mu(x) = \varepsilon$. Calculate μ^G.

(h) Prove that $\chi_3 := \mu^G - \chi_5 - \chi_4$ is an irreducible character.

(i) Finish the character table of A_5.

Solution. (a). Suppose $a, b, c \in A_n$ are conjugate in S_n: $a^x = b$, $b^y = c$. Suppose that a, b are not conjugate in A_n and b, c are not. Then $x, y \in S_n \setminus A_n$ so $xy \in A_n$. Also $a^{xy} = (a^x)^y = b^y = c$ so a, c are conjugate in A_n.

(b). The answer is:

A_4:

1	(123)	(321)	(12)(34)
1	4	4	3

A_5:

1	(123)	(12)(34)	(12345)	(12354)
1	20	15	12	12

Most of these are easily found using (a) and our knowledge of the conjugacy classes in S_n. What remains to prove is that $(123), (132)$ are not conjugate in A_4 and that $x := (12345)$ and $y := (12354)$ are not conjugate in A_5.

Suppose that x, y are conjugate in A_5, say, $z \in A_5$ satisfies $yz = zx$. By multiplying z with a power of x we may suppose $z(1) = 1$. Then $z = (45)$ which is not in A_5.

For A_4 there is a similar argument and left to you.

(c). Note $[G : H] = 5$. Using the method of example 145 we get:

G	$1:1$	$(123):20$	$(12)(34):15$	$(12345):12$	$(12354):12$
H	$1:1$	$(123):4, (321):4$	$(12)(34):3$		
$(1_H)^G$	5	2	1	0	0
λ^G	5	-1	1	0	0

because $\omega + \omega^2 = -1$.

(d). By Frobenius reciprocity we have $((1_H)^G, 1_G)_G = (1_H, 1_H)_H = 1$. It follows that χ_4 is a character.

(e). By (c)

	1	(123)	(12)(34)	(12345)	(12354)
	1	20	15	12	12
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

and it readily follows that $\#G \cdot (\chi_4, \chi_4)_G = 1 \cdot 4^2 + 20 \cdot 1^2 + 12 \cdot (-1)^2 + 12 \cdot (-1)^2 = 16 + 20 + 12 + 12 = 60$, that is, $(\chi_4, \chi_4)_G = 1$. Therefore χ_4 is irreducible.

Likewise $\#G \cdot (\chi_5, \chi_5)_G = 1 \cdot 5^2 + 20 \cdot (-1)^2 + 15 \cdot 1^2 = 25 + 20 + 15 = 60$ so $(\chi_5, \chi_5)_G = 1$ whence χ_5 is irreducible.

(f). We claim

$$(12345)^G \cap K = \{x, x^4\}, \qquad (12354)^G \cap K = \{x^2, x^3\}.$$

Firstly,

$$(14)(23)x(14)(23) = (14)(23)(12345)(14)(23) = (54321) = x^4$$

so x is conjugate to x^4 and therefore x^2 is conjugate to $(x^4)^2 = x^3$. Moreover

$$x^2 = (13524) = (235)(12354)(235)^{-1}$$

and the claim is proved.

(g). Note $[G : K] = 12$. Using the method of example 145 we get the following.

G	$1:1$	$(123):20$	$(12)(34):15$	$(12345):12$	$(12354):12$
K	$1:1$			$x:1,\ x^4:1$	$x^2:1,\ x^3:1$
μ^G	12	0	0	$\varepsilon + \varepsilon^4$	$\varepsilon^2 + \varepsilon^3$

(h). This is equivalent to saying that $(\mu^G, \chi_4)_G$ and $(\mu^G, \chi_5)_G$ are nonzero and $(\chi_3, \chi_3)_G = 1$. These are straightforward calculations and left to you.

(i). For the same reason $\chi_2 := (\mu^2)^G - \chi_5 - \chi_4$ is an irreducible character. This involves no extra calculations: just observe that it amounts to replacing ε by ε^2 and that this doesn't affect what we did with χ_3.

Another short proof that χ_2 is an irreducible character is that it is $\chi_3 \circ \alpha$ where α is the automorphism of A_5 defined by $\alpha(x) = (45)x(45)$.

We get the following.

A_5	1	(123)	(12)(34)	(12345)	(12354)
χ_1	1	1	1	1	1
χ_2	3	0	-1	$1+\varepsilon^2+\varepsilon^3$	$1+\varepsilon+\varepsilon^4$
χ_3	3	0	-1	$1+\varepsilon+\varepsilon^4$	$1+\varepsilon^2+\varepsilon^3$
χ_4	4	1	0	-1	-1
χ_5	5	-1	1	0	0

As an aside, note $\varepsilon + \varepsilon^4 = \frac{-1+\sqrt{5}}{2}$. Note also that it follows immediately from the character table and theorem 133b that A_5 is simple. $\square$

8.3 Induction and restriction for modules

Definition 148. Let $H \leq G$ be finite groups. Let V be a finite-dimensional $\mathbb{C}H$-module with character p. We define the **induced module** V^G to be the $\mathbb{C}G$-module whose character is p^G.

Note that V^G is well-defined, but only up to isomorphism, for the following reasons. Firstly, p^G is a character as we proved in corollary 142. Secondly, any finite-dimensional $\mathbb{C}G$-module is determined up to isomorphism by its character. □

This is not a very satisfactory definition. There could be many reasons why you are interested in a module rather than its character. In some other theories, a module is not even determined by its character. We now ask how to recognise or construct V^G without reference to characters.

Definition 149. Let V be a $\mathbb{C}G$-module. An **imprimitivity decomposition** of V is a tuple $(W_1, \dots, W_k)$ of linear subspaces of V such that:

- Direct sum: $V = W_1 \oplus \cdots \oplus W_k$.
- Invariance: For all $g \in G$ and i there exists j with $gW_i = W_j$.
- Transitivity: For all i, j there exists $g \in G$ such that $gW_i = W_j$.

We call this a **proper** imprimitivity decomposition if $k > 1$. A nonzero $\mathbb{C}G$-module is said to be **primitive** if it admits no proper imprimitivity decompositions.

If $V = W_1 \oplus \cdots \oplus W_k$ is a proper imprimitivity decomposition then W_i is certainly not a submodule. However, if $H = \{g \in G \mid gW_1 = W_1\}$ (the so-called **stabiliser** $\mathrm{Stab}_G(W_1)$ of W_1) then W_1 is a $\mathbb{C}H$-module.

Proposition 150. *Let V be a finite-dimensional $\mathbb{C}G$-module with character q. Let $V = W_1 \oplus \cdots \oplus W_k$ be an imprimitivity decomposition. Put $H := \mathrm{Stab}_G(W_1)$ and let p be the character of W_1 over H. Then $q = p^G$.*

Proof. Let T be a **left transversal** for H in G, that is, $T \subset G$ and G is the disjoint union of tH as t runs through T. Then tW runs through the W_i as t runs through T so

$$V = \bigoplus_{t \in T} tW.$$

Choose a basis $\{w_1, \dots, w_m\}$ for W. Then $\{tw_i \mid t \in T,\ 1 \leq i \leq m\}$ is a basis for V. Let $g \in G$. We compute $q(g)$ using this basis.

For $t \in T$, the contribution of the basis vectors tw_i to $q(g)$ will be zero unless $gtW = tW$, that is, $t^{-1}gt \in H$. Assume now $t^{-1}gt = h \in H$ and write $hw_i = \sum_j a_{ij} w_j$. Then $p(t^{-1}gt) = \sum_i a_{ii}$.

Now

$$g(t\,w_i) = t(h\,w_i) = \sum_j a_{ij}\,t\,w_j$$

and therefore the contribution of tw_i to $q(g)$ is a_{ii}. Therefore the total contribution of the tw_i (for fixed t but varying i) is $p(t^{-1}gt)$. It follows that

$$q(g) = \sum_{t \in T} p^{\circ}(t^{-1}gt) \stackrel{*}{=} p^G(g)$$

where the starred equality is left to you (exercise 8.10). □

Proposition 151. *Let $H \subset G$ be finite groups and let W be a $\mathbb{C}H$-module. Then there exists a $\mathbb{C}G$-module V having an imprimitivity decomposition $V = W_1 \oplus \cdots \oplus W_k$ such that $H = \mathrm{Stab}_G(W_1)$ and $W \cong W_1$ as $\mathbb{C}H$-modules.*

Proof. (Not on the syllabus). Let T be a left transversal for H in G such that $1 \in T$. Let V be a vector space and for all $t \in T$ let $t \otimes W$ be subspaces of V such that $t \otimes W \cong W$ and $V = \bigoplus_{t \in T} t \otimes W$. We know that such V and $t \otimes W$ can be found. Let $a_t \colon W \to t \otimes W$ be an isomorphism. Write $t \otimes w$ instead of $a_t(w)$ whenever $w \in W$, $t \in T$. We then have $t \otimes W = \{t \otimes w \mid w \in W\}$.

For $g \in G$ and $w \in W$ define $g \otimes w$ as follows. Write $g = th$ and set $g \otimes w := t \otimes hw$. Note (exercise):

$$g \otimes xw = gx \otimes w \qquad \text{for all } g \in G,\, x \in H,\, w \in W.$$

The usual notation for what we have constructed is $V = \mathbb{C}G \otimes_{\mathbb{C}H} W$.

The action of G on V is defined as follows. Every element of V can uniquely be written $\sum_{t \in T} t \otimes w_t$ where $w_t \in W$. We put

$$g \sum_{t \in T} t \otimes w_t := \sum_{t \in T} (gt) \otimes w_t.$$

This makes V into a $\mathbb{C}G$-module. It is clear that $\{t \otimes W \mid t \in T\}$ is an imprimitivity decomposition of V. Also $H = \mathrm{Stab}_G(1 \otimes W)$ and $W \cong 1 \otimes W$ as $\mathbb{C}H$-modules (exercise). The proof is complete. $\square$

See exercise 8.13 for a different proof of proposition 151.

In the notation of proposition 151 we have $V \cong W^G$ by proposition 150, provided that V is finite-dimensional.

8.4 Exercises

(8.2) Let $H \le G$ be finite groups. Prove $((1_H)^G, 1_G)_G > 0$.

(8.3) Let $H \le G$ be finite groups. Let $C \subset G$ and $D \subset H$ be conjugacy classes such that $D \subset C$ and let $g \in C$. Prove that

$$\frac{\#\{x \in G \mid xgx^{-1} \in D\}}{\#G} = \frac{\#D}{\#C}.$$

(8.4) Let $H \subset G$ be finite groups. Let q be an irreducible character of H. Prove that there exists an irreducible character p of G such that $(p_H, q)_H > 0$.

(8.5) Let $H \subset G$ be finite groups. Let $p \in \mathrm{CF}(H)$ and $q \in \mathrm{CF}(G)$. Prove that $(p\, q_H)^G = p^G\, q$.

(8.6) Let $H, K, \le G$ be finite groups such that $G = HK := \{hk \mid h \in H,\ k \in K\}$. Let $p \in \mathrm{CF}(H)$. Prove $(p^G)_K = (p_{H \cap K})^K$.

(8.7) Let $H, K \le G$ be finite group. Let $T \subset G$ be a subset such that G is the disjoint union of the HtK where t ranges over T. Let $p \in \mathrm{CF}(H)$ and, for all $t \in T$, define $p^t \in \mathrm{CF}(t^{-1}Ht)$ by $p^t(x) = p(txt^{-1})$. Prove **Mackey's theorem**

$$(p^G)_K = \sum_{t \in T} ((p^t)_{t^{-1}Ht \cap K})^K.$$

Note: this generalizes exercise 8.6.

(8.8) Let $H \le G$ be finite groups and p a character of H. Let $K \le G$ and assume that $(p^G)_K$ is an irreducible character of K. Prove that $HK = G$.

Hint: use Mackey's theorem.

(8.9) Let H be a normal subgroup of a finite group G and $p \in \mathrm{CF}(H)$. Let C be a conjugacy class of G. Let $D_1, \ldots, D_k$ be the conjugacy classes of H that are contained in C and assume $k > 0$. Prove that

$$p^G(C) = \frac{[G:H]}{k} \sum_{i=1}^{k} p(D_i).$$

(8.10) Prove the last equality sign in the proof of proposition 150.

(8.11) Fill the gaps in the proof of proposition 151.

(8.12) Give an example of a nontrivial group G and a character q of G such that there is no subgroup $H < G$ and a character p of H with $q = p^G$.

(8.13) The proof of proposition 151 is somewhat disappointing in that it depends on the choice of a transversal T. Here is a construction that doesn't depend on such a choice.

Put

$$V = \{u \colon G \to W \mid u(xy) = x(uy) \quad \text{for all } x \in H,\ y \in G\}.$$

(a) Prove that this is a vector space under the pointwise operations $(au + bv)(x) := a \cdot u(x) + b \cdot v(x)$ ($a, b \in \mathbb{C}$, $u, v \in V^G$, $x \in G$).

(b) Prove that V is a $\mathbb{C}G$-module by putting

$$\begin{aligned} G \times V &\longrightarrow V \\ (g, u) &\longmapsto gu, \quad (gu)(x) := u(xg) \quad \text{for all } x \in G. \end{aligned}$$

(c) Let $H\backslash G = \{H_i \mid 1 \le i \le m\}$ be the cosets and assume $H_1 = H$. Let $W_i := \{u \in V \mid u(H_j) = \{0\} \text{ whenever } i \neq j\}$. Prove that $(W_1, \ldots, W_m)$ is an imprimitivity decomposition of V.

(d) Prove that $H = \mathrm{Stab}_G(W_1)$ and $W \cong W_1$ as $\mathbb{C}H$-modules.

(8.14) Let G be a finite group and V a $\mathbb{C}G$-module. Let $A \subset V$ be a G-invariant basis (that is, $gx \in A$ for all $g \in G$, $x \in A$). Let $a \in A$ and consider the subgroup $H = \{h \in G \mid ha = a\}$. Prove that the character of V is $(1_H)^G$.

(8.15) We define the group $G = \langle a, b \mid a^3, b^7, a\,b\,a^{-1}\,b^{-2} \rangle$.

(a) Prove that there exists a unique homomorphism $f \colon G \to C_3 := \langle c \mid c^3 \rangle$ such that $f(a) = c$, $f(b) = 1$.

(b) Prove that every element of G can uniquely be written in the form $a^k\, b^\ell$ with $0 \le k < 3$ and $0 \le \ell < 7$.

(c) Put

$$D_1 = \{1\}, \qquad D_2 = \{b, b^2, b^4\}, \qquad D_3 = \{b^3, b^5, b^6\},$$
$$D_4 = \{a\,b^\ell \mid \ell \in \mathbb{Z}\}, \qquad D_5 = \{a^2\, b^\ell \mid \ell \in \mathbb{Z}\}.$$

Prove that $D_1, \ldots, D_5$ are the conjugacy classes of G.

(d) Find three distinct linear characters χ_1, χ_2, χ_3 of G explicitly.

(e) Write $H = \langle b \rangle \le G$ and $\varepsilon = \exp(2\pi i/7)$. Let λ, μ be the linear characters of H defined by $\lambda(b^\ell) = \varepsilon^\ell$ and $\mu(b^\ell) = \varepsilon^{3\ell}$ for all ℓ. Calculate the induced characters $\chi_4 := \lambda^G$ and $\chi_5 := \mu^G$. These should be expressed in terms of ε.

(f) Prove that χ_4 and χ_5 are irreducible.

(g) Prove that χ_4 and χ_5 are distinct and finish the character table.

(h) Use the character table to find all normal subgroups of G.

(8.16) Let $H \le K \le G$ be finite groups and p a class function on H. Prove $(p^K)^G = p^G$.

(8.17) Let $H \le G$ be finite groups and p a nonzero character of H. Prove that

$$\ker(p^G) = \bigcap_{x \in G} x^{-1}(\ker p)x.$$

Where does your proof break down if $p = 0$?

(8.18) In this exercise you will compute the character table for $G := S_5$ by induction from A_5 and S_4. Recall the **permutation character** χ^p which is the character of the representation $\rho^p \colon S_n \to \mathrm{GL}(n, \mathbb{C})$ defined by $(\rho^p s)e_i = e_{si}$ for all $s \in S_n$.

(a) For each conjugacy class in S_5, find its cardinality and give one element.

(b) Find two linear characters χ_1, χ_2 of S_5 where χ_1 is trivial.

(c) Compute $\chi_3 := \chi^p - \chi_1$ and $\chi_4 := \chi_3\chi_2$ and prove that they are irreducible characters.

(d) Choose an irreducible character ϕ of A_5 of degree 3. Compute $\chi_5 := \phi^G$ and prove that it is irreducible.

(e) Let μ be the following irreducible character of S_4:

	1	(12)	(12)(34)	(123)	(1234)
μ	3	−1	−1	0	1

Compute $\chi_6 := \mu^G - \chi_5 - \chi_4$ and prove that it is an irreducible character.

(f) Finish the character table.

9 Algebraic integers and Burnside's $p^a q^b$ theorem

9.1 Introduction

It is easy to show that the only abelian finite simple groups are the cyclic groups of prime order. Also, if the order of a finite simple group G is p^a where p is a prime number, then $\#G = p$. See exercises 9.2 and 9.4.

In 1904 Burnside proved that the order of a finite simple group cannot be of the form $p^a q^b$ where p, q are distinct prime numbers and $a, b > 0$. It is remarkable that his proof made use of character theory though the statement doesn't mention them. Later on people found different proofs of Burnside's theorem not using character theory but they are much harder.

We begin by summarizing the necessary background on algebraic integers without proof. Then we give Burnside's proof.

9.2 Algebraic integers

Definition/Lemma 152.

(a) A polynomial $f = \sum_{k=0}^{n} a_k x^k$ ($a_n \neq 0$) is said to be **monic** if $a_n = 1$.

(b) A complex number is said to be an **algebraic number** if it is a root of a nonzero polynomial in $\mathbb{Q}[x]$. The set of algebraic numbers is written $\overline{\mathbb{Q}}$.

(c) A complex number is said to be an **algebraic integer** if it is a root of a monic polynomial in $\mathbb{Z}[x]$. The set of algebraic integers is written $\mathbb{I}$.

(d) **Lemma**. Let $\alpha \in \overline{\mathbb{Q}}$. Then there exists a unique monic polynomial $f \in \mathbb{Q}[x]$ of minimal degree such that $f(\alpha) = 0$. We call f the **minimal polynomial** of α (over $\mathbb{Q}$).

(e) Two algebraic numbers are said to be **(algebraically) conjugate** (over $\mathbb{Q}$) if they have the same minimal polynomial. □

Example 153. Let $T \in M(n, \mathbb{Z})$. Then every complex eigenvalue of T is in $\mathbb{I}$ because it is a root of $\det(x\, I_n - T)$ which is a monic polynomial in $\mathbb{Z}[x]$.

The following theorem collects the results about algebraic integers used in the proof of Burnside's theorem. We shall use these results without proving them. The proofs belong to algebraic number theory or Galois theory.

Theorem 154.

(a) *$\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.*

(b) *$\mathbb{I}$ is a subring of $\mathbb{C}$.*

(c) $\mathbb{I} \cap \mathbb{Q} = \mathbb{Z}$.

(d) *Let $\alpha \in \overline{\mathbb{Q}}$ and $f \in \mathbb{Q}[x]$ be such that $f(\alpha) = 0$. Then the minimal polynomial of α divides f in $\mathbb{Q}[x]$.*

(e) *Let f be the minimal polynomial of an algebraic number α. Let $\beta \in \mathbb{C}$ also be a root of f. Then α and β are conjugate.*

(f) *The minimal polynomial of an algebraic integer is in $\mathbb{Z}[x]$.*

(g) *Let $\alpha, \beta \in \overline{\mathbb{Q}}$. Then every conjugate to $\alpha + \beta$ is of the form $\alpha' + \beta'$ for some conjugate α' to α and some conjugate β' to β. Same for multiplication instead of addition.* □

Example 155. (a). Every complex root of unity ω is an algebraic integer. Indeed, write $\omega^n = 1$ where $n > 0$. Then ω is a root of the monic polynomial $f = x^n - 1 \in \mathbb{Z}[x]$.

(b). Using the foregoing notation, let ε be a conjugate to ω. We shall prove that then ε is again a root of unity. Let g be the minimal polynomial of ω. By theorem 154(d) $g \mid f$ in $\mathbb{Q}[x]$. But g is also the minimal polynomial of ε. So $f(\varepsilon) = 0$ and $\varepsilon \in \mathbb{I}$.

(c). The following converse to (b) holds. Let α, β be complex roots of unity. Then α, β are conjugate if and only if each generates the same multiplicative group: $\langle\alpha\rangle = \langle\beta\rangle$. We shall not prove or use this.

Exercise (9.1) Find $\alpha, \alpha', \beta, \beta' \in \overline{\mathbb{Q}}$ such that α, α' are conjugate and β, β' are conjugate but $\alpha + \beta$ is not conjugate to $\alpha' + \beta'$. So the converse to theorem 154(g) is false.

9.3 Burnside's theorem

Lemma 156. *Let χ be a character of a finite group G and $g \in G$.*

(a) $\chi(g) \in \mathbb{I}$.

(b) *If χ is irreducible then* $\dfrac{\chi(g)}{\chi(1)} \#g^G \in \mathbb{I}$.

Proof. (a). By lemma 103 there are roots of unity $\omega_1, \ldots, \omega_k$ such that $\chi(g) =$

$\omega_1 + \cdots + \omega_k$. We have seen that $\omega_i \in \mathbb{I}$. Also $\mathbb{I}$ is a ring by theorem 154(b) so $\chi(g) \in \mathbb{I}$.

(b). Write $\chi = \chi_\rho$, $\deg \chi = n$. For any representation σ of G, write

$$T(\sigma) = \sum_{h \in g^G} \sigma(h)$$

and put $T = T(\rho)$. Then T is an intertwiner from ρ to itself because for all $x \in G$

$$\rho(x)\,T = \rho(x) \sum_{h \in g^G} \rho(h) = \sum_{h \in g^G} \rho(xh) = \sum_{f \in g^G} \rho(fx) = \Big(\sum_{f \in g^G} \rho(f)\Big)\rho(x) = T\,\rho(x).$$

Since ρ is irreducible, Schur's lemma implies $T = \alpha \cdot I_n$ for some $\alpha \in \mathbb{C}$, where I_n is the $n \times n$ identity matrix. Also

$$n\,\alpha = \operatorname{tr} \alpha \cdot I_n = \operatorname{tr} T = \operatorname{tr} \sum_{h \in g^G} \rho(h) = \#g^G\,\chi(g)$$

so

$$\alpha = \frac{\chi(g)}{\chi(1)}\,\#g^G.$$

It remains to prove that $\alpha \in \mathbb{I}$. But $\rho^{\text{reg}} \sim \rho \oplus \sigma$ for some representation σ and α is an eigenvalue of $T(\rho)$ hence of $T(\rho^{\text{reg}})$. Now $T(\rho^{\text{reg}})$ is in $M(m, \mathbb{Z})$ where $m = \#G$ so its eigenvalues, including α, are in $\mathbb{I}$ by example 153. $\square$

As a diversion we present the following theorem which will not be used in the proof of Burnside's theorem.

Theorem 157. *Let χ be an irreducible character of a finite group G. Then $\chi(1)$ divides $\#G$.*

Proof. Let $C_1, \ldots, C_k$ be the conjugacy classes of G. By row orthogonality (theorem 128) we have

$$\sum_{j=1}^{k} \#C_j\,\chi(C_j)\,\overline{\chi}(C_j) = \#G.$$

It follows that

$$\sum_{j=1}^{k} \Big(\#C_j\,\frac{\chi(C_j)}{\chi(1)}\Big)\,\overline{\chi}(C_j) = \frac{\#G}{\chi(1)}.$$

The left hand side is in $\mathbb{I}$ by lemma 156 and because $\mathbb{I}$ is a ring. Therefore the right hand side is in $\mathbb{I} \cap \mathbb{Q}$, which is $\mathbb{Z}$. $\square$

We return to the proof of Burnside's theorem.

Proposition 158. *Let ρ be an irreducible representation of G of degree n and let $g \in G$. If $\gcd(n, \#g^G) = 1$ then $\chi_\rho(g) = 0$ or $\rho(g)$ is a scalar matrix.*

Proof. Write $\lambda = \frac{1}{n}\chi_\rho(g)$. There are $a, b \in \mathbb{Z}$ such that $an + b\#g^G = 1$. Multiplying with λ we get

$$a\,\chi_\rho(g) + b\,\frac{\chi_\rho(g)}{n}\,\#g^G = \frac{\chi_\rho(g)}{n} = \lambda.$$

The left hand side is in $\mathbb{I}$ by lemma 156. Therefore $\lambda \in \mathbb{I}$.

Let $\omega_1, \ldots, \omega_n$ be the eigenvalues of $\rho(g)$. Then $\lambda = \frac{1}{n}(\omega_1 + \cdots + \omega_n)$. Also the ω_i are roots of unity so they lie on the unit circle and $0 \le |\lambda| \le 1$.

Case 1: $\boldsymbol{\lambda = 0}$. Then there is nothing to prove.

Case 2: $|\lambda| = 1$. Then the ω_i are all equal and $\rho(g)$ is a scalar matrix as required.

Case 3: $0 < |\lambda| < 1$. We shall deduce a contradiction from this. Let f be the minimal polynomial of λ: $f = \prod_{i=1}^{k}(x - \lambda_i) \in \mathbb{Z}[x]$, say $\lambda = \lambda_1$. Then $f \in \mathbb{Z}[x]$ by theorem 154(f) and because λ is an algebraic integer. It follows that $\lambda_1 \cdots \lambda_k = (-1)^k f(0) \in \mathbb{Z}$.

Let $1 \leq i \leq k$. Then λ_i is a conjugate to λ by theorem 154(e). By theorem 154(g) λ_i is of the form $\frac{1}{n}(\varepsilon_1 + \cdots + \varepsilon_n)$ where ε_i is a conjugate to ω_i. But a conjugate to a root of unity is again a root of unity (example 155) so $0 < |\lambda_i| \leq 1$ as before.

Taking the product over all i and using the fact that $|\lambda_1| < 1$ we find $0 < |\lambda_1 \cdots \lambda_k| < 1$, which is the promised contradiction. □

Proposition 159. *Let p be a prime number and $r \in \mathbb{Z}_{>0}$. Then there doesn't exist a nonabelian finite simple group with a conjugacy class of size p^r.*

Proof. Let G be a nonabelian finite simple group and let $g \in G$ be such that $\#g^G = p^r$. Note that $g \neq 1$.

Let $\chi_1, \ldots, \chi_k$ be the irreducible characters of G with χ_1 trivial. Suppose χ_i is the character of a representation ρ_i. Since G is simple, ρ_i is injective unless $i = 1$.

We claim that if $i \neq 1$ then $\rho_i(g)$ is not a scalar matrix. Indeed if it is then the group $\mathrm{im}(\rho_i)$ contains a nontrivial central element $\rho_i(g)$, contradicting the fact that $\mathrm{im}(\rho_i)$ is isomorphic to G and hence simple.

By proposition 158, if $i \neq 1$ and p does not divide $\deg \rho_i$ then $\chi_i(g) = 0$.

Consider now orthogonality of columns g and 1:

$$0 = \sum_{i=1}^{k} \chi_i(g) \deg \rho_i = 1 + \sum_{\substack{i \neq 1 \\ p \mid \deg \rho_i}} \chi_i(g) \deg \rho_i.$$

It follows that

$$\sum_{\substack{i \neq 1 \\ p \mid \deg \rho_i}} \chi_i(g) \frac{\deg \rho_i}{p} = \frac{-1}{p}.$$

But $\chi_i(g) \in \mathbb{I}$ by lemma 156 so the left hand side is in $\mathbb{I}$. Therefore $\frac{-1}{p}$ is in $\mathbb{I} \cap \mathbb{Q}$ which is $\mathbb{Z}$. This contradiction finishes the proof. □

Theorem 160: Burnside's $p^a q^b$ theorem. *Let p, q be distinct prime numbers and $a, b \in \mathbb{Z}_{\geq 0}$. Then there doesn't exist a nonabelian simple group of order $p^a q^b$.*

Proof. Let G be a nonabelian simple group of order $p^a q^b$. We have $Z(G) \trianglelefteq G$. As G is simple we must have $Z(G) = 1$ or $Z(G) = G$. As G is nonabelian $Z(G) = 1$. Therefore there is exactly one conjugacy class of size 1, namely $\{1\}$.

Let $C_1, \ldots, C_k$ be the conjugacy classes of G with $C_1 = \{1\}$. Note that $\#C_i$ divides $\#G$ (exercise 9.3). Therefore $pq \mid \#C_i$ if $i \neq 1$ by proposition 159. After interchanging p and q if necessary we have $p \mid \#G$ so

$$p \mid \#G - \Big(\sum_{i=2}^{k} \#C_i \Big) = 1.$$

This is a contradiction and finishes the proof. □

9.4 *Exercises*

(9.2) Let G be an abelian finite group. Prove that G is simple if and only if $\#G$ is a prime number.

(9.3) Let C be a conjugacy class in a finite group G. Prove that $\#C$ divides $\#G$.

(9.4) Let G be a simple group whose order is a power of a prime number. Without using the results of this chapter, prove that G is abelian. Hint: use exercise 9.3.

(9.5) Let χ be an irreducible character of a finite group G. Use the results of exercise 5.17 to give another proof that $\deg \chi$ divides $\#G$.

(9.6) Give another proof of part (b) of lemma 156(b) (stating that if χ is an irreducible character of a finite group G and $g \in G$ then $\chi(1)^{-1}\chi(g)\#g^G \in \mathbb{I}$) by using the Frobenius formula proved in exercise 6.3.

10 Tensor products

10.1 The universal property for tensor products

Definition 161. Let U, V, W be vector spaces (over $\mathbb{C}$). A map $r\colon U \times V \to W$ is said to be **bilinear** if

$$r(au + bv, x) = a\, r(u, x) + b\, r(v, x),$$
$$r(u, ax + by) = a\, r(u, x) + b\, r(u, y)$$

for all $u, v \in U$, $x, y \in V$, $a, b \in \mathbb{C}$. In words, $r(x, y)$ is linear in x if y is fixed and it is linear in y if x is fixed.

Exercise (10.1)

(a) Let $m, n \geq 0$. Let $a_{ij} \in \mathbb{C}$ for all $(i, j) \in \{1, \ldots, m\} \times \{1, \ldots, n\}$ and define $r\colon \mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}$ by

$$r(\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}\, x_i\, y_j.$$

Prove that r is bilinear.

(b) Prove that, conversely, every bilinear map $\mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}$ is of this form.

(c) What about bilinear maps $\mathbb{C}^m \times \mathbb{C}^n \to \mathbb{C}^k$?

Exercise (10.2) Let U_1, U_2, V_1, V_2, W, X be vector spaces. Let

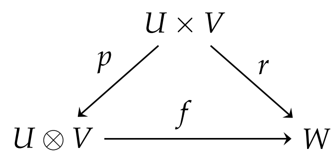
$$f\colon U_1 \to U_2, \quad g\colon V_1 \to V_2, \quad h\colon W \to X$$

be linear maps and $r_2\colon U_2 \times V_2 \to W$ bilinear. Prove that the map

$$r_1\colon U_1 \times V_1 \to X\colon \quad r_1(x, y) = h(r_2(fx, gy))$$

is also bilinear.

Definition 162: Tensor product. Let U, V be vector spaces. A **tensor product** of U, V is a vector space $U \otimes V$ together with a bilinear map $p\colon U \times V \to U \otimes V$ with the following property, the **universal property**. Let W be a vector space and $r\colon U \times V \to W$ a bilinear map. Then there exists a unique linear map $f\colon U \otimes V \to W$ such that $r = f \circ p$.



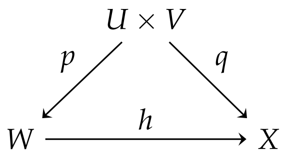
We write $u \otimes v$ instead of $p(u, v)$. □

The notation $u \otimes v$ is almost always preferred over $p(u,v)$. The expressions $u \otimes v$ are sometimes called pure tensors.

We often say "$U \otimes V$ is a tensor product of U and V" though we should really say "$(U \otimes V, p)$ is a tensor product of U and V". The map p is part of it. It doesn't do too much harm not to mention p because we have the notation $u \otimes v$ for $p(u,v)$. Sometimes we call p the **natural map**.

In the above definition we have to write *a tensor product* rather than *the tensor product* because it is not unique: one can always replace it by an isomorphic copy. But it is unique in the sense of the following theorem.

Theorem 163. *Let U, V be vector spaces. Then there exists a tensor product $p\colon U \times V \to U \otimes V$. Moreover it is unique in the following sense. Let $p\colon U \times V \to W$ and $q\colon U \times V \to X$ be tensor products. Then there exists a unique bijective linear map $h\colon W \to X$ such that $q = h \circ p$.*



Proof. See section 10.2. □

Remark 164. The most general kind of tensor products (outside our scope) are as follows. Let R be an associative ring with centre S. Let U be a right R-module and V a left R-module. A tensor product is then an S-module $U \otimes_R V$ together with an S-bilinear map $p\colon U \times V \to U \otimes_R V$ such that $p(ua, v) = p(u, av)$ for all $(u,v) \in U \times V$, $a \in R$ and satisfying the following universal property.

Let W be an S-module and $r\colon U \times V \to W$ an S-bilinear map such that $r(ua, v) = r(u, av)$ for all $(u,v) \in U \times V$, $a \in R$. Then there exists a unique S-linear map $f\colon U \otimes_R V \to W$ such that $r = f \circ p$. □

Understanding tensor products means knowing how to use theorem 163 and the universal property rather than how to prove theorem 163. So before we prove it we look at many examples.

Example 165. Let U, V be vector spaces and fix a tensor product $U \otimes V$. Let $f\colon U \to \mathbb{C}$ and $g\colon V \to \mathbb{C}$ be linear maps. Prove that there exists a unique linear map $h\colon U \otimes V \to \mathbb{C}$ such that $h(u \otimes v) = f(u)\, g(v)$ for all $(u,v) \in U \times V$.

Solution. Consider the map $r\colon U \times V \to \mathbb{C}$ defined by $r(u,v) = f(u)\, g(v)$.

We claim that r is bilinear. Let $x, y \in U$, $v \in V$ and $a, b \in K$. Then

$$\begin{aligned} r(ax + by, v) = f(ax+by)\, g(v) &= \big(a\, f(x) + b\, f(y)\big)\, g(v) \\ &= a\, f(x)\, g(v) + b\, f(y)\, g(v) = a\, r(x,v) + b\, r(y,v). \end{aligned}$$

Likewise $r(u,v)$ is linear in v if u is fixed. This proves our claim that r is bilinear.

Let $p\colon U \times V \to U \otimes V$ be the natural map, $p(u,v) = u \otimes v$. By the definition of tensor product (the universal property) there exists a unique linear map $h\colon U \otimes V \to \mathbb{C}$ such that $r = h \circ p$. The latter means precisely $f(u)\, g(v) = h(u \otimes v)$ for all $(u,v) \in U \times V$. This finishes the proof. □

Example 166. Let U, V be vector spaces. Let $f\colon U \to U$ and $g\colon V \to V$ be linear maps. Prove that there exists a unique linear map $h\colon U \otimes V \to U \otimes V$ such that $h(u \otimes v) = f(u) \otimes g(v)$ for all $(u,v) \in U \times V$. Notation: $h = f \otimes g$.

Note that in the above example we don't bother saying "let $U \otimes V$ be a tensor product for U, V". This is a bit sloppy but very common. It doesn't do too much harm because the tensor product is unique in the sense of theorem 163.

It is proved below in the proof of theorem 163 that there is a "natural" way of picking a tensor product for all pairs of vector spaces (U, V) (all other tensor products are only isomorphic to it) but it is convenient to ignore this. In any case, we can't do without the universal property.

Solution. Let $p\colon U \times V \to U \otimes V$ be the natural map. Consider $r\colon U \times V \to U \otimes V\colon r(u,v) = f(u) \otimes g(v) = p(f(u), g(v))$.

Prove yourself that r is bilinear (use that p is bilinear). By the universal property of tensor products, there is a unique linear map $h\colon U \otimes V \to U \otimes V$ such that $r = h \circ p$. The latter means precisely that $h(u \otimes v) = f(u) \otimes g(v)$ for all $u \in U$, $v \in V$ and the proof is finished. □

Example 167. Let U, V be vector spaces. Prove that $U \otimes V$ is spanned by $\{u \otimes v \mid (u,v) \in U \times V\}$.

This is in fact already proved in the proof of theorem 163 but we'd like to prove it here directly from the universal property.

Solution. Let $p\colon U \times V \to U \otimes V$ be the natural map. Let K be the span of the image of p. Choose a subspace $L \subset U \otimes V$ such that $U \otimes V = K \oplus L$. We must prove $L = 0$.

Let $r\colon U \times V \to L$ be the zero map; it is certainly bilinear. Let $f_1\colon U \otimes V = K \oplus L \to L$ be the projection on L, that is, $f_1(k, \ell) = \ell$ for all $(k, \ell) \in K \times L$. Let $f_2\colon U \otimes V \to L$ be the zero map.

Then f_i is a linear map satisfying $r = f_i \circ p$, for all i. But the universal property says that such maps are unique. Therefore $f_1 = f_2$, that is, $L = 0$. This finishes the proof. □

Example 168. Let G be a group and let U, V be $\mathbb{C}G$-modules. Prove that there exists a unique way to make $U \otimes V$ into a $\mathbb{C}G$-module such that

$$g(u \otimes v) = g(u) \otimes g(v) \quad \text{for all } (u,v) \in U \times V. \tag{169}$$

Solution. From example 166 it follows immediately that for every $g \in G$ there exists a unique linear map $L_g\colon U \otimes V \to U \otimes V$ such that

$$L_g(u \otimes v) = g(u) \otimes g(v) \quad \text{for all } (u,v) \in U \times V.$$

It is trivial that $L_1 = \text{id}$. The result will follow once we can prove

$$L_{gh} = L_g L_h \quad \text{for all } g, h \in G \tag{170}$$

because it implies that $U \otimes V$ becomes a $\mathbb{C}G$-module by putting $gx := L_g(x)$ for all $g \in G$, $x \in U \otimes V$.

In order to prove (170), let $g, h \in G$. For all $(u,v) \in U \times V$ we have

$$L_{gh}(u \otimes v) = (gh)u \otimes (gh)v = g(hu) \otimes g(hv) = L_g(hu \otimes hv) = L_g L_h(u \otimes v).$$

This proves $L_{gh}(x) = L_g L_h(x)$ if x is a pure tensor $u \otimes v$. But $U \otimes V$ is spanned by the pure tensors by example 167 and L_g, L_h are linear. This proves (170). □

Exercise (10.3) If U, V are vector spaces, let $\text{Hom}(U, V)$ denote the set of linear maps $U \to V$. This is a vector space by the pointwise operations $(af + bg)(x) = a\,f(x) + b\,g(x)$ ($a, b \in \mathbb{C}$, $x \in U$, $f, g \in \text{Hom}(U, V)$.

Let U, V, W be vector spaces. Prove that there exists a unique linear map

$$\mathrm{Hom}(V,W) \otimes \mathrm{Hom}(U,V) \to \mathrm{Hom}(U,W)$$

taking $S \otimes T$ to $S \circ T$ for all $(S,T) \in \mathrm{Hom}(V,W) \times \mathrm{Hom}(U,V)$.

10.2 Existence and uniqueness for tensor products

We now prove theorem 163.

Unicity of the tensor product. Note that $p\colon U \times V \to W$ and $q\colon U \times V \to X$ are bilinear. We apply the universal property to the tensor product $p\colon U \times V \to W$ together with the bilinear map $q\colon U \times V \to X$. It says that there exists a unique linear map $h\colon W \to X$ such that $q = h \circ p$.

Note that we're not done yet proving unicity. We must still prove that h is bijective.

By reversing the roles of p, q we find that there exists a unique linear map $g\colon X \to W$ such that $p = g \circ q$. It follows that $g \circ h\colon W \to W$ is a linear map such that $p = g \circ h \circ p$.

Now apply the universal property to the tensor product $p\colon U \times V \to W$ and the bilinear map $p\colon U \times V \to W$. It states that there exists a *unique* linear map $\ell\colon U \otimes V \to W$ such that $p = \ell \circ p$. But we know two such maps ℓ, namely $g \circ h$ and identity. It follows that $g \circ h$ is identity.

A similar argument shows that $h \circ g$ is also identity. Therefore h is bijective. This proves unicity.

Existence of the tensor product. Let E be a vector space with basis $U \times V$. Let F be the subspace of E spanned by

$$\begin{aligned}&\big\{(au+bv,x) - a(u,x) - b(v,x) \;\big|\; a,b \in \mathbb{C},\ u,v \in U,\ x \in V\big\}\\ \cup\, &\big\{(u,ax+by) - a(u,x) - b(u,y) \;\big|\; a,b \in \mathbb{C},\ u \in U,\ x,y \in V\big\}.\end{aligned}$$

Put $U \otimes V := E/F$. The natural map $E \to E/F$ will be written $e \mapsto e + F$ or $e \mapsto h(e)$. Define $p\colon U \times V \to U \otimes V$ by

$$p(u,v) = (u,v) + F = h(u,v) \quad \text{for all } (u,v) \in U \times V.$$

Recall that $u \otimes v$ is another notation for $p(u,v)$.

First we prove that p is bilinear. Let $a, b \in \mathbb{C}$, $u, v \in U$, $x \in V$. Then

$$\begin{aligned}&p(au+bv,x) - a\,p(u,x) - b\,p(v,x)\\ &= h(au+bv,x) - a\,h(u,x) - b\,h(v,x)\\ &= h\big((au+bv,x) - a(u,x) - b(v,x)\big) = 0.\end{aligned}$$

Likewise $p(u,v)$ is linear in u if v is fixed. This proves that p is bilinear.

It remains to prove the universal property. Let W be a vector space and $r\colon U \times V \to W$ bilinear. We need to prove that there exists a unique linear map $f\colon U \otimes V \to W$ such that $r = f \circ p$.

Unicity of f. Note that E is spanned by $U \times V$. Therefore E/F (that is, $U \otimes V$) is spanned by the image of the natural map $U \times V \to E/F$ which is $\{u \otimes v \mid (u,v) \in U \times V\}$. There is only one choice for the values of f on this spanning set because for all $(u,v) \in U \times V$ we have $f(u \otimes v) = (f \circ p)(u,v) = r(u,v)$. This proves unicity of f.

Existence of f. Note that $U \times V$ is a basis for E. Therefore there is a linear map $g\colon E \to W$ such that $g(u,v) = r(u,v)$ for all $(u,v) \in U \times V$.

We claim

$$F \subset \ker g. \tag{171}$$

Let $a, b \in \mathbb{C}$, $u, v \in U$, $x \in V$. Then

$$g\big((au + bv, x) - a(u, x) - b(v, x)\big) = r(au + bv, x) - a\,r(u, x) - b\,r(v, x) = 0.$$

Likewise for the second kind of generators of F. This proves (171).

From (171) it follows that there exists a linear map $f\colon E/F \to W$ such that $f(e + F) = g(e)$ for all $e \in E$. In particular, for $e = (u, v)$, this means $f(u \otimes v) = g(u, v)$. In order to prove that this is the map f we're looking for, it suffices to observe that $r = f \circ p$ because for all $(u, v) \in U \times V$

$$r(u, v) = g(u, v) = f(u \otimes v) = (f \circ p)(u, v). \qquad \square$$

10.3 Bases and tensor products

The bases for vector spaces used in this section are unordered and indexed; this means the following.

Let V be a (possibly infinite-dimensional) vector space. An indexed family $(v_i \mid i \in I)$ of vectors in V is said to be an (unordered, indexed) **basis** of V if for every element v of V there are unique $a_i \in \mathbb{C}$ $(i \in I)$, only finitely many being nonzero, such that $v = \sum_i a_i v_i$.

The notation $(v_i \mid i \in I)$ knows by definition how often a vector appears in the family. But a basis cannot contain the same vector more than once. Therefore, if we are told that $(v_i \mid i \in I)$ is a basis we may conclude that $v_i \neq v_j$ whenever $i \neq j$. This is false if we are only given that the set $\{v_i \mid i \in I\}$ is a basis, which explains why we use the notation $(v_i \mid i \in I)$.

Incidentally, unordered indexed bases are quite convenient for infinite-dimensional vector spaces. It is known that every (possibly infinite-dimensional) vector space has a basis in the foregoing sense.

Theorem 172. *Let U be a vector space with basis $(u_i \mid i \in I)$. Let V be a vector space with basis $(v_j \mid j \in J)$. These may be infinite-dimensional.*

(a) *Then $U \otimes V$ admits the basis $\big(u_i \otimes v_j \mid (i, j) \in I \times J\big)$.*

(b) *If U, V are finite-dimensional then* $\dim(U \otimes V) = \dim(U)\,\dim(V)$.

Proof. It is clear that (b) follows from (a). We prove (a).

Let W be a vector space with basis $(w_{ij} \mid (i, j) \in I \times J)$. Define

$$q\colon U \times V \to W, \quad q\Big(\sum_{i \in I} a_i u_i, \sum_{j \in J} b_j v_j\Big) = \sum_{(i,j) \in I \times J} a_i b_j w_{ij}.$$

Here only finitely many a_i and b_j are nonzero. We claim that $q\colon U \times V \to W$ is a tensor product.

Prove yourself that q is bilinear. We must prove the universal property. Let $r\colon U \times V \to X$ be bilinear. We must prove that there exists a unique linear map $f\colon W \to X$ such that $r = f \circ q$.

Unicity of f. We have $f(w_{ij}) = (f \circ q)(u_i, v_j) = r(u_i, v_j)$. But the w_{ij} span W so f is unique.

Existence of f. Since $(w_{ij} \mid (i, j) \in I \times J)$ is a basis of W there exists a unique linear map $f\colon W \to X$ such that $f(w_{ij}) = r(u_i, v_j)$ for all i, j. Let f be so defined.

We have $f \circ q = r$ because

$$\begin{aligned}(f \circ q)\big(\sum_{i\in I} a_i\, u_i, \sum_{j\in J} b_j\, v_j\big) &= f\big(\sum_{(i,j)\in I\times J} a_i\, b_j\, w_{ij}\big) = \sum_{(i,j)\in I\times J} a_i\, b_j\, f(w_{ij}) \\ &= \sum_{(i,j)\in I\times J} a_i\, b_j\, r(u_i, v_j) = r\big(\sum_{i\in I} a_i\, u_i, \sum_{j\in J} b_j\, v_j\big).\end{aligned}$$

Again only finitely many a_i and b_j are nonzero. This shows that f exists.

We have shown that $q\colon U \times V \to W$ is a tensor product.

Recall that theorem 163 implies that the tensor product of U and V is unique up to some isomorphism. We may therefore ignore which tensor product our theorem is thinking of and instead use W, the one we have constructed. The statement of the theorem then becomes that $(q(u_i, v_j) \mid (i, j) \in I \times J)$ is a basis for W. This is true by construction. The proof is complete. □

Remark 173. Hidden in the proof of theorem 172 there is an alternative proof that a tensor product of U and V exists. It is even a bit shorter than the first proof (in the proof of theorem 163). The disadvantage of the construction in the proof of theorem 172 is that it doesn't generalize to tensor products over other rings than fields (outside our scope).

Theorem 174. *Let U, V be finite-dimensional vector spaces and let $f\colon U \to U$ and $g\colon V \to V$ be linear maps. Let $f \otimes g\colon U \otimes V \to U \otimes V$ be the unique linear map such that $(f \otimes g)(u \otimes v) = f(u) \otimes g(v)$ for all $(u, v) \in U \otimes V$ (see example 166).*

(a) *Write the characteristic polynomials of f and g as*

$$\det(x - f) = \prod_{i\in I}(x - \alpha_i), \qquad \det(x - g) = \prod_{j\in J}(x - \beta_j).$$

Then the characteristic polynomial of $f \otimes g$ is $\prod_{(i,j)\in I\times J}(x - \alpha_i\, \beta_j)$.

(b) $\operatorname{tr}(f \otimes g) = \operatorname{tr}(f)\ \operatorname{tr}(g)$.

Proof. Proof of (a). We only prove this if f, g are diagonalisable and leave the general case to you (exercise 10.4).

Let $(u_i \mid i \in I)$ be a basis of U such that $f(u_i) = \alpha_i\, u_i$ for all i. Likewise, let $(v_j \mid j \in J)$ be a basis of V such that $g(v_j) = \beta_j\, v_j$ for all j.

By theorem 172, $(u_i \otimes v_j \mid (i, j) \in I \times J)$ is a basis for $U \otimes V$. The definition of $f \otimes g$ implies that for all i, j

$$(f \otimes g)(u_i \otimes v_j) = f(u_i) \otimes g(v_j) = (\alpha_i\, u_i) \otimes (\beta_j\, v_j) = \alpha_i\, \beta_j \cdot (u_i \otimes v_j).$$

This proves part (a). We deduce (b) from (a) as follows:

$$\operatorname{tr}(f \otimes g) = \sum_{(i,j)\in I\times J} \alpha_i\, \beta_j = \Big(\sum_{i\in I} \alpha_i\Big)\Big(\sum_{j\in J} \beta_j\Big) = \operatorname{tr}(f)\ \operatorname{tr}(g).$$ □

Corollary 175. *Let G be a group. Let U, V be $\mathbb{C}G$-modules and recall that then $U \otimes V$ is a $\mathbb{C}G$-module. Recall that χ_U denotes the character of U. Then $\chi_{U\otimes V} = \chi_U\, \chi_V$.*

Proof. Immediate from theorem 174(b). □

So the product of two characters is again a character.

10.4 Exercises

(10.4) Finish the proof of theorem 174(a) by handling the case where f and g may not be diagonalisable.

Hint for a first solution: put f, g into upper diagonal form.

Hint for a second solution: use that the set of diagonalisable matrices in $\mathrm{End}(U)$ is dense in your favourite sense.

(10.5) Let $(u_i \mid i \in I)$ be vectors in a vector space U. Likewise, let $(v_j \mid j \in J)$ be vectors in a vector space V. True or false?

(a) If the u_i are independent and the v_j are independent then the $u_i \otimes v_j$ are independent.

(b) If the $u_i \otimes v_j$ are independent then the u_i are independent or the v_j are independent.

(c) If the $u_i \otimes v_j$ are independent then the u_i are independent.

(d) If the u_i span U and the v_j span V then the $u_i \otimes v_j$ span $U \otimes V$.

(e) If the $u_i \otimes v_j$ span $U \otimes V$ then the u_i span U or the v_j span V.

(f) If the $u_i \otimes v_j$ span $U \otimes V$ then the u_i span U.

(10.6) Let p, q be characters of a finite group G. Prove that if p is not irreducible then neither is pq.

(10.7) Find an example of irreducible characters p, q of a finite group G such that pq is not irreducible.

(10.8) Let G, H be groups. Let p be a character of G and q a character of H. Prove that the map

$$\begin{aligned} p * q \colon G \times H &\longrightarrow \mathbb{C} \\ (g, h) &\longmapsto p(g)\, q(h) \end{aligned}$$

is a character of $G \times H$.

(10.9) Let U, V be finite-dimensional vector spaces. Let $B(U, V)$ denote the set of bilinear maps $U \times V \to \mathbb{C}$.

(a) Prove that $B(U, V)$ becomes a vector space by the pointwise operations $(ar + bs)(u, v) := a\, r(u, v) + b\, s(u, v)$ for all $r, s \in B(U, V)$, $a, b \in \mathbb{C}$, $(u, v) \in U \times V$.

(b) For a vector space W, define the **dual** W^* to be $\mathrm{Hom}(W, \mathbb{C})$. Prove that there exists a unique bijective linear map $f \colon U^* \otimes V^* \to B(U, V)$ such that $(f(p \otimes q))(u, v) = p(u)\, q(v)$ for all $(u, v) \in U \times V$.

(10.10) See exercise 10.3 for the definition of $\mathrm{Hom}(U, V)$. Fix a group G.

(a) Let U, V be $\mathbb{C}G$-modules. Prove that a G-action on $\mathrm{Hom}(U, V)$ is obtained by putting $(gL)(u) = gLg^{-1}(u)$ for all $g \in G$, $L \in \mathrm{Hom}(U, V)$, $u \in U$.

(b) Let U, V, W be $\mathbb{C}G$-modules. Prove that there exists a unique homomorphism of $\mathbb{C}G$-modules $\mathrm{Hom}(V, W) \otimes \mathrm{Hom}(U, V) \to \mathrm{Hom}(U, W)$ taking $S \otimes T$ to $S \circ T$ for all $(S, T) \in \mathrm{Hom}(V, W) \times \mathrm{Hom}(U, V)$.

(c) Assume that G is finite and let U, V be finite-dimensional $\mathbb{C}G$-modules with characters χ_U, χ_V. Prove that the character of $\mathrm{Hom}(U, V)$ is $\bar{\chi}_U\, \chi_V$.

(d) See exercise 10.9 for the definition of dual vector space. Let U, V be $\mathbb{C}G$-modules. Prove that there exists a unique bijective homomorphism of $\mathbb{C}G$-

modules $L\colon U^* \otimes V \to \mathrm{Hom}(U,V)$ such that $(L(T\otimes v))u = T(u)\cdot v$ for all $T \in U^*$, $u \in U$, $v \in V$.

(10.11) Recall that U, V are $\mathbb{C}G$-modules then so are $U \oplus V$ and $U \otimes V$. Let U, V, W be $\mathbb{C}G$-modules. Prove that there are isomorphisms of $\mathbb{C}G$-modules as follows. You cannot use that both sides have the same character because G is not assumed to be finite!

(a) $U \otimes V \cong V \otimes U$.

(b) $(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$.

(c) $(U \oplus V) \otimes W \cong (U \otimes W) \oplus (V \otimes W)$.

11 Appendix: Summary of linear algebra

11.1 Introduction

In this section we summarise linear algebra. We give all definitions and the most important results needed for our module. Proofs, simpler results and examples cannot be found here.

This is not a place where you can learn linear algebra. The summary is too short for that.

Throughout we fix a field K (for example $K = \mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p$) whose elements are called **constants** or **scalars**.

11.2 Vector spaces

Definition 176: Vector spaces. A **vector space** over K is a non-empty set V together with maps $V \times V \to V$ written $(x,y) \mapsto x+y$ and $K \times V \to V$ written $(a,x) \mapsto ax$ such that

$$a(bx) = (ab)x \qquad (a+b)x = ax+bx$$
$$a(x+y) = ax+ay \qquad (x+y)+z = x+(y+z)$$

for all $a, b \in K$ and $x, y, z \in V$.

Every vector space V has a unique element $0 = 0_V$ such that $0_V + x = x + 0_V = x$ and $0 \cdots x = 0_V$ for all $x \in V$.

We make K^n into a vector space over K by putting

$$(x_1,\dots,x_n) + (y_1,\dots,y_n) := (x_1+y_1,\dots,x_n+y_n),$$
$$a(x_1,\dots,x_n) := (ax_1,\dots,ax_n).$$

Definition 177: Linear subspace. Let V be a vector space over K and $U \subset V$ a non-empty subset. We say that U is a **(linear) subspace** of V if $ax+by \in U$ whenever $a,b \in K$ and $x,y \in U$.

In particular, $\{0\}$ is a linear subspace of V. It is usually simply written 0.

Theorem/Definition 178. *Let X, Y be subspaces of a vector space V. Then $X \cap Y$ and $X + Y := \{x+y \mid x \in X,\ y \in Y\}$ are again subspaces of V.*

11.3 Basis, dimension

Definition 179. Let V be a vector space over K.

(a) A sequence $(x_1, \dots, x_k)$ of elements of V is called **(linearly) independent** if

$$\sum_{i=1}^{k} a_i x_i = 0 \quad \Longrightarrow \quad a_i = 0 \text{ for all } i$$

for all $a_1, \dots, a_k \in K$.

(b) A sequence $(x_1, \dots, x_n)$ of elements of V is said to **span** V if V is spanned by the subspaces $U_k = Kx_k := \{ax_k \mid a \in K\}$.

(c) A sequence $(x_1, \dots, x_n)$ of elements of V is called a **basis** of V if it is independent and spans V.

Proposition 180: Basis. *Let V be a vector space spanned by finitely many vectors. Then V has a basis. Any two bases have the same number of elements.*

Definition 181. Let V be a vector space spanned by finitely many vectors. The **dimension** of V is the number of elements in one (hence any, by proposition 180) basis.

The **standard basis** of K^n is $(e_1, \dots, e_n)$ where e_i has a 1 in the ith slot and zeroes elsewhere.

Proposition 182. *Let X, Y be finite-dimensional subspaces of a vector space V. Then*

$$\dim(X \cap Y) + \dim(X + Y) = \dim(X) + \dim(Y).$$

11.4 Linear maps, matrices

Definition 183: Linear map. Let V, W be vector spaces over K. A **linear map** $V \to W$ is a map f such that

$$f(ax + by) = a\, f(x) + b\, f(y)$$

for all $a, b \in K$, $x, y \in V$. Let $\mathrm{Hom}(V, W)$ denote the set of linear maps $V \to W$.

Proposition/Definition 184. *Let $A = (a_1, \dots, a_v)$ be a basis of a vector space V and $B = (b_1, \dots, b_w)$ a basis of a vector space W, both vector spaces over K. There is a unique bijection* $\mathrm{Hom}(W, V) \to M_{v \times w}(K)$ *written $f \mapsto \langle A, f, B\rangle$ such that if c_{ij} are the entries of $\langle A, f, B\rangle$ then*

$$f(b_j) = \sum_{i=1}^{v} c_{ij}\, a_i$$

for all $j \in \{1, \dots, w\}$. We call

$$\langle A, f, B\rangle = (c_{ij})_{1 \le i \le v}^{1 \le j \le w} = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1w} \\ c_{21} & c_{22} & \cdots & c_{2w} \\ \cdots & \cdots & \cdots & \cdots \\ c_{v1} & c_{v2} & \cdots & c_{vw} \end{pmatrix}$$

the **matrix of f with respect to bases A and B.**

Let

$$A = (a_{ij})_{1\le j\le q}^{1\le i\le p}, \qquad B = (b_{jk})_{1\le k\le r}^{1\le j\le q}, \qquad C = (c_{ik})_{1\le k\le r}^{1\le i\le p}$$

be three matrices. We write $AB = C$ provided

$$c_{ik} = \sum_{j=1}^{q} a_{ij}\, b_{jk}$$

for all i, k.

Proposition 185. *Matrix multiplication is compatible with composition of linear maps in the sense that*

$$\langle A, f, B\rangle\langle B, g, C\rangle = \langle A, fg, C\rangle.$$

The set $M_n(K)$ of $n \times n$ matrices is a non-commutative ring under matrix multiplication and addition.

If V is a vector space, let $\mathrm{End}(V)$ denote the set of **endomorphisms** of V, that is, linear maps from V to itself. Then $\mathrm{End}(V)$ is a non-commutative ring in which multiplication is given by composition and addition is defined by $(f+g)(x) := f(x) + g(x)$.

In fact, if V is n-dimensional and A is a basis of V then we have an isomorphism of rings $\mathrm{End}(V) \to M_n(K)$ given by $f \mapsto \langle A, f, A\rangle$.

Two elements X, Y of $M_n(K)$ are called **similar** if there exists $P \in \mathrm{GL}(n, K)$ such that $X = PYP^{-1}$.

If A, B are two bases of a finite-dimensional vector space V and $f \in \mathrm{End}(V)$ then $\langle A, f, A\rangle$ and $\langle B, f, B\rangle$ are similar.

Let $f\colon V \to W$ be a linear map. Its **kernel** is $\ker f = \{x \in V \mid f(x) = 0\}$. Its image is $\mathrm{im}\, f = \{f(x) \mid x \in V\}$. Then $\ker f$ is a subspace of V and $\mathrm{im}\, f$ is a subspace of W.

Proposition 186. *Let $f\colon V \to W$ be a linear map and suppose that V is finite-dimensional. Then*

$$\dim \ker f + \dim \mathrm{im}\, f = \dim V.$$

11.5 Determinants, characteristic polynomial

Proposition/Definition 187. *There exists a unique homomorphism* $\mathrm{sign}\colon S_n \to \{-1, 1\}$ *such that* $\mathrm{sign}(i, j) = -1$ *for all distinct $i, j \in \{1, \ldots, n\}$.*

Definition 188. The **determinant** of an $n \times n$ matrix $A = (a_{ij})$ is

$$\det(A) = \sum_{s\in S_n} \mathrm{sign}(s) \prod_{k=1}^{n} a_{k,s(k)}.$$

The **characteristic polynomial** of A is $\det(t - A)$ where t is a variable.

Proposition 189. (a) *Let $A, B \in M_n(K)$. Then* $\det(AB) = \det(A)\det(B)$.

(b) *Let $A \in M_n(K)$. Then A is invertible if and only if* $\det(A) \neq 0$.

(c) *Any two similar matrices have the same characteristic polynomial. In particular, they have the same determinant.*

The group of invertible elements of $M_n(K)$ is written $\mathrm{GL}(n, K)$ and called the **general linear group**.

Proposition/Definition 190. *Let A, B be two bases of a finite-dimensional vector space and let $f\colon V \to V$ be a linear map. Then $\langle A, f, A\rangle$ and $\langle B, f, B\rangle$ have equal determinants. They are called the* **determinant** *of f and written* $\det(f)$.

Definition 191. Let V be a vector space and $f\colon V \to V$ a linear map.

(a). The **characteristic polynomial** of f is $\det(t - f)$.

(b). It is easy to see that there exists a unique monic polynomial $M \in K[X]$ of minimal degree such that $M(f) = 0$. We call M the **minimal polynomial of f**.

Proposition 192: Cayley-Hamilton. *Let V be a finite-dimensional vector space and $f \in \mathrm{End}(V)$. Then f is a root of its characteristic polynomial, that is, substituting f for the variable t yields zero. Equivalently, the minimal polynomial of f divides the characteristic polynomial.*

Definition 193. A matrix $X \in M_n(K)$ is said to be **upper triangular** if $X_{ij} = 0$ whenever $j < i$.

Proposition 194. *The determinant of an upper triangular matrix is the product of the diagonal entries.*

11.6 Eigenvectors, Jordan blocks

Let V be a vector space and $f\colon V \to V$ a linear map. If $v \in V \setminus \{0\}$ and $a \in K$ are such that $f(v) = av$ then we say that v is an eigenvector of f with eigenvalue a.

Proposition 195. *Let V be a vector space and $f\colon V \to V$ a linear map. Let a be a constant. Then a is an eigenvalue for f if and only if* $\det(a - f) = 0$, *that is, a is a root of the characteristic polynomial of f.*

A **diagonal matrix** is a square matrix all of whose off-diagonal entries are zero. A matrix is said to be **diagonalisable** if it is similar to a diagonal matrix. Similar definitions hold for endomorphisms in $\mathrm{End}(V)$ if V is finite-dimensional.

Proposition 196. *Let A be a square matrix. If K is algebraically closed (for example $K = \mathbb{C}$) then the following are equivalent:*

(1) *A is diagonalisable.*

(2) *K^n is spanned by the eigenvectors of A.*

(3) *The minimal polynomial of A has no multiple roots.*

If K is not algebraically closed then the first two items are equivalent.

Definition 197. An $n \times n$ matrix (a_{ij}) is said to be a **Jordan block** if there exists $b \in K$ such that $a_{kk} = b$ for all k and $a_{k,k+1} = 1$ for all k and $a_{k\ell} = 0$ elsewhere.

Proposition 198: Jordan normal form. *Assume that K is algebraically closed, for example $K = \mathbb{C}$.*

(a) *Let $A \in M_n(K)$. Then there exists $T \in \mathrm{GL}(n, K)$ such that TAT^{-1} is in* **Jordan normal form**, *that is, is in block form such that the diagonal blocks are Jordan blocks and the off-diagonal blocks are zero.*

(b) *Let $A, B \in M_n(K)$ both be in Jordan normal form. Let $(A_1, \ldots, A_p)$ be the Jordan blocks of A and $(B_1, \ldots, B_q)$ those of B. Then A, B are similar if and only if $p = q$ and there exists $s \in S_p$ such that $A_k = B_{s(k)}$ for all k.*

(11.1) Let G be the presented group

$$G = \langle x, y \mid x^7,\ y^6,\ x^{-3}yxy^{-1} \rangle.$$

Let H be the group of permutations of $\mathbb{F}_7 = \mathbb{Z}/7$ of the form $x \mapsto ax + b$ where $a, b \in \mathbb{F}_7$, $a \neq 0$. You may assume that H is indeed a group. Define $r, s \in H$ by

$$r(x) = x + 1, \qquad s(x) = 3x.$$

(a) Recall that the free group F on a set A is the set of reduced words in A. Define the multiplication in this group.

(b) What is a group presentation? What is the group presented by it?

(c) Prove that there exists a unique homomorphism $f\colon G \to H$ such that $f(x) = r$, $f(y) = s$. State any theorems you use.

(d) Prove that f is surjective.

(e) Prove that every element of G can be written $x^k y^\ell$ with $0 \leq k < 7$ and $0 \leq \ell < 6$.

(f) Prove that f is bijective.

(11.2) Let G be a finite group and V, W be finite-dimensional $\mathbb{C}G$-modules.

(a) Define **homomorphism** of $\mathbb{C}G$-modules $V \to W$.

(b) Let $L\colon V \to W$ be a homomorphism of $\mathbb{C}G$-modules. Prove that the image of L is a submodule of W.

In the remainder of the question, you may also assume that under the present assumptions, the kernel of L is a submodule of V.

(c) Define what it means for a $\mathbb{C}G$-module to be **simple**.

(d) Assume that V, W are simple. Prove that every $\mathbb{C}G$-homomorphism $L\colon V \to W$ is 0 or an isomorphism.

(e) Assume that V is simple. Prove that every $\mathbb{C}G$-homomorphism $L\colon V \to V$ is scalar.

(f) Let V be a simple $\mathbb{C}G$-module. Recall

$$Z(G) := \{g \in G \mid ag = ga \text{ for all } a \in G\}$$

and let $g \in Z(G)$. Prove that there exists $\lambda \in \mathbb{C}$ such that $gx = \lambda x$ for all $x \in V$.

(11.3)

(a) Calculate the character table of S_4. Show the intermediate steps and justify them.

(b) Put $H = S_4$, $G = S_5$. Calculate the induced character χ^G where χ is the unique irreducible degree 2 character of H.

(c) Prove that there are two distinct irreducible characters λ, μ of G such that $\chi^G = \lambda + \mu$. State all results that you use.

(11.4) Let $n \geq 1$ be odd, $n = 2s + 1$. Recall that the dihedral group D_{2n} is presented as $\langle r, s \mid r^n,\ s^2,\ (rs)^2 \rangle$. We write $G = D_{2n}$.

(a) Find all 1-dimensional representations of G. There are two of them.

(b) Let $\omega = \exp(2\pi i/n)$ and put

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

From now on you may assume that for all $k \in \mathbb{Z}$ there exists a unique representation ρ_k of D_{2n} such that $\rho(r) = A^k$, $\rho(s) = B$.

For which k is ρ_k irreducible? Prove your result.

Hint: Every 1-dimensional submodule is clearly spanned by an eigenvector of B.

(c) Briefly explain the relation between linear representations $G \to \mathrm{GL}(n, \mathbb{C})$ and $\mathbb{C}G$-modules, that is, give two sets between which a bijection exists. Define this bijection in one direction.

(d) Define what it means for two representations $\rho\colon G \to \mathrm{GL}(m, \mathbb{C})$ and $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ to be **equivalent**.

(e) Prove that the 1-dimensional representations of G together with $\rho_1, \ldots, \rho_s$ form a maximal set of inequivalent irreducible representations of D_{2n}. You may assume without proof that $\rho_1, \ldots, \rho_s$ are pairwise inequivalent.

(f) Define conjugacy class.

(g) How many conjugacy classes does G have? State any results that you use.

(11.5) (a) Define class function.

(b) If p, q are class functions on a finite group G, define their inner product $(p, q)_G$.

(c) Define induction of class functions.

(d) Let $H \leq G$ be finite groups. Let $p \in \mathrm{CF}(G)$ and $q \in \mathrm{CF}(H)$ be class functions. Prove Frobenius reciprocity: $(p_H, q)_H = (p, q^G)_G$.

(e) Put $H = A_3 \subset G = S_4$. Write $\omega = \exp(2\pi i/3)$ and let λ be the linear character of H such that $\lambda((123)) = \omega$. Calculate the induced character λ^G. State any results that you use.

(f) Let 1_K denote the trivial linear character of any group K. Let $H \subset G$ be finite groups. Prove that $(1_H)^G - 1_G$ is a character of G. State any results from the lectures that you use.

(11.6) (a) Let N be a subgroup of a group G. What does it mean to say that N is normal in G?

(b) Let $N_1, \ldots, N_t$ be normal subgroups of a group G and put $M = N_1 \cap \cdots \cap N_t$. Prove that M is also normal in G. You don't need to prove that it is a subgroup.

(c) Let N be a normal subgroup of a finite group G. Prove that there exist irreducible characters $\lambda_1, \ldots, \lambda_t$ of G such that

$$N = \ker(\lambda_1) \cap \cdots \cap \ker(\lambda_t).$$

(d) Let ρ be an n-dimensional representation of a finite group G. Recall that we define the kernel of χ_ρ to be the kernel of ρ. Prove:

$$\ker(\chi_\rho) = \{g \in G \mid \chi_\rho(g) = \chi_\rho(1)\}.$$

(e) Find the character table of A_4. You may assume that there exists a linear character χ_2 of A_4 such that $\chi_2((123)) = \omega := \exp(2\pi i/3)$ and $\chi_2((12)(34)) = 1$.

(f) Combine the foregoing results to find all normal subgroups of A_4.

12 Index

13 Index of notation