INTRODUCTION TO REPRESENTATION THEORY AND CHARACTERS

DAN CIUBOTARU

1. Algebras and modules

1.1. **Definitions.** We begin by defining some basic notions in algebra: rings, algebras, modules. All of this (with the possible exception of algebras) has been defined in the Part A "Ring and Modules" option.

Definition 1.1. *A* ring *is a triple* $(A, +, \cdot)$, *where* A *is a set,* $+$ *and* $\cdot$ *are binary operations on* A *(addition and multiplication, respectively), such that*

(1) $(A, +)$ *is an abelian group;*
(2) $\cdot$ *is associative*[1]*;*
(3) $+, \cdot$ *satisfy the distributivity laws.*

The ring A is called commutative if $\cdot$ is commutative. The rings in this course will all have identity $1 \in A$ (with respect to multiplication)[2].

A *left ideal* I of A is a subgroup of $(A, +)$ such that $a \cdot i \in I$ for all $a \in A$ and $i \in I$. We simarly have the notion of right ideal and two-sided ideal (left and right). If I is a two-sided ideal, we may define the quotient ring A/I, which is the set $\{a + I \mid a \in A\}$ with the operations

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I) \cdot (b + I) = a \cdot b + I.$$

Definition 1.2. *Let* k *be a field. A* k-algebra A *is a ring* A *which is also a* k*-vector space such that*

$$(\lambda a) \cdot b = a \cdot (\lambda b) = \lambda(a \cdot b).$$

The dimension $\dim_k A$ of A as a vector space is called the dimension of the algebra A.

Example 1.3. *(1) If* F *is a field extension of* k*, then* F *is a* k*-algebra.*
(2) The polynomial ring in n *variables* $\mathsf{k}[x_1, \dots, x_n]$ *is a* k*-algebra.*
(3) The ring of $n \times n$ *matrices* $M_n(\mathsf{k})$ *with entries in* k *is a* k*-algebra.*
(4) Let V *be a* k*-vector space. Consider the endomorphism ring*

$$\mathrm{End}_{\mathsf{k}}(V) = \{T : V \to V \ \mathsf{k}\text{-linear map}\},$$

under the addition and composition of linear maps. This is k*-algebra. The identity is the identity map. If* V *is finite dimensional, then it is isomorphic to* k^n*, and* $\mathrm{End}_{\mathsf{k}}(V)$ *can be identified with* $M_n(\mathsf{k})$*.*

1.2. **The group algebra.** An important example is the *group algebra.* If G is a group, we define $\mathsf{k}G$ to be the vector space with basis $\{v_g \mid g \in G\}$. Here v_g are just some symbols indexed by $g \in G$. Then we define the multiplication by

$$v_{g_1} \cdot v_{g_2} = v_{g_1 g_2}.$$

A typical element in $x \in \mathsf{k}G$ is $x = \sum_{g \in G} a_g v_g$, where $a_g \in \mathsf{k}$ and only finitely many a_g are nonzero (so that the sum is finite). If $y = \sum_{g \in G} b_g v_g$ is another element in $\mathsf{k}G$, then

$$x \cdot y = \sum_{g,h \in G} a_g b_h v_{gh} = \sum_{s \in G} (\sum_{t \in G} a_t b_{t^{-1}s}) v_s \tag{1.1}$$

It is immediate that $\mathsf{k}G$ is a k-algebra.

---

[0] Notes for Oxford's Part B course B2.1, Michaelmas 2017.

[1] There exist interesting nonassociative rings, e.g., the Lie algebras, but we won't consider them in this course.

[2] There exist important associative rings with no identity, e.g., most of the convolution rings that appear in analysis or in infinite-dimensional representation theory.

Example 1.4. *Take $C_3 = \langle \xi \mid \xi^3 = 1 \rangle$. If $x, y \in \mathsf{k}C_3$ are $x = v_\xi + 2v_{\xi^2}$ and $y = v_1 + v_\xi$, then $x \cdot y = 2v_1 + v_\xi + 3v_{\xi^2}$.*

It is tedious to carry the notation v_g in the group algebra. If we think of G as a multiplicative group, then we can write $x = \sum_{g \in G} a_g g$ in place of $x = \sum_{g \in G} a_g v_g$, with no danger of confusion.

1.3. **Homomorphisms.** If A is a k-algebra, the ideals in A are the usual ideals with respect to the ring structure. If I is a two-sided ideal of A, then A/I is the quotient k-algebra. A subalgebra of A is a k-subspace which is also closed under the multiplication.

If B is another k-algebra, an algebra homomorphism is a map $\phi : A \to B$ such that

(1) ϕ is a homomorphism of rings with identity, and
(2) ϕ is a k-linear map.

We then have the three usual isomorphism theorems, whose proof is always the same, and therefore we skip.[3]

Theorem 1.5 (First isomorphism theorem)**.** *If $\phi : A \to B$ is an algebra homomorphism, then $\ker \phi$ is a two-sided ideal of A, $\operatorname{im} \phi$ is a subalgebra, and $A/\ker \phi \cong \operatorname{im} \phi$.*

Theorem 1.6 (Second isomorphism theorem)**.** *Suppose B is a subalgebra of A and I is a two-sided ideal of A. Then BI is a subalgebra of A, $B \cap I$ is an ideal of B and $BI/I \cong B/B \cap I$.*

Theorem 1.7 (Third isomorphism theorem)**.** *Suppose I is a two-sided ideal of the algebra A and J is a two-sided ideal of I. Then I/J is an ideal of A/J and $(A/J)/(I/J) \cong A/I$.*

In a k-algebra A, the field k can be identified with $\mathsf{k} \cdot 1$, where 1 is the identity in A. More precisely, we consider the map $\tau : \mathsf{k} \to A$, $\lambda \mapsto \lambda \cdot 1$. This is a k-algebra homomorphism, and it is injective, because A is a k-vector space and $1 \neq 0$, hence $\lambda \cdot 1 = 0$ if and only if $\lambda = 0$. We will make this identification implicitly.

1.4. **Modules.**

Definition 1.8. *Let A be a ring. A left* A-module *M is an abelian group with an action $A \times M \to M$, $(a, m) \mapsto a \cdot m$, satisfying*

(1) $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$;
(2) $a \cdot (b \cdot m) = (ab) \cdot m$;
(3) $(a + b) \cdot m = a \cdot m + b \cdot m$;
(4) $1 \cdot m = m$.

Notice that if A is a k-algebra and M is an A-module, then M is also a k-vector space (thinking of k as a subfield of A as mentioned before):

$$\lambda m = (\lambda 1) \cdot m, \quad \lambda \in \mathsf{k},\ m \in M.$$

If M and N are A-modules, a map $f : M \to N$ is called an *A-module homomorphism* (or *A-linear*) if

(1) $f(m_1 + m_2) = f(m_1) + f(m_2)$, $m_1, m_2 \in M$;
(2) $f(a \cdot m) = a \cdot f(m)$, $a \in A$, $m \in M$.

If f is a A-linear then, in particular, it is k-linear. We define submodules and direct sums of modules in the usual way, just as for modules over rings.

If M and N are A-modules, define

$$\operatorname{Hom}_A(M, N) = \{f : M \to N \mid f \text{ is an } A\text{-homomorphism}\}. \tag{1.2}$$

Notice that $\operatorname{Hom}_A(M, N)$ is a k-vector space. If $M = N$, denote

$$\operatorname{End}_A(M) = \operatorname{Hom}_A(M, M). \tag{1.3}$$

Then $\operatorname{End}_A(M)$ is an A-algebra with multiplication given by composition. If we regard A as a left A-module under multiplication, then it is natural to ask what is $\operatorname{End}_A(A)$ as an algebra.

[3]When you take the Part C course "Category Theory", you will see that these theorems and their proofs are general "abstract nonsense" concepts.

Definition 1.9. *If A is a ring (or a k-algebra) define the* opposite ring *(or algebra) to be $A^{\mathsf{op}} = A$ as an abelian group (or k-vector space), but with the multiplication in A^{op} given by*

$$a \cdot_{\mathsf{op}} b = b \cdot a,$$

where $b \cdot a$ is the multiplication in A.

For every $a \in A$, define the map $r_a : A \to A$, $r_a(x) = xa$. Since the multiplication by a is on the right, it is clear that r_a is an endomorphism of left A-modules, hence $r_a \in \mathrm{End}_A(A)$.

Proposition 1.10. *The map $\psi : A^{\mathsf{op}} \to \mathrm{End}_A(A)$, $a \mapsto r_a$ is an algebra isomorphism.*

Proof. Let 1_A be the identity in A. Begin by noticing that if $f \in \mathrm{End}_A(A)$, then $f(a) = f(a \cdot 1_A) = a \cdot f(1_A)$, so every endomorphism of A is uniquely determined by where it sends 1_A. In particular, $f = r_{f(1_A)}$. This means that ψ is surjective. It is also injective since $r_a = r_b$ implies that $r_a(1_A) = r_b(1_A)$, hence $a = b$.

Next, it is immediate that $r_a + r_b = r_{a+b}$. To check the multiplication, we see that $(r_a \circ r_b)(x) = r_a(xb) = xba = r_{ba}(x)$, so $r_a \circ r_b = r_{a \cdot_{\mathsf{op}} b}$ and the claim is proved. □

Example 1.11. *If $A = M_n(\mathsf{k})$ is the matrix algebra, then $A^{\mathsf{op}} \cong A$ as algebras, with the isomorphism given by the matrix transpose.*

1.5. **Representations.** Let A be a k-algebra. A *representation* of A is a pair (ρ, V), where V is a vector space and $\rho : A \to \mathrm{End}_{\mathsf{k}}(V)$ is an algebra homomorphism.

Every A-representation (ρ, V) gives rise to an A-module on V via

$$a \cdot v = \rho(a)v.$$

Conversely, if V is an A-module, we define an A-representation by setting $\rho(a)v = a \cdot v$. So the notions of A-representations and A-modules are the "same thing". (In categorical language, we say that the corresponding categories are equivalent.)

A particularly important case is when G is a group and $A = \mathsf{k}G$ is the group algebra. A *G-representation* is a pair (ρ, V), where V is a vector space and $\rho : G \to GL(V)$ is a group homomorphism. We claim that G-representations and $\mathsf{k}G$-modules are the "same thing". In one direction, if (ρ, V) is a G-representation, define a $\mathsf{k}G$-module structure on V by setting

$$(\sum_g a_g g) \cdot v = \sum_g a_g \ \rho(g)v.$$

Here $\sum_g a_a g$ denotes an element of $\mathsf{k}G$ and $v \in V$. Conversely, if V is a $\mathsf{k}G$-module, we define a G-representation ρ on V by setting

$$\rho(g)v = g \cdot v,$$

where in the right hand side we think of g as an element of $\mathsf{k}G$.

Remark 1.12. *The group algebra $\mathsf{k}G$ is isomorphic to its opposite algebra $(\mathsf{k}G)^{\mathsf{op}}$ with the isomorphism given by $\sum_g a_g g \mapsto \sum_g a_g g^{-1}$.*

We know what isomorphism for modules means. The analogous notion for representations is *equivalence*.

Definition 1.13. *Let $\rho_i : A \to \mathrm{End}_{\mathsf{k}}(V_i)$, $i = 1, 2$, be two representations of the k-algebra A. We say that ρ_1 and ρ_2 are equivalent is there exists a linear isomorphism $\psi : V_1 \to V_2$ such that*

$$\psi(\rho_1(a)v) = \rho_2(a)\psi(v), \quad a \in A, \ v \in V.$$

Another way to write this relation is $\rho_1(a) = \psi^{-1} \circ \rho_2(a) \circ \psi$, for all $a \in A$.

After all of this "tautological mathematics", let's look at an example.

Example 1.14. *Let $G = D_{2n} = \langle r, \sigma \mid r^n = \sigma^2 = 1, \ \sigma r \sigma^{-1} = r^{-1} \rangle$ be the dihedral group. For every $1 \le m \le n-1$, we may define the representation $\rho_m : G \to GL(\mathbb{R}^2) = GL(2, \mathbb{R})$:*

$$\rho_m(r) = \begin{pmatrix} \cos(m\theta) & -\sin(m\theta) \\ \sin(m\theta) & \cos(m\theta) \end{pmatrix}, \quad \rho_m(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

where $\theta = \frac{2\pi}{n}$. It is easy to verify that $\rho_m(r)^n = \mathrm{Id} = \rho_m(\sigma)^2$, and $\rho_m(\sigma r \sigma^{-1}) = \rho_m(\sigma)\rho_m(r)\rho_m(\sigma)^{-1} = \rho_m(r)^{-1} = \rho_m(r^{-1})$. Since the relations in G are satisfied, it follows that ρ_m are all representations. We will return later to the question of whether or not they are equivalent.

Example 1.15. *Suppose the group G acts on a set Ω. We may define the* permutation module $M = \mathsf{k}\Omega$ *as follows. Let M be the k-vector space with basis $\{\omega \in \Omega\}$. Then the action of G on M is*

$$g \cdot (\sum_{\omega\in\Omega} \lambda_\omega \omega) = \sum_{\omega\in\Omega} \lambda_\omega (g \cdot \omega).$$

This is extended to an action of $\mathsf{k}G$ by linearity:

$$(\sum_{g\in G} a_g g) \cdot (\sum_{\omega\in\Omega} \lambda_\omega \omega) = \sum_{a\in G}\sum_{\omega\in\Omega} a_g \lambda_\omega (g \cdot \omega).$$

In this way, $\mathsf{k}\Omega$ is a $\mathsf{k}G$-module.

Example 1.16. *If G is a group, the* trivial representation *of G is (ρ, V), where $V = \mathsf{k}$ (i.e., a one-dimensional vector space) and $\rho(g)v = v$ for all $g \in G$, $v \in V$. The* trivial module *of $\mathsf{k}G$ is $V = \mathsf{k}$ with the action*

$$(\sum_{g\in G} a_g g) \cdot v = (\sum_{g\in G} a_g)v, \quad v \in V.$$

2. The Jordan-Hölder Theorem

If A is a k-algebra that we would like to decompose an A-module into "atoms", namely into *simple modules.*

2.1. **Simple modules.** An A-module $M \neq 0$ is called *simple* if its only submodules are 0 and M. The first example of a simple module is the trivial module from Example 1.16.

Exercise 2.1. *Let $A = \mathsf{k}S_n$ be the group algebra of the symmetric group S_n. Let $M = \{(x_1, \dots, x_n) \in \mathsf{k}^n \mid x_1 + \cdots + x_n = 0\}$ with the action of S_n given by permutation of indices. Show that M is a simple A-module.*

An important example is the following.

Lemma 2.2. *Let $A = M_n(\mathsf{k})$ be the algebra of $n \times n$ matrices and $M = \mathsf{k}^n$ (column vectors), which is viewed as an A-module by matrix multiplication. Then M is simple.*

Proof. We denote by E_{ij} the matrix which has 1 on the (i, j) position and 0 everywhere else. Also e_i denote the standard basis vectors of M.

Suppose N is a nonzero submodule of M. Let $0 \neq v = (x_1, \dots, x_n)$ be a vector of N. If $x_i \neq 0$, then $E_{ii} \cdot v = x_i e_i$ which must then be in N. So $e_i \in N$. Then $e_j = E_{ji} \cdot e_i \in N$ as well. Hence $N = M$. □

When $A = \mathsf{k}G$, we have the equivalent notion of *irreducible representation.* We say that $\rho : G \to GL(V)$ is reducible if there exists a proper subspace $0 \neq W \subset V$ such that $\rho(g)W \subseteq W$ for all $g \in G$. (We say that W is a G-stable.) If (ρ, V) is not reducible, we say that it is irreducible. It is immediate that irreducible G-representations are the same notion as simple $\mathsf{k}G$-modules.

If M is an A-module, a submodule N of M is called *maximal* if for every submodule L of M such that $N \subseteq L$, either $L = N$ or $L = M$.

If N is a submodule of M, we have a natural one-to-one correspondence between submodules of the quotient module M/N and submodules of M containing N. This is just the obvious thing: if L is a submodule of M containing N, then L/N is a submodule of M/N. But this implies that $N \subset M$ is maximal if and only if M/N is a simple module.

Now suppose M is a simple A-module. Fix $m \in M$, $m \neq 0$. We may define a map

$$f_m : A \to M, \quad a \mapsto a \cdot m.$$

Since $f_m(1) = m \neq 0$, this is a nonzero map. It is trivial to check that f_m is A-linear:

$$f_m(ax) = (ax) \cdot m = a \cdot (x \cdot m) = a \cdot f(x), \quad a, x \in A.$$

By the first isomorphism theorem $A/\ker f_m \cong \operatorname{im} M = M$ since M is simple. But $\ker f_m$ is a left ideal of A, which means that every simple A-module can be realised as a quotient $M = A/I$ for a (maximal) left ideal of A. In particular, this means that if A is a finite-dimensional k-algebra, then every simple A-module is finite dimensional over k.

2.2. **Composition series.** Let M be an A-module.

Definition 2.3. *A* composition series *for M is a sequence of A-submodules of M*

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_\ell = M$$

such that M_{i+1}/M_i is a simple module for all i. The integer ℓ is called the length of the series, and the simple modules M_{i+1}/M_i are called the composition factors.

Example 2.4. *Let $G = C_p = \langle \xi \mid \xi^p = 1 \rangle$, where p is a prime number. Set $\mathsf{k} = \mathbb{F}_p$, the field with p elements. Consider the module $M = \mathsf{k}\langle x_1, \dots, x_p\rangle \cong \mathsf{k}^p$, where the action is given by*

$$\xi \cdot x_i = x_i + x_{i-1} \quad (x_0 := 0).$$

In other words, in the basis $\mathcal{B} = \{x_1, \dots, x_p\}$, the matrix of ξ looks like $[\xi]_{\mathcal{B}} = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$. This means that $[\xi - 1]_{\mathcal{B}}$ is strictly upper triangular with 1's immediately above the main diagonal. Therefore $[\xi - 1]_{\mathcal{B}}^p = 0$. But since we are in characteristic p, $(\xi - 1)^p = \xi^p - 1$, so $[\xi]_{\mathcal{B}}^p = 1$. This shows that the action is well defined and M is indeed a $\mathsf{k}C_p$-module.

It is clear that $M_i = \mathsf{k}\langle x_1, \dots, x_i\rangle$ are all submodules of M. Moreover $M_i/M_{i-1} = \mathsf{k}\langle \overline{x}_i\rangle$ is the trivial C_p-module. This means that M has a composition series of length p given by the submodules M_i and all of the composition factors are isomorphic to the trivial module. (It is easy to see in fact that the only simple module of $\mathsf{k}C_p$ is the trivial module!)

Lemma 2.5. *Let M be a finite-dimensional A-module and $N \subset M$ a submodule. Then M has a composition series containing N.*

Proof. Suppose $N \neq M$. If N and M/N are both simple, then $0 \subset N \subset M$ is a composition series of M. Otherwise, say for example that M/N is not simple. We may find N' such that $N \subsetneq N' \subseteq M$, so we extend the chain of submodules to $0 \subset N \subset N' \subset M$ and continue. (Similarly with $0 \subset N$ if N is not simple.) Since M is finite dimensional, this process has to stop. □

Theorem 2.6. *[Jordan-Hölder Theorem for finite-dimensional modules] Let M be a nonzero finite-dimensional A-module. Then M has a composition series and all composition series are* equivalent*: they have the same length and the same composition factors (up to isomorphism) counted with multiplicity.*

Proof. The proof is by induction on $\dim_{\mathsf{k}} M$. The base case is when $\dim_{\mathsf{k}} M = 1$. Then $0 \subset M$ is the unique composition series. Assume $\dim_{\mathsf{k}} M > 1$ and suppose

(i) $0 \subset M_1 \subset \cdots \subset M_{k-1} \subset M_k = M$,
(ii) $0 \subset N_1 \subset \cdots \subset N_{\ell-1} = M$

are two composition series of M. If $M_{k-1} = N_{\ell-1}$, then we are done by the induction step applied to $M' := M_{k-1} = N_{\ell-1}$. Otherwise, $M_{k-1} \neq N_{\ell-1}$, so $M_{k-1} + N_{\ell-1}$ is a strictly larger submodule than M_{k-1} and $N_{\ell-1}$, implying that $M_{k-1} + N_{\ell-1} = M$.

Set $L = M_{k-1} \cap N_{\ell-1}$. By the second isomorphism theorem,

$$M/M_{k-1} \cong (M_{k-1} + N_{\ell-1})/M_{k-1} \cong N_{\ell-1}/(M_{k-1} \cap N_{\ell-1}) = N_{\ell-1}/L, \tag{2.1}$$

and similarly

$$M/N_{\ell-1} \cong M_{k-1}/L.$$

Let $0 \subset L_1 \subset \cdots \subset L_t = L$ be a composition series of L. Then

(iii) $0 \subset L_1 \subset \cdots \subset L_t = L \subset M_{k-1} \subset M$,
(iv) $0 \subset L_1 \subset \cdots \subset L_t = L \subset N_{\ell-1} \subset M$

are composition series of M. They are equivalent, both of length $t + 2$, and composition factors given by the composition factors of L plus $M/N_{\ell-1} \cong M_{k-1}/L$ and $M/M_{k-1} \cong N_{\ell-1}/L$. On the other hand, by induction, the composition series (i) and (iii) are equivalent, and so are (ii) and (iv). Since the equivalence of composition series is obviously an equivalence relation, it implies that (i) and (ii) are equivalent too. □

Example 2.7. *Let $A = M_n(\mathsf{k})$ viewed as a left A-module. Denote by N_i the subspace of matrices where the last $(n-i)$ columns are all zero. It is clear that N_i is a left A-submodule of A and $N_{i+1}/N_i \cong \mathsf{k}^n$ which we have seen it is a simple $M_n(\mathsf{k})$-module. Hence*

$$0 \subset N_1 \subset \cdots \subset N_n = A$$

is a composition series of A and all the composition factors are isomorphic to k^n.

Corollary 2.8. *Let A be a finite-dimensional k-algebra. Every simple A-module S appears as a composition factor in every composition series of the A-module A.*

Proof. By Theorem 2.6, it is sufficient to prove that S occurs in one composition series of A. We have seen that S must be isomorphic (as a left A-module) to $S \cong A/I$, where I is a left ideal of A. But left ideals of A are the same as submodules of A. By Lemma 2.5, there exists a composition series of A containing I, which, since A/I is simple, must be of the form $) = M_0 \subset M_1 \subset \cdots \subset M_{\ell-1} = I \subset A$. This exhibits S as a composition factor.

□

Example 2.9. *The only simple module of $M_n(\mathsf{k})$ is k^n. This follows from Example 2.7 and Corollary 2.8.*

Corollary 2.10. *If A is a finite-dimensional k-algebra, there are only finitely many isomorphism classes of simple A-modules.*

Proof. This is immediate from Corollary 2.8 since in any given composition series, only finitely many simple modules appear. □

3. Basic results: Schur's Lemma, modules for commutative algebras

3.1. **Schur's Lemma.** This is one of the first results in representation theory. Let A be a k-algebra. The first part is a triviality.

Lemma 3.1 (Schur's Lemma).
(1) *Let M, N be simple A-modules and $f : M \to N$ be an A-homomorphism. Then $f = 0$ or f is an isomorphism.*
(2) *Suppose that k is algebraically closed and let M be a finite dimensional simple A-module. Every A-homomorphism $f : M \to M$ is a scalar multiple of the identity, i.e., $f = \lambda\,\mathrm{Id}_M$ for some $\lambda \in \mathsf{k}$.*

Proof. (1) Since $\ker f$ is a submodule of M which is simple, either $\ker f = 0$ (f injective) or $f = 0$. In the first situation, we look at $\operatorname{im} f$ which is a nonzero (because $f \neq 0$) submodule of N. Since N is simple, $\operatorname{im} f = N$ (f surjective).

(2) Since $f : M \to M$ is A-linear, it is k-linear. As k is algebraically closed, there exists $\lambda \in \mathsf{k}$ an eigenvalue of f. Let $0 \neq v \in M$ be a λ-eigenvector. Consider $g = f - \lambda\,\mathrm{Id}_M : M \to M$. This is A-linear, and $v \in \ker g$. Hence $\ker g \neq 0$ and by part (1), $g = 0$, which implies $f = \lambda\,\mathrm{Id}_M$. □

The second part of Schur's Lemma says that $\mathrm{End}_A(M) = \mathsf{k}$ when M is simple finite dimensional and k is algebraically closed.

Example 3.2. *The second part of Schur's Lemma is false when k is not algebraically closed. For example, take $G = C_3 = \langle \xi \mid \xi^3 = 1 \rangle$ acting on $M = \mathbb{R}^2$ by rotations: ξ acts by the rotation with angle of $\frac{2\pi}{3}$. Notice that M is a simple $\mathbb{R}C_3$-module: if it were not, then it would have a one-dimensional submodule, which is the same as a line stable under the action of ξ; but ξ does not have real eigenvalues. We may think of an element of $\mathrm{End}_{\mathbb{R}C_3}(M)$ as a 2×2 real matrix which commutes with the matrix given by the action of ξ: $R(2\pi/3) = \begin{pmatrix} \cos(2\pi/3) & -\sin(2\pi/3) \\ \sin(2\pi/3) & \cos(2\pi/3) \end{pmatrix}$. Then we see that $\mathrm{End}_{\mathbb{R}C_3}(M) = \mathbb{R}\langle I_2, R(2\pi/3), R(-2\pi/3) \rangle \cong \mathbb{R}C_3$.*

3.2. **Central characters.** Suppose that k is algebraically closed and let M be an A-module. Recall that the centre of A is

$$Z(A) = \{z \in A \mid za = az, \text{ for all } a \in A\}.$$

For every $z \in Z(A)$, we can define a map

$$f_z : M \to M,\ f_z(m) = z \cdot m.$$

Then $f_z(a \cdot m) = z \cdot (a \cdot m) = (za) \cdot m = (az) \cdot m = a \cdot (z \cdot m) = a \cdot f_z(m)$, which shows that f_z is A-linear. If M is simple finite dimensional, then by Schur's Lemma, there exists $\lambda_z \in \mathsf{k}$ such that $f_z(m) = \lambda_z m$, for all $m \in M$.

Proposition 3.3. *Suppose M is a finite-dimensional simple A-module, where A is an algebra over the algebraically closed field k. There exists a algebra homomorphism, called the* central character *of M*

$$c_M : Z(A) \to \mathsf{k},\ z \mapsto \lambda_z.$$

Proof. It is immediate from the definition of λ_z that c_M is in fact an algebra homomorphism. □

Corollary 3.4. *Let A be a commutative algebra over an algebraically closed field k. Then every simple finite dimensional A-module is one dimensional.*

Proof. Since A is commutative, then $A = Z(A)$. Suppose S is a simple A-module. Then by Proposition 3.3, every $a \in A$ acts by a scalar $c_S(a)$ multiple of the identity. This means that every one dimensional subspace of S is A-stable, which implies that S must be one dimensional. □

In particular, if A is a finite-dimensional commutative k-algebra (algebraically closed k), then all simple A-modules are one dimensional.

Example 3.5. *Let G be a finite abelian group. Then all irreducible representations of G over an algebraically closed field are one dimensional. We saw in Example 3.2 that this is false if the field is not algebraically closed.*

3.3. **The Pontrijagin dual.** Suppose G is a finite abelian group. Then, as a consequence of the Schur Lemma, we now know that every irreducible G-representation is one dimensional, i.e., it is a group homomorphism

$$\rho : G \to GL(\mathbb{C}) = \mathbb{C}^\times.$$

Since these are one-dimensional representations, any two different homomorphisms are in fact non-isomorphic. Notice also that since G is finite, every $g \in G$ has finite order, and so $\rho(g)$ has finite order in $\mathbb{C}^\times$. But then $\rho(g) \in S^1$, where

$$S^1 = \{z \in \mathbb{C}^\times \mid |z| = 1\} \text{ with multiplication}$$

is the circle group. So we may think of these one-dimensional representations as group homomorphisms $\rho : G \to S^1$.

Definition 3.6. *The Pontrijagin dual of G is $\widehat{G} = \{\rho : G \to S^1 \text{ group homomorphism}\}$ endowed with the pointwise product, $(\rho_1 \cdot \rho_2)(g) = \rho_1(g)\rho_2(g)$, $g \in G$. This is group with identity element $\mathbf{1}(g) = 1$ for all g (the trivial representation of G) and inverses $\rho^{-1}(g) = \rho(g^{-1})$ for all $g \in G$.*

In other words, when G is an finite abelian group, the set of isomorphism classes of irreducible G-representations over $\mathbb{C}$ has a natural structure of an abelian group.

Lemma 3.7. *Let G_1 and G_2 be two finite abelian groups and $G_1 \times G_2$ their direct product. Then we have a natural isomorphism $\widehat{G_1 \times G_2} \cong \widehat{G}_1 \times \widehat{G}_2$.*

Proof. Left as an exercise. □

By the fundamental theorem of finitely generated abelian groups, we know that every finite abelian group is a direct product of finite cyclic groups. In light of the previous lemma, we need to understand the dual of C_n, the cyclic group of order n.

Suppose C_n is generated by an element ξ such that $\xi^n = 1$. Fix a primitive n-th root ζ_n of 1 in S^1. For every $m \in \mathbb{Z}$, define

$$\rho_m : C_n \to S^1, \quad \xi \mapsto \zeta_n^m. \tag{3.1}$$

It is clear that $\rho_m = \rho_k$ if and only if $m \equiv k \bmod n$. Hence we have a set of nonisomorphic one-dimensional representations $\{\rho_m : C_n \to S^1 \mid m \in \mathbb{Z}/n\mathbb{Z}\}$.

On the other hand, if $\rho : C_n \to S^1$ is any group homomorphism, it must map ξ to an n-th root of 1, and therefore $\rho = \rho_m$ for some m. This means that

$$\widehat{C}_n \cong \mathbb{Z}/n\mathbb{Z} \tag{3.2}$$

as sets.

Lemma 3.8. $\widehat{C}_n \cong (\mathbb{Z}/n\mathbb{Z}, +) \cong C_n$ *as abelian groups.*

Proof. Of course, we only need to prove the first isomorphism. In other words, we need to check that the set bijection $\mathbb{Z}/n\mathbb{Z} \to \widehat{C}_n$ given by $m \mapsto \rho_m$ is a group homomorphism, or in other words that $\rho_{m+k} = \rho_m \cdot \rho_k$. Since these homomorphims are uniquely determined by their value on ξ, we check:

$$\rho_{m+k}(\xi) = \zeta_n^{m+k} = \zeta_n^m \cdot \zeta_n^k = \rho_m(\xi) \cdot \rho_k(\xi) = (\rho_m \cdot \rho_k)(\xi).$$

□

Proposition 3.9. *There is a (non-canonical) isomorphism as abelian groups $G \cong \widehat{G}$ for any finite abelian group G. In particular, $|\widehat{G}| = |G|$.*

Proof. This is immediate from the previous lemmas and the classification of finite abelian groups. The fact that this isomorphism is non-canonical has to do with the fact that we needed to choose primitive roots on 1 in S^1 in order to construct the one-dimensional representations. □

One should compare the result above with the familiar situation of finite dimensional vector spaces and their duals. Also, just as for finite dimensional vector spaces, we have the following result.

Proposition 3.10. *There is a canonical isomorphism of abelian groups $\widehat{\widehat{G}} \cong G$.*

Proof. Left as exercise (mimic the proof from vector spaces). □

4. Semisimple modules and semisimple algebras

4.1. **Semisimple modules.** Let A be a k-algebra and let M be an A-module.

Definition 4.1. (1) *The module M is called* semisimple *if there exists a family of simple submodules $\{S_i : i \in I\}$ such that $M = \bigoplus_{i\in I} S_i$.*
(2) *We say that M is* completely reducible *if whenever N is a submodule of M, there exists another submodule N' (a complement) such that $M = N \oplus N'$.*

Proposition 4.2. *Suppose M is a finite-dimensional A-module. Then M is semisimple if and only if it is completely reducible.*

Proof. Suppose first that M is completely reducible. If M is simple, then it is semisimple. If not, then let U be a nonzero proper submodule of M. By complete reducibility, there exists a submodule V such that $M = U \oplus V$. Since U and V are both finite dimensional and of strictly smaller dimension than M, by induction we may assume that U and V are both semisimple, and then so is M.

For the converse, let U be a submodule of M, $U \neq M$. We wish to construct a complement for U. Let $\mathcal{C} = \{W \text{ submodule of } M \mid W \cap U = 0\}$. Since $0 \in \mathcal{C}$, then $\mathcal{C} \neq \emptyset$. Moreover, M is finite dimensional, and so there must exist an element V of $\mathcal{C}$ of maximal dimension. If $M = U + V$, then $M = U \oplus V$, so we constructed the complement. Otherwise, write $M = \oplus S_i$, where S_i are simple submodules and there exists a simple submodule $S = S_i$ of M such that $S \not\subset U + V$. Since S is simple, this means that $S \cap (U + V) = 0$. Set $V' = V + S$. We claim that $V' \cap U = 0$ and this leads to the contradiction with the maximality of V since $\dim V' > \dim V$. Indeed, let $u = s + v \in V' \cap U$, then $s = u - v \in U + V$, so $s = 0$ and $u \in V \cap U = 0$. □

Remark 4.3. *Using Zorn's Lemma, one can see that a semisimple module M is completely reducible even when M is infinite dimensional (same proof as above). But we will see in the Appendix that it is possible to have infinite dimensional completely reducible modules (e.g.,* unitary *modules) which are not semisimple. This has to do with the fact that simple submodules may not exist at all in an infinite dimensional reducible module!*

Example 4.4. (1) *If $A = \mathsf{k}$, then A-modules are the same as k-vector spaces. In this case every k-vector space is semisimple (a direct sum of one-dimensional subspaces given by the existence of a basis) and completely reducible (which is the linear algebra fact that every linearly independent subset can be extended to a basis).*
(2) *If $A = M_n(\mathsf{k})$, then A is a direct sum of its column left ideals, so it is a semisimple A-module.*
(3) *If G is a finite group acting transitively on a finite set Ω, then the permutation representation $\mathsf{k}\Omega$, $\mathrm{char}\,\mathsf{k} = p$, is a semisimple $\mathsf{k}G$-module if and only if $p \not| \ |\Omega|$. (Exercise.)*
(4) *A direct sum of semisimple modules is a semisimple module.*

Here are the first easy properties.

Lemma 4.5. *If M is a completely reducible A-module, then every submodule and every quotient of M are completely reducible modules.*

Proof. Let N be a submodule of M and U a submodule of N. Then U is a submodule of M and there exists a submodule V of M such that $M = U \oplus V$. We claim that $N = U \oplus (V \cap N)$. Firstly, $U \cap (V \cap N) = (U \cap V) \cap N = 0 \cap N = 0$. Secondly, if $n \in N$, then $n \in U \oplus V$, so we may write $n = u + v$. But then $v = n - u \in N$ since $U \subset N$.

For quotients, let N be a submodule of M. As M is completely reducible, there exists N' submodule of M such that $M = N \oplus N'$. But then $M/N \cong N'$ and this is completely reducible as we have just proved. □

4.2. **Semisimple algebras. From now on, unless explicitly stated otherwise, the algebra A is assumed to be finite dimensional.** By the equivalence between complete reducibility and semisimplicity, the same claims in Lemma 4.5 hold for semisimple A-modules.

Definition 4.6. *An algebra A is called* semisimple *if it is semisimple as an A-module.*

Example 4.7. *If $A = M_n(\mathsf{k})$, then A is semisimple.*

A particular case is the following. If A is a semisimple algebra and I is a left ideal of A, then I is an A-submodule, hence both A and A/I are semisimple A-modules.

Proposition 4.8. *A is semisimple if and only if every finite-dimensional A-module is semisimple.*

Proof. The 'only if' part is clear since A itself is a finite-dimensional A-module.

For the other implication, suppose M is a finite-dimensional A-module. Fix a k-basis of M, $\{m_1, \dots, m_\ell\}$ of M. Define

$$f : \underbrace{A \oplus \cdots \oplus A}_{\ell \text{ copies}} \to M,\ (a_1, \dots, a_\ell) \mapsto \sum a_i \cdot m_i.$$

This is an A-linear map: for every $a \in A$,

$$f(a((a_1, \dots, a_\ell)) = f((aa_1, \dots, aa_\ell)) = \sum (aa_i) \cdot m_i = a \sum a_i m_i = af((a_1, \dots, a_\ell)).$$

The map f is also clearly surjective since every element of M is a k-linear combination of the $\{m_i\}$. The direct sum of copies of A is a semisimple A-module. By the first isomorphism theorem, M is isomorphic to a quotient of this direct sum, hence it is also semisimple. □

Lemma 4.9. *(1) Let A be a semisimple algebra and I a two-sided ideal of A. Then the algebra $B = A/I$ is semisimple.*

(2) Let A_1, A_2 be k-algebras. Then $A_1 \times A_2$ is semisimple if and only if A_1 and A_2 are semisimple.

Proof. (1) Let V be a finite dimensional B-module. Then we may regard V as a finite-dimensional A-module such that $I \cdot V = 0$. Let U be a B-submodule of V (which we can identify with an A-submodule of V such that $I \cdot U = 0$.) Since A is semisimple, there exists a complement W, an A-submodule of V, such that $V = U \oplus W$ as A-modules. But since $W \subset V$, we also have $I \cdot W = 0$, so W can be viewed as a B-module, hence we found a B-complement of U.

(2) Exercise. □

4.3. **Artin-Wedderburn Theorem.** This is an important result which gives a description of finite dimensional semisimple algebras. We are only concerned with the case when the field k is algebraically closed.

Theorem 4.10. *Let A be a (finite dimensional) k-algebra, where k is algebraically closed. Then A is semisimple if and only if*

$$A \cong M_{n_1}(\mathsf{k}) \times \dots M_{n_s}(\mathsf{k}),$$

for a unique set of integers $n_1, \dots, n_s \in \mathbb{N}$.

Proof. The proof is non-examinable. We will not give a complete proof, but only explain the ideas. You can find a complete proof in many texts, for example, in [1].

The starting point is to recall from Proposition 1.10 that $A \cong \mathrm{End}_A(A)^{\mathsf{op}}$ as k-algebras. If we show that $\mathrm{End}_A(A)$ is a product of matrix algebras, then so is $\mathrm{End}_A(A)^{\mathsf{op}}$ (since a matrix algebra is isomorphic to its opposite), so the claim follows for A.

To avoid potential confusion, let's replace A by some arbitrary finite dimensional A-module M. Then M is semisimple and write $M = \sum_{i=1}^{\ell} S_i$, where S_i are simple A-modules. (At the end, we can can specialise $M = A$.) Recall that $\mathrm{End}_A(M)$ is an algebra of A-homomorphisms with composition. By the easy part of Schur's Lemma, there are no nozero A-homomorphisms between S_i and S_j unless $S_i \cong S_j$. So group together the S_i's according to isomorphism classes and identify the isomorphic copies of the same simple module. So we write

$$M = \oplus_{j=1}^{s} (\underbrace{S_{i_j} \oplus \cdots \oplus S_{i_j}}_{n_j \text{ times}}).$$

Then, using that there are no nonzero homomorphisms between nonisomorphic simple modules:

$$\mathrm{End}_A(M) = \prod_{j=1}^{s} \mathrm{End}_A(\underbrace{S_{i_j} \oplus \cdots \oplus S_{i_j}}_{n_j \text{ times}})$$

as algebras. This reduces the problem to describing the algebra

$$\mathrm{End}_A(\underbrace{S \oplus \cdots \oplus S}_{n \text{ times}}) \tag{4.1}$$

where S is a simple A-module. (Notice that so far we have not used that k is algebraically closed.) To orient ourselves and see how matrix algebras will appear, think of the simplest case $A = \mathsf{k}$ and $S = \mathsf{k}$, then $\mathrm{End}_{\mathsf{k}}(\mathsf{k}^n) = M_n(\mathsf{k})$.

Now we assume that k is algebraically closed. We claim that

$$\mathrm{End}_A(\underbrace{S \oplus \cdots \oplus S}_{n \text{ times}}) \cong M_n(\mathsf{k}). \tag{4.2}$$

We use the second part of Schur's Lemma, which says that $\mathrm{End}_A(S) \cong \mathsf{k}$. To distinguish between the copies of S, write S^i for the i-th copy of S, $1 \le i \le n$. Suppose $\phi : \oplus_{i=1}^{n} S^i \to \oplus_{i=1}^{n} S^i$ is an A-linear map. Consider the restriction

$$\phi_{S^j} : S^j \to \oplus_{i=1}^{n} S^i \to S^i$$

where the last map is the projection p_i onto the S^i term. The composition is then a map $\phi_{i,j} : S^j \to S^i$. Identifying both S^i and S^j with S, we can think of $\psi_{i,j}$ as an element of $\mathrm{End}_A(S)$. But this is a scalar multiple of the identity, say the scalar is $a_{ij} \in \mathsf{k}$. This defines an asisgnment

$$\mathrm{End}_A(\underbrace{S \oplus \cdots \oplus S}_{n \text{ times}}) \to M_n(\mathsf{k}), \quad \phi \to (a_{ij}),$$

which is the desired isomorphism. (One needs to check that composition in the left hand side corresponds to matrix multiplication in the right hand side, but this is not hard.) $\square$

Example 4.11. *The theorem as stated is false if one drops the assumption* k *algebraically closed. For example, consider* $\mathbb{H}$ *the algebra of real quaternions*

$$\mathbb{H} = \mathbb{R}\langle i, j, k \mid i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j\rangle.$$

This is a division algebra and in particular, it has no left ideals, meaning that $\mathbb{H}$ *is a simple (hence semisimple) algebra. Clearly,* $\dim_{\mathbb{R}} \mathbb{H} = 4$*, so if the Artin-Wedderburn Theorem were to hold as stated, we would have* $\mathbb{H} \cong M_2(\mathbb{R})$ *or* $\mathbb{H} \cong_1 (\mathbb{R})^4$*. But these are both false, the first because* $M_2(\mathbb{R})$ *is not a division algebra and the second because* $\mathbb{H}$ *is not commutative.*

Corollary 4.12. *Let* A *be a finite dimensional semisimple* k*-algebra,* $A \cong \prod_{i=1}^{s} M_{n_i}(\mathsf{k})$*. Then*

(1) A has exactly s simple modules (up to isomorphism) $M_1, \ldots, M_s$ *such that* $\dim_{\mathsf{k}} M_i = n_i$*.*
(2) The integer s equals the dimension $\dim_{\mathsf{k}} Z(A)$*.*
(3) $\dim_{\mathsf{k}} A = n_1^2 + \ldots n_s^2 = \sum_{i=1}^{s} (\dim_{\mathsf{k}} M_i)^2$*.*

Proof. All of these claims follow immediately from Theorem 4.10. For (1), we use the fact that each $M_{n_i}(\mathsf{k})$ has a unique simple module $V_i = \mathsf{k}^{n_i}$. In fact, using the semisimplicity of $M_{n_i}(\mathsf{k})$, we may write $M_{n_i}(\mathsf{k}) = \oplus_{r=1}^{n_i} V_i^r$, where V_i^r is the space of $n_i \times n_i$ matrices with 0 everywhere except on the r-th column. Clearly $V_i^r \cong V_i$ for all r. Then, as A-modules:

$$A \cong \oplus_{i=1}^{s} \oplus_{r=1}^{n_i} V_i^r.$$

This defines a composition series of A composition factors isomorphic to $\{V_i^r \mid 1 \leq i \leq s,\ 1 \leq r \leq n_i\}$. In this set, for every fixed i, $V_i^r \cong V_i^{r'} \cong \mathsf{k}^{n_i}$. Moreover, if $i \neq j$, then $V_i^r \not\cong V_j^{r'}$. To see this, consider the element $a_i \in A$ corresponding to $(0, \dots, 0, \mathrm{Id}_{n_i}, 0, \dots, 0) \in \prod_{i=1}^s M_{n_i}(\mathsf{k})$. Then a_i acts by the identity on V_i^r, but it acts by 0 on $V_j^{r'}$. Since every simple A-module (up to isomorphism) must appear in every composition series of A, we conclude that A has s nonisomorphic simple modules of dimensions n_i.

(2) We have $Z(A) \cong Z(\prod_{i=1}^s M_{n_i}(\mathsf{k})) = \prod_{i=1}^s Z(M_{n_i}(\mathsf{k})) = \prod_{i=1}^s \mathsf{k}\,\mathrm{Id}_{n_i} \cong \mathsf{k}^s$. This means that $\dim_{\mathsf{k}} Z(A) = s$.

(3) The first equality is immediate since $\dim M_{n_i}(\mathsf{k}) = n_i^2$. The second one now follows from (1). □

4.4. **Maschke's Theorem.** We would like to apply Theorem 4.10 to finite groups.

Theorem 4.13. *Let G be a finite group and k a field. The algebra $\mathsf{k}G$ is semisimple if and only if char$\mathsf{k} \not| \, |G|$. In particular, $\mathbb{C}G$ is semisimple.*

Proof. Suppose that char $\mathsf{k} \not| \, |G|$. Then $|G$ is invertible in k. Let $U \subset \mathsf{k}G$ be a submodule. We want to find a complement V which is a $\mathsf{k}G$-submodule. As k-vector spaces, there exists V' such that $\mathsf{k}G = U \oplus V'$ as k-vector spaces.

Let $f : \mathsf{k}G \to U$ be the projection $f(u) = u$, $f(v') = v'$. This is only k-linear! We want to define a $\mathsf{k}G$-linear projection. This is possible since we can average over G:

$$\phi : \mathsf{k}G \to U,\ \phi(x) = \frac{1}{|G|} \sum_{g \in G} g \cdot f(g^{-1} \cdot x),\ x \in \mathsf{k}G. \tag{4.3}$$

For every $h \in G$,

$$\phi(h \cdot x) = \frac{1}{|G|} \sum_{g \in G} g \cdot f(g^{-1} h \cdot x) = \frac{1}{|G|} \sum_{g_1 \in G} (hg_1) \cdot f(g_1^{-1} \cdot x) = h \cdot \phi(x),$$

where we made the change of variable $g_1 = h^{-1} g$. This means that ϕ is G-linear and hence $\mathsf{k}G$-linear. Now ϕ is also surjective because

$$\phi(u) = \frac{1}{|G|} \sum_{g \in G} g \cdot f(g^{-1} \cdot u) = \frac{1}{|G|} \sum_{g \in G} g \cdot g^{-1} \cdot u = u,\ u \in U.$$

Define $V = \ker \phi$ which is a $\mathsf{k}G$-submodule. Because of the rank-nullity theorem (over k), $\dim \mathsf{k} = \dim U + \dim V$. Moreover, if $x \in U \cap V$, then $\phi(x) = x$ (because $x \in U$) and $\phi(x) = 0$ (because $x \in V$). Hence $U \cap V = 0$. This means that $\mathsf{k}G = U \oplus V$ which shows that $\mathsf{k}G$ is completely reducible, hence semisimple.

For the converse, recall the exercise that when $p \mid \mathrm{char}\mathsf{k}$ then $\mathsf{k}G$ has a one-dimensional submodule $U = \mathsf{k}\langle \sum_{g \in G} g \rangle$ which does not have a complement. □

Corollary 4.14. *Suppose that k is algebraically closed of characteristic p and $p \not| |G|$. Then $\mathsf{k}G$ has exactly s nonisomorphic simple modules, where s is the number of conjugacy classes. If $n_1, \dots, n_s$ are the dimensions of the simple modules, then*

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

Proof. Via Maschke's Theorem, we may apply the Artin-Wedderburn Theorem, more precisely Corollary 4.12. Then the only remaining thing is to remark that the centre $Z(\mathsf{k}G)$ is spanned by $\delta_C = \sum_{g \in C} g$, where C ranges over the conjugacy classes of G. Hence $\dim_{\mathsf{k}} Z(\mathsf{k}G)$ equals the number of conjugacy classes in G. □

Remark 4.15. *In the appendix, we will give another proof of Maschke's Theorem when $\mathsf{k} = \mathbb{C}$, using the notion of unitary representations.*

Example 4.16. *If $G = C_p$ and k has characteristic p, then Maschke's Theorem says that $\mathsf{k}C_p$ is not semisimple. In this case, one can see directly that the only simple $\mathsf{k}C_p$ module is the trivial (one-dimensional) module.*

5. More linear algebra: tensor products

5.1. **Duals.** Let k be a field. If V and W are k-vector spaces, we denote by

$$V^* = \{f : V \to \mathsf{k} \mid f \text{ is } \mathsf{k}\text{-linear}\} \tag{5.1}$$

the dual k-vector space and by

$$\mathrm{Hom}_{\mathsf{k}}(V, W) = \{\phi : V \to W \mid \phi \text{ is } \mathsf{k}\text{-linear}\} \tag{5.2}$$

the k-vector space of linear maps between V and W. Of course, $\mathrm{Hom}_{\mathsf{k}}(V, W) = V^*$. Moreover, we use the notation $\mathrm{End}_{\mathsf{k}}(V) = \mathrm{Hom}_{\mathsf{k}}(V, V)$ for the k-vector space of endomorphisms of V. You may recall that $\mathrm{End}_{\mathsf{k}}(V)$ is in fact a k-algebra under composition of linear maps.

If V is finite dimensional with basis $\{e_i : 1 \le i \le n\}$, then a dual basis of V^* is defined by

$$\{f_i : 1 \le i \le n\},\ f_i(e_j) = \delta_{ij},\ 1 \le i, j \le n.$$

It is easy to check that this is indeed a basis of V^*.

In such a case, one may say that V and V^* are isomorphic, since any two vector spaces with the same dimension are, but this isomorphism is not natural (or "canonical"), since it depends on the choice of basis for V.

Exercise 5.1. *Prove that there is always a natural injective linear map $V \to (V^*)^*$. Deduce that this is a natural isomorphism when V is finite dimensional. (When V is infinite dimensional, the dimension of V^* is strictly larger than that of V.)*

5.2. **Direct products and sums.** If $\{V_i\}_{i \in I}$ is a family of k-vector spaces, define the direct product

$$\prod_{i \in I} V_i = \{(v_i),\ i \in I\} \tag{5.3}$$

and the direct sum

$$\bigoplus_{i \in I} V_i = \{(v_i),\ i \in I \mid v_i = 0 \text{ except for finitely many } i\}. \tag{5.4}$$

Both are k-vector spaces under the coordinate sum and scalar multiplication, i.e.,

$$(v_i)_{i \in I} + (v'_i)_{i \in I} = (v_i + v'_i)_{i \in I}, \quad \lambda(v_i)_{i \in I} = (\lambda v_i)_{i \in I},\ \lambda \in \mathsf{k}.$$

In general, $\bigoplus_{i \in I} V_i$ is a k-linear subspace of $\prod_{i \in I} V_i$. When I is a finite set, then $\bigoplus_{i \in I} V_i = \prod_{i \in I} V_i$. If V has basis $\{e_i\}$ and W_i has basis $\{e'_i\}$, then $V \oplus W$ has basis $\{(e_i, 0)\} \cup \{(0, e'_i)\}$. In particular,

$$\dim(V \oplus W) = \dim V + \dim W.$$

5.3. **Tensor products.** Suppose V and W are two k-vector spaces. We define the tensor product $V \otimes W$ as follows. Let M be the k-vector space with basis (v, w) for all $v \in V$, $w \in W$. Notice that this a huge vector space, for example even when V and W are finite dimensional, M is infinite-dimensional as long as k is infinite. Let N be the vector subspace of M spanned by all elements of the form

$$(v_1 + v_2, w) - (v_1, w) - (v_2, w), \quad (v, w_1 + w_2) - (v, w_1) - (v, w_2),$$
$$\lambda(v, w) - (\lambda v, w), \quad \lambda(v, w) - (v, \lambda w),$$

$v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$, and $\lambda \in \mathsf{k}$.

Definition 5.2. *The tensor product is the vector space $V \otimes W = M/N$. Denote by $v \otimes w$ the image of (v, w) in $V \otimes W$.*

Lemma 5.3. *The tensor product space $V \otimes W$ is spanned by the simple tensors $v \otimes w$, meaning that every element in $V \otimes W$ is a finite sum of simple tensors. Moreover, the simple tensors satisfy the following bilinear properties:*

(i) $(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$;
(ii) $v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$;
(iii) $\lambda(v \otimes w) = (\lambda v) \otimes w = v \otimes (\lambda w)$.

Proof. Straightforward from the definition. □

Another way to phrase the properties in the lemma above is to say that the natural map $p : V \times W \to V \otimes W$, $(v, w) \mapsto v \otimes w$ is bilinear. The tensor product satisfies the following universal property.

Lemma 5.4. *Let U is a k-vector space with a bilinear map $\phi : V \times W \to U$. Then there exists a unique k-linear map $\widetilde{\phi} : V \otimes W \to U$ such that $\phi = \widetilde{\phi} \circ p$.*

In light of this lemma, we may think of $V \otimes W$ as the "largest" vector space which has the bilinearity properties from the definition. It is also easy to prove the following lemma.

Lemma 5.5. *If $\{v_i : i \in I\}$ and $\{w_j : j \in J\}$ are bases for V and W, respectively, then $\{v_i \otimes w_j : i \in I, j \in J\}$ is a basis of $V \otimes W$. In particular,*

$$\dim(V \otimes W) = \dim V \cdot \dim W.$$

Exercise 5.6. *Prove Lemmas 5.4 and 5.5.*

Proposition 5.7. *Let V, W be k-vector spaces and suppose that V is finite dimensional. Then the map*

$$\tau : V^* \otimes W \to \mathrm{Hom}_{\mathsf{k}}(V, W),\ f \otimes w \mapsto (\phi : V \to W,\ \phi(v) = f(v)w),$$

is a linear isomorphism.

Proof. To begin, notice that τ is well defined since the assignment $(v, w) \to f(v)w$ is bilinear. We also emphasize that we have only defined τ on the simple tensors, but one extends the definition to a finite sum of simple tensors in the obvious way, by summing up the corresponding images of simple tensors.

The inverse map is not constructed naturally, we need to fix a basis of V. Let $\{e_i : 1 \le i \le n\}$ be a basis of V and let $\{f_i : 1 \le i \le n\}$ be the dual basis of V^*. Define

$$\eta : \mathrm{Hom}_{\mathsf{k}}(V, W) \to V^* \otimes W,\ \phi \mapsto \sum_{i=1}^{n} f_i \otimes \phi(e_i).$$

We verify directly that τ and η are inverses to each other:

$$\begin{aligned}
(\eta \circ \tau)(f \otimes w) = \eta(\phi) &= \sum_{i=1}^{n} f_i \otimes \phi(e_i), \quad (\text{where } \phi = \tau(f \otimes w)) \\
&= \sum_{i=1}^{n} f_i \otimes f(e_i)w = (\sum_{i=1}^{n} f(e_i)f_i) \otimes w = f \otimes w; \\
(\tau \circ \eta)(\phi)(v) &= \tau(\sum_{i=1}^{n} f_i \otimes \phi(e_i))(v) = \sum_{i=1}^{n} f_i(v)\phi(e_i) \\
&= \phi(\sum_{i=1}^{n} f_i(v)e_i) = \phi(v).
\end{aligned}$$

□

6. Characters

If G is a group, recall that a representation of G over k is a pair (ρ, V), where V is a k-vector space and $\rho : G \to GL(V)$ is a group homomorphism.

6.1. **Basics.** We define characters.

Definition 6.1. *Let (ρ, V) be a finite dimensional representation of G. The character of the representation is the function $\chi_\rho : G \to \mathsf{k}$ (or we may also denote it by χ_V) defined by*

$$\chi_\rho(g) = \mathrm{tr}\, \rho(g).$$

Notice that we need V to be finite dimensional for the definition to make sense. (There are various notions of characters for infinite dimensional representations, but there are more complicated.) From now on, we assume that the representations are finite dimensional, unless stated otherwise. The following properties are immediate.

Lemma 6.2. *Let (ρ, V) be a G-representation.*

(i) *If (ρ_1, V_1) and (ρ_2, V_2) are equivalent representations, then $\chi_{\rho_1} = \chi_{\rho_2}$.*
(ii) *$\chi_\rho(e) = \dim V$, where e is the identity element of G.*
(iii) *For every $g, h \in G$, $\chi_\rho(hgh^{-1}) = \chi_\rho(g)$.*
(iv) *Suppose that $\mathsf{k} = \mathbb{C}$ and $g \in G$ has finite order. (This is automatic when G is finite.) Then $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$, where denotes complex conjugation.*

Proof. (i) By definition, ρ_1 and ρ_2 are equivalent if there exists a k-linear isomorphism $T : V_1 \to V_2$ such that $\rho_1(g) = T^{-1} \circ \rho_2(g) \circ T$ for all g. Since $\operatorname{tr}(A^{-1}BA) = \operatorname{tr}(B)$ for any linear maps A, B, the claim follows.

(ii) This is clear since $\rho(e) = \mathrm{Id}_V$.

(iii) Since $\rho(hgh^{-1}) = \rho(h) \circ \rho(g) \circ \rho(h)^{-1}$, this follows again from the invariance of the trace under conjugation.

(iv) Since $\mathbb{C}$ is algebraically closed, $\rho(g)$ has n eigenvalues (counted with multiplicity), if $n = \dim V$, say $\lambda_1, \dots, \lambda_n$. If $g^m = e \in G$, it follows that $\lambda_i^m = 1$ for all i. This means that λ_i are roots of unity and therefore $\lambda_i^{-1} = \overline{\lambda}_i$. On the other hand, the eigenvalues of $\rho(g^{-1})$ are $\lambda_1^{-1}, \dots, \lambda_n^{-1}$. So $\chi_\rho(g^{-1}) = \sum \lambda_i^{-1} = \sum \overline{\lambda}_i = \overline{\chi_\rho(g)}$. □

It is often tedious and confusing to write the homomorphism ρ as part of the representation. We may write

$$g \cdot v \text{ in place of } \rho(g)v, \quad g \in G, v \in V,$$

in other words, using the same notation as for group actions.

Suppose that V and W are G-representations (not necessarily finite-dimensional). We may define representations of G on:

(1) $V \oplus W$ via $g \cdot (v, w) = (g \cdot v, g \cdot w)$;
(2) V^* via $(g \cdot f)(v) = f(g^{-1} \cdot v)$, where $f \in V^*$, $v \in V$, $g \in G$;
(3) $V \otimes W$ via $g \cdot (v \otimes w) = (g \cdot v) \otimes (g \cdot w)$.

It is straightforward to check that these are indeed representations. A little more subtle is to define a structure of G-representation on $\mathrm{Hom}_{\mathsf{k}}(V, W)$. To emphasize the actions, let (ρ, V) and (μ, W) be the corresponding representations. Then we define a representation ν on $\mathrm{Hom}_{\mathsf{k}}(V, W)$ by

$$(\nu(g)\phi)(v) = \mu(g)\phi(\rho(g^{-1})v), \text{ or, more simply, } (g \cdot \phi)(v) = g \cdot \phi(g^{-1} \cdot v). \tag{6.1}$$

Proposition 6.3. *The k-linear isomorphism $\tau : V^* \otimes W \to \mathrm{Hom}_{\mathsf{k}}(V, W)$ from Proposition 5.7 is G-linear, and therefore $V^* \otimes W \cong \mathrm{Hom}_{\mathsf{k}}(V, W)$ as G-representations.*

Proof. This is a direct verification:

$$\tau(g \cdot (f \otimes w))(v) = \tau(g \cdot f \otimes g \cdot w)(v) = (g \cdot f)(v)(g \cdot w) = f(g^{-1} \cdot v)(g \cdot w).$$

On the other hand, if $\phi = \tau(f \otimes w)$, then

$$(g \cdot \phi)(v) = g \cdot \phi(g^{-1} \cdot v) = g \cdot (f(g^{-1}v)w) = f(g^{-1} \cdot v)(g \cdot w),$$

where in the last step, we used that $f(g^{-1} \cdot v)$ is a scalar. We see that the two results are the same. □

Lemma 6.4. *Suppose that V and W are G-representations. Then for every $g \in G$:*

(i) $\chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g)$;
(ii) $\chi_{V \otimes W}(g) = \chi_V(g) \cdot \chi_W(g)$;
(iii) $\chi_{V^*}(g) = \chi_V(g^{-1})$.

Proof. Left as exercise. □

6.2. **A fixed point formula.** We assume from now on that G is finite. Suppose that U is a G-representation. We define subspace of G-fixed points

$$U^G = \{u \in U \mid g \cdot u = u, \text{ for all } g \in G\}. \tag{6.2}$$

This is a subrepresentation of U, and in fact it built out of copies of the trivial representation: clearly, for every $u \in U^G$, $g \cdot u = u$ for all g.

Proposition 6.5 (Fixed point formula)**.** *Suppose that $|G|$ is invertible in k. Then*

$$\dim U^G = \frac{1}{|G|}\sum_{g\in G}\chi_U(g).$$

Proof. Define $\psi : U \to U$ by

$$\psi(u) = \frac{1}{|G|}\sum_{g\in G} g\cdot u.$$

Then $\operatorname{im}\psi \subseteq U^G$ because

$$h\cdot\psi(u) = \frac{1}{|G|}\sum_{g\in G} hg\cdot u = \frac{1}{|G|}\sum_{g'\in G} g'\cdot u = \psi(u),$$

where $g' = hg$. On the other hand, if $u \in U^G$, then

$$\psi(u) = \frac{1}{|G|}\sum_{g\in G} g\cdot u = \frac{1}{|G|}\sum_{g\in G} u = \frac{|G|}{|G|}u = u.$$

We have seen this trick already in the proof of Maschke's Theorem. This means that ψ is a projection of U onto U^G. But then

$$\dim U^G = \operatorname{tr}(\psi) = \frac{1}{|G|}\sum_{g\in G}\operatorname{tr}(g\cdot) = \frac{1}{|G|}\sum_{g\in G}\chi_U(g).$$

□

We denote by $\operatorname{Hom}_G(V,W)$ the space of G-linear maps (G-homomorphisms) between the G-representations V and W. This is a subrepresentation of $\operatorname{Hom}_{\mathsf{k}}(V,W)$, but in fact:

Lemma 6.6. $\operatorname{Hom}_{\mathsf{k}}(V,W)^G = \operatorname{Hom}_G(V,W)$.

Proof. This is simply a matter of unravelling the definitions. A k-linear map $\phi \in \operatorname{Hom}_{\mathsf{k}}(V,W)$ belongs to $\operatorname{Hom}_{\mathsf{k}}(V,W)^G$ if and only if for every $g \in G$, $g\cdot\phi = \phi$. But this means $(g\cdot\phi)(v) = \phi(v)$, or equivalently $g\cdot\phi(g^{-1}\cdot v) = \phi(v)$, or $\phi(g^{-1}\cdot v) = g^{-1}\cdot\phi(v)$. Since this condition holds for all g, we may change g for g^{-1}, and hence $\phi(g\cdot v) = g\cdot\phi(v)$ for all g and v. But this is precisely the definition of G-linear maps. □

Corollary 6.7. *Let V, W be G-representations. Then*

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

Proof. By Lemma 6.6, $\dim\operatorname{Hom}_G(V,W) = \dim\operatorname{Hom}_{\mathsf{k}}(V,W)^G$. We apply the fixed point formula to $U = \operatorname{Hom}_{\mathsf{k}}(V,W)$ and it follows that

$$\dim\operatorname{Hom}_G(V,W) = \frac{1}{|G|}\sum_{g\in G}\chi_{\operatorname{Hom}_{\mathsf{k}}(V,W)}(g).$$

Now, by Proposition 6.3, $\operatorname{Hom}_{\mathsf{k}}(V,W) \cong V^*\otimes W$ as G-representations and so $\chi_{\operatorname{Hom}_{\mathsf{k}}(V,W)}(g) = \chi_{V^*\otimes W}(g)$. Finally, we have seen that $\chi_{V^*\otimes W}(g) = \chi_{V^*}(g)\chi_W(g) = \chi_V(g^{-1})\chi_W(g)$. The corollary is proved.

□

6.3. **The character pairing.** Let $\mathcal{C}_{\mathsf{class}}(G)$ denote the k-vector space of class functions, i.e., the functions $f : G \to \mathsf{k}$ that are constant on the conjugacy classes of G: $f(hgh^{-1}) = f(g)$ for all $h, g \in G$. As noted before, $\chi_V \in \mathcal{C}_{\mathsf{class}}(G)$ for all G-representations V.

Definition 6.8. *Define the pairing $\langle\ ,\ \rangle$ on $\mathcal{C}_{\mathsf{class}}(G)$:*

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{g\in G} f_1(g^{-1})f_2(g).$$

Lemma 6.9. *The pairing $\langle\ ,\ \rangle$ is symmetric and bilinear.*

Proof. The bilinearity in f_1 and f_2 is clear. The symmetry $\langle f_1, f_2\rangle = \langle f_2, f_1\rangle$ follows by changing g to g^{-1} in the summation. □

If C is a conjugacy class in G, we denote by δ_C the function which is 1 on each element of C, and 0 everywhere else. It is immediate that $\{\delta_C : C \text{ conjugacy class in } G\}$ is a k-basis of $\mathcal{C}_{\mathsf{class}}(G)$.

If g_1 and g_2 are conjugate, then so are g_1^{-1} and g_2^{-1}. If C is the conjugacy class of g, denote by C^{-1} the conjugacy class of g^{-1}. Then $|C| = |C^{-1}|$. Suppose C and C' are two conjugacy classes. We calculate

$$\begin{aligned}\langle \delta_C, \delta_{C'} \rangle &= \frac{1}{|G|} \sum_{g \in G} \delta_C(g^{-1}) \delta_{C'}(g) = \frac{1}{|G|} \sum_{g \in C' \cap C^{-1}} 1 = \frac{|C' \cap C^{-1}|}{|G|} \\ &= \begin{cases} \frac{|C|}{|G|}, & \text{if } C' = C^{-1}, \\ 0, & \text{otherwise.} \end{cases}\end{aligned} \tag{6.3}$$

Finally, we have the first important result. Recall that we assume that G is finite, $|G|$ is invertible in k and the representations are finite dimensional.

Theorem 6.10. *Let V, W be G-representations. Then*

$$\langle \chi_V, \chi_W \rangle = \dim \operatorname{Hom}_G(V, W). \tag{6.4}$$

Proof. This follows immediately now from Corollary 6.7 and the definition of $\langle\ ,\ \rangle$. $\square$

Corollary 6.11. *Suppose V and W are irreducible G-representations.*

(i) If $V \ncong W$, then $\langle \chi_V, \chi_W \rangle = 0$.
(ii) If $V = W$ and k is algebraically closed, then $\langle \chi_V, \chi_V \rangle = 1$.

Proof. By the first part of Schur's Lemma, $\operatorname{Hom}_G(V, W) = 0$ when $V \ncong W$. By the second part of Schur's Lemma, $\operatorname{End}_G(V)$ is one-dimensional when k is algebraically closed. $\square$

Corollary 6.12. *Suppose that k is algebraically closed and that $|G|$ is invertible in k. Then the set $\{\chi_V\}$ where V ranges over the irreducible G-representations (up to isomorphism) is an orthonormal basis of $\mathcal{C}_{\mathsf{class}}(G)$ with respect to $\langle\ ,\ \rangle$.*

Proof. By Corollary 6.11, we see that $\{\chi_V\}$, where V ranges over the irreducible G-representations (up to isomorphism), is an orthonormal set in $\mathcal{C}_{\mathsf{class}}(G)$. In particular, it is a linearly independent set. From Maschke's Theorem, we know that under the assumptions on k, $\mathsf{k}G$ is a (finite-dimensional) semisimple algebra. Hence by the Artin-Wedderburn Theorem, we know that there are as many irreducible G-representations as there are conjugacy classes of G. This means that $\{\chi_V\}$ is a maximal linearly independent set, hence a basis. $\square$

Remark 6.13. *Suppose that $\mathsf{k} = \mathbb{C}$. Then $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ as we have seen. Because of this, it is more customary in this case to define the pairing $\langle\ ,\ \rangle$ in $\mathcal{C}_{\mathsf{class}}(G)$ by:*

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)} f_2(g).$$

Notice that this doesn't make any difference for $\langle \chi_V, \chi_W \rangle$, hence the orthogonality results hold equally well with this pairing. But it makes a difference for arbitrary class functions f_1, f_2. More precisely, this form is not symmetric, but it is hermitian:

$$\langle f_1, f_2 \rangle = \overline{\langle f_2, f_1 \rangle},$$

as it can be seen immediately. It is not bilinear, but sesquilinear, i.e., conjugate-linear in the first variable, and linear in the second. But it is positive definite too, which is why we prefer to use it when $\mathsf{k} = \mathbb{C}$:

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

with equality if and only if $f = 0$.

6.4. **Character tables.** Assume from now on that $\mathsf{k} = \mathbb{C}$. Let $\{C_1, \dots, C_n\}$ be the conjugacy classes of G, and $\{\chi_1, \dots, \chi_n\}$ be the characters of inequivalent irreducible G-representations. The inner product on $\mathcal{C}_{\mathsf{class}}(G)$ can be rewritten as:

$$\langle f_1, f_2 \rangle = \sum_{j=1}^{n} \frac{|C_j|}{|G|} \overline{f_1(C_j)} f_2(C_j), \tag{6.5}$$

where for $f \in \mathcal{C}_{\mathsf{class}}(G)$, and C a conjugacy class, $f(C)$ denotes the common value $f(g)$ for $g \in C$. Then the orthogonality relation that we have just proven says that:

$$\sum_{j=1}^{n} \frac{|C_j|}{|G|} \overline{\chi_{i_1}(C_j)} \chi_{i_2}(C_j) = \delta_{i_1, i_2}. \tag{6.6}$$

Definition 6.14. *The character table of G is the finite square matrix $A = (a_{ij})$ where $a_{ij} = \chi_i(C_j)$.*

If we denote by D the diagonal matrix with diagonal entries $(d_j : j = 1, \dots, n)$,

$$d_j = \frac{|C_j|}{|G|},$$

then the orthogonality of characters can be rewritten as

$$\overline{A} \cdot D \cdot A^t = I, \tag{6.7}$$

where I is the identity matrix.

Lemma 6.15. *If $\overline{B} \cdot B^t = I$, then $B^t \cdot \overline{B} = I$.*

Proof. This is clear since the first relation implies that $B^t = (\overline{B})^{-1}$. $\square$

Set $B = A \cdot D^{1/2}$ where $D^{1/2}$ is the diagonal matrix whose diagonal entries are $\sqrt{d_j}$. The equation (6.7) says that $\overline{B} \cdot B^t = I$ and hence $B^t \cdot \overline{B} = I$. Translating back we get $D^{1/2} A^t \overline{A} D^{1/2} = I$, and therefore

$$A^t \cdot A = D^{-1}. \tag{6.8}$$

Expressing this in terms of the columns of A we arrive at the second orthogonality relation.

Proposition 6.16. *The columns of the character table are orthogonal, more precisely*

$$\sum_{i=1}^{n} \overline{\chi_i(C_{j_1})} \chi_i(C_{j_2}) = \begin{cases} \frac{|G|}{|C_{j_1}|}, & \text{if } C_{j_1} = C_{j_2}, \\ 0, & \text{otherwise.} \end{cases}$$

6.5. **Examples.** The following situation appears quite often. Let G act on a finite set Ω and define the permutation G-representation on $\mathsf{k}\Omega$:

$$g \cdot \sum_{\omega \in \Omega} \lambda_\omega \omega = \sum_{\omega \in \Omega} \lambda_\omega (g \cdot \omega).$$

Lemma 6.17. *The character of a permutation representation is*

$$\chi_{\mathsf{k}\Omega}(g) = |\Omega^g|, \quad g \in G,$$

where $\Omega^g = \{\omega \in \Omega \mid g \cdot \omega = \omega\}$.

Proof. By definition $\chi_{\mathsf{k}\Omega}(g)$ is the trace of the action of g on $\mathsf{k}\Omega$. But a basis of $\mathsf{k}\Omega$ is precisely Ω, and so the matrix of the action of g is a permutation matrix with the 1's on the diagonal coming precisely from Ω^g. $\square$

Example 6.18. *Let $\Omega_n = \{e_1, \dots, e_n\} \cong \mathsf{k}^n$ and $G = S_n$ acting by usual permutation of indices. Then*

$$\chi_{\mathsf{k}\Omega_n}(\sigma) = |\{i \mid \sigma(i) = i,\ 1 \le i \le n\}|.$$

In particular, recall that $\mathbb{C}\Omega_n \cong \mathbb{C}^n$ decomposes into a direct sum

$$\mathbb{C}^n = \mathsf{St}_n \oplus \mathsf{triv}_n,$$

where $\mathsf{St}_n = \{(x_1, \dots, x_n) \mid \sum x_i = 0\}$ is an irreducible $(n-1)$-representation and $\mathsf{triv}_n = \mathbb{C}\langle x_1 + \dots + x_n \rangle$ is a copy of the trivial representation. This implies that

$$\chi_{\mathsf{St}_n}(\sigma) = |\{i \mid \sigma(i) = i,\ 1 \le i \le n\}| - 1.$$

As an explicit example of a character table, take $G = S_3$. There are three conjugacy classes with representatives e, (12), and (123) of sizes 1, 3, and 2, respectively. There are three irreducible representations, triv, sgn (the sign representation, one dimensional where σ acts by the signature of σ) and St_2. The character table is

	e	(12)	(123)
χ_{triv}	1	1	1
χ_{sgn}	1	-1	1
χ_{St_2}	2	0	-1

One may verify easily that the two orthogonality formulas hold in this case.

Here is a more involved example, namely the character table of S_4. We use this calculation as a pretext to illustrate a couple of useful techniques for determining characters. The first is about tensoring with one-dimensional representations.

Lemma 6.19. *Let V be a G-representation and W be a one-dimensional G-representation. Then*

(1) V is irreducible if and only the contragredient representation V^* is irreducible;
(2) $V \otimes W$ is irreducible if and only if V is irreducible.

Proof. Exercise. □

Example 6.20. *Let V be an irreducible S_n-representation. Then $V \otimes \mathsf{sgn}$ is also irreducible. It may be possible that $V \otimes \mathsf{sgn} \cong V$, we will see this for S_4. In general, one can tell easily from the character table if that is the case or not: check if $\chi_V \cdot \chi_{\mathsf{sgn}}$ is equal or not to χ_V.*

For example, we know that $\chi_{\mathsf{St}_n}((12)) = n-3$. This means that $\chi_{\mathsf{St}_n \otimes \mathsf{sgn}}((12)) = 3-n$ and therefore, if $n \geq 4$, $\mathsf{St}_n \otimes \mathsf{sgn}$ is an irreducible S_n-representation which is nonisomorphic to St_n (but of the same dimension).

Now, taking $G = S_4$, we see that we already know 4 irreducible representations: triv, sgn, St_4 and $\mathsf{St}_4 \otimes \mathsf{sgn}$. On the other hand, S_4 has 5 conjugacy classes with representatives: e, (12), (123), $(12)(34)$, and (1234), respectively. By the general theory, we know we are missing one irreducible S_4-representation, call it U. If n is the dimension of U, since the sum of squares of irreducible representations equals the size of the group, we see that

$$24 = 1^2 + 1^2 + 3^2 + 3^2 + n^2,$$

hence $n = 2$. We can start to fill in the character table, since we know the characters of triv, sgn, but also of St_4 (hence also $\mathsf{St}_4 \otimes \mathsf{sgn}$) by Example 6.18, to get

S_4	e	(12)	(123)	$(12)(34)$	(1234)
size	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{St_4}	3	1	0	-1	-1
$\chi_{St_4 \otimes \mathsf{sgn}}$	3	-1	0	-1	1
χ_U	2				

The remaning entries in the table can be found by using the the columns are orthogonal . For example, using the first and second colum: $1 \cdot 1 + 1 \cdot (-1) + 3 \cdot 1 + 3 \cdot (-1) + 2 \cdot x = 0$ implies that the unknown entry is $x = 0$. The complete table is:

S_4	e	(12)	(123)	$(12)(34)$	(1234)
size	1	6	8	3	6
χ_{triv}	1	1	1	1	1
χ_{sgn}	1	-1	1	1	-1
χ_{St_4}	3	1	0	-1	-1
$\chi_{St_4 \otimes \mathsf{sgn}}$	3	-1	0	-1	1
χ_U	2	0	-1	2	0

To double-check that U is irreducible, we can compute the inner product of χ_U with itself, it should come out 1:

$$\langle \chi_U, \chi_U \rangle = \frac{1}{24}(1 \cdot 2^2 + 6 \cdot 0^2 + 8 \cdot (-1)^2 + 3 \cdot 2^2 + 6 \cdot 0^2) = 1.$$

We may ask however how one could construct U explicitly as a representation. We get lucky here because $\chi_U((12)(34)) = \chi_U(e) = 2$.

Lemma 6.21. *Let $\rho : G \to GL(V)$ be a representation, and define $N = \{g \in G \mid \chi_V(g) = \chi_V(e)\}$. Then $N = \ker \rho$, in particular, N is normal in G.*

Proof. Exercise. □

Whenever N is a normal subgroup of G, so G/N is a group, it is easy to construct (irreducible) representations of G from (irreducible) representations of G/N. Suppose $\overline{\rho} : G/N \to GL(V)$ is a representation, and let $\pi_N : G \to G/N$ be the natural projection homomorphism. Then the composition

$$\rho = \overline{\rho} \circ \pi_N : G \to GL(V) \tag{6.9}$$

is a group homomorphism, hence it is a G representation. Explicitly, $\rho(g) = \overline{\rho}(gN)$ for all $g \in G$. In particular,

$$\chi_\rho(g) = \chi_{\overline{\rho}}(gN), \quad g \in G. \tag{6.10}$$

Notice that this implies that $N \subseteq \ker \rho$. Moreover, it is easy to see that $N = \ker \rho$ if and only if $\bar{\rho}$ is a faithful G/N-representation, i.e., $\bar{\rho}$ is injective. We call ρ the *lift* of $\overline{\rho}$.

Lemma 6.22. *The lift ρ is an irreducible G-representation if and only if $\bar{\rho}$ is an irreducible G/N-representation.*

Proof. Exercise. □

Now, back to the motivating S_4 example, setting $N = \{\sigma \in S_4 \mid \chi_U(\sigma) = \chi_U(e) = 2\}$, we see that $N = \{e, (12)(34), (13)(24), (14)(23)\}$, a normal subgroup of S_4. By the discussion above, the representation $\rho_U : S_4 \to GL(U)$ is the lift of the representation $\bar{\rho}_U : S_4/N \to GL(U)$ such that $\rho_U(\sigma) = \bar{\rho}_U(\sigma U)$ for all $\sigma \in S_4$. It is easy to check that G/N is naturally isomorhic to S_3, for example, by considering the representatives e, (12), (23), (13), (123) and (132) of the left cosets G/N. A neat way to visualize this is to think of the "essential" labels of a rectangle. Consider a rectangle (not a square) with vertices labelled by $1, 2, 3, 4$. The essential labels of the rectangle are all the possible labels of the rectangle up to rigid symmetries, i.e., geometric transformations which map the rectangle to itself without twisting its shape. If we think of the rectangle with (x, y)-coordinates $(-2, 1)$, $(2, 1)$, $(2, -1)$, and $(-2, -1)$, it is clear that the group of rigid symmetries is $C_2 \times C_2$, where the two generators of $C_2 \times C_2$ are the reflections in the x-axis and in the y-axis. If we label a "base" rectangle 1, 2, 3, 4, in the order above, then the permutation (12)(34) corresponds to the reflection in the y-axis, while (14)(23) to the reflection in the x-axis. Hence the group of symmetries can be identified with N. But then it follows that the set of essential labels of the rectangle can be naturally identified with S_4/N. On the other hand, fixing the label 4 on the bottom left corner of the rectangle, we see that all other permutations of $1, 2, 3$ define different essential labels.

Thus $\bar{\rho}_U$ is a faithful representation of S_3, and we know it is 2-dimensional, because U is, hence $\bar{\rho}_U$ must be the standard representation St_2. In conclusion, U is the lift of St_2.

7. Induction and restriction

The discussion at the end of the previous section shows that it is very easy to relate representations of a group and representation of its quotient groups. But what about the relation with representations of subgroups? In other words, if H is a subgroup of G, is there a way to construct representations of H from G and viceversa?

7.1. **Restriction.** One direction is very easy. Suppose that $\rho : G \to GL(V)$ is a representation of G and $H \le G$. Then we can *restrict* the representation ρ to H, namely, define the H-representation

$$\operatorname{Res}^G_H V := \rho|_H : H \to GL(V), \quad \rho|_H(h) = \rho(h). \tag{7.1}$$

In particular, it is clear that

$$\chi_{\operatorname{Res}^G_H V}(h) = \chi_V(h), \text{ for all } h \in H.$$

In general, if V is an irreducible G-representation, $\operatorname{Res}^G_H V$ is a reducible H-representation.

Exercise 7.1. *Verify, using the character tables that* $\operatorname{Res}^{S_4}_{S_3} \mathsf{St}_4 = \mathsf{St}_3 \oplus \mathsf{triv}_3$.

7.2. **Induction.** On the other hand, to construct representations of G from H-representations is a more difficult. The best known construction is called *induction*.

Definition 7.2. *If $H \le G$ and (μ, W) is an H-representation, define the induced representation*

$$\operatorname{Ind}^G_H W = \{f : G \to W \mid f(xh) = \mu(h^{-1})f(x), \text{ for all } x \in G,\ h \in H\}.$$

In this definition, in the right hand side of the condition, $f(x) \in W$ and $\mu(h^{-1})$ is the action of h^{-1} on W. The action of G on $\operatorname{Ind}^G_H W$ is the left-regular action

$$(g \cdot f)(x) = f(g^{-1}x), \quad g \in G,\ x \in G.$$

We remark that $\mu(h^{-1})$ rather than $\mu(h)$ is needed for the condition to make sense. This is so that

$$f(xh_1h_2) = \mu(h_2^{-1})f(xh_1) = \mu(h_2^{-1})\mu(h_1^{-1})f(x) = \mu((h_1h_2)^{-1})f(x),$$

which is consistent.

Lemma 7.3. $\operatorname{Ind}^G_H W$ *is indeed a G-representation.*

Proof. Let $\operatorname{Fun}(G) = \{f : G \to \mathbb{C}\}$ be the $\mathbb{C}$-vector space of functions on G. As we have seen before, this is a representation of G with the left regular action. Hence we only need to check that $\operatorname{Ind}^G_H W$ is a G-stable subspace. Let $f \in \operatorname{Ind}^G_H W$ and $g \in G$, then:

$$(g \cdot f)(xh) = f(g^{-1}xh) = \mu(h^{-1})f(g^{-1}x) = \mu(h^{-1})(g \cdot f)(x),$$

hence $g \cdot f$ satisfies the defining condition. □

Example 7.4. *Let W be the trivial representation of H. Then $\operatorname{Ind}^G_H \mathsf{triv} = \{f : G \to \mathbb{C} \mid f(xh) = f(x), \text{ for all } x \in G,\ h \in H\} = \{\bar{f} : G/H \to \mathbb{C}\}$ with the left regular action. But this is nothing by $\mathbb{C}G/H$ as a left representation of G. Hence*

$$\operatorname{Ind}^G_H \mathsf{triv} = \mathbb{C}G/H.$$

In particular, $\operatorname{Ind}^G_{\{e\}} \mathsf{triv} = \mathbb{C}G$ as a G-representation, where e is the identity element of G.

To understand the induced representation better, notice that if we choose a set of representative S for the left cosets G/H, then every $f \in \operatorname{Ind}^G_H W$ is uniquely determined by the set $\{f(s) \mid s \in S\}$. On the other hand, we are free to choose $f(s) \in W$, which means that

$$\dim \operatorname{Ind}^G_H W = [G : H] \cdot \dim W, \tag{7.2}$$

where $[G : H]$ is the index of H in G, i.e., the number of left cosets G/H. We compute now the character of the induced representation.

Theorem 7.5. *The character of* $\operatorname{Ind}^G_H W$ *is*

$$\chi_{\operatorname{Ind}^G_H W}(g) = \sum_{\substack{s \in S \\ s^{-1}gs \in H}} \chi_W(s^{-1}gs) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \chi_W(x^{-1}gx). \tag{7.3}$$

Proof. The second equality is easy. This is because every $x \in G$ is of the form $x = sh$ for some $s \in S$, $h \in H$, and $x^{-1}gx \in H$ if and only if $s^{-1}gs \in H$; moreover $\chi_W(x^{-1}gx) = \chi_W(h^{-1}s^{-1}gsh) = \chi_W(s^{-1}gs)$ because χ_W is an H-character, hence an H-class function.

To prove the first equality[4], for every $s \in S$, define

$$W_s = \{f \in \operatorname{Ind}_H^G W \mid f(g) = 0 \text{ for all } g \notin sH\}.$$

In other words, each W_s consists of functions which are 0 outside the coset sH. In addition, every $f \in W_s$ is uniquely determined by its value $f(s)$, which means that, as a vector space $W_s \cong W$. Then

$$\operatorname{Ind}_H^G W = \bigoplus_{s\in S} W_s, \text{ as vector spaces.}$$

As a side remark, notice that this decomposition is not one of G-representations since W_s is not G-stable; indeed the action of G is via the left regular representation, so it mixes the left cosets in G/H.

Let us denote by $\rho : G \to GL(\operatorname{Ind}_H^G W)$ the induced representation homomorphism. Fix $g \in G$. We wish to compute the trace $\chi_\rho(g)$ of the linear map $\rho(g) : \operatorname{Ind}_H^G W \to \operatorname{Ind}_H^G W$. If we compute this trace using a basis of $\operatorname{Ind}_H^G W$ coming from the concatenation of the bases of the W_s, $s \in S$, then

$$\chi_\rho(g) = \sum_{s\in S} \chi_s(g),$$

where $\chi_s(g)$ is the trace of the diagonal block of $\rho(g)$ corresponding to W_s. (We are not claiming that $\rho(g)$ is block diagonal with respect to the decomposition $\bigoplus_{s\in S} W_s$, which isn't true, but, since we compute the trace, we only need to worry about these pieces of the matrix of $\rho(g)$.)

If $gsH \neq sH$, then $\rho(g)$ maps W_s to W_{gs} which different than W_s, and hence there won't be any contribution to the trace, i.e., $\chi_s(g) = 0$.

So assume that $gsH = sH$, which is equivalent to $s^{-1}gs \in H$. Denote $s^{-1}gs = h \in H$. Define

$$\alpha : W_s \to W, \quad \alpha(f) = f(s).$$

This is a linear map, and as already remarked, f is uniquely determined by f_s, hence α is the natural isomorphism between W_s and W. We wish to see how the action of g on W_s transforms under this isomorphism to an action on W. We calculate

$$\alpha(g \cdot f) = (g \cdot f)(s) = f(g^{-1}s) = f(sh^{-1}) = \mu(h)f(s) = \mu(h)\alpha(f).$$

In other words, the action of g on f corresponds to the action of $h = s^{-1}gs$ on $\alpha(f)$. This implies that $\chi_s(g) = \chi_W(h) = \chi_W(s^{-1}gs)$, hence the first equality in the theorem is proved. □

If we wish to compute the induced character using the character table, then we need to rephrase (7.3) in terms of conjugacy classes. Firstly, notice that if C is a conjugacy class in G such that $C \cap H = \emptyset$, then the condition $x^{-1}gx \in H$ is never satisfied for $g \in C$, hence

$$\chi_{\operatorname{Ind}_H^G W}(C) = 0, \text{ for all } C \text{ such that } C \cap H = \emptyset.$$

On the other hand, suppose that $C \cap H \neq \emptyset$. Then $C \cap H$ is closed under conjugation by H, so it breaks up into a disjoint union of H-conjugacy classes $C = \sqcup_{i=1}^{\ell} D_i$.

Corollary 7.6. *If $C \cap H = \sqcup_{i=1}^{\ell} D_i$, then*

$$\chi_{\operatorname{Ind}_H^G W}(C) = \frac{|G|}{|H|} \sum_{i=1}^{\ell} \frac{|D_i|}{|C|} \chi_W(D_i). \tag{7.4}$$

Proof. Fix $g \in C$. Denote by $Z_G(g) = \{x \in G \mid x^{-1}gx = g\}$ the centralizer of g in G. From (7.3), we know that

$$\chi_{\operatorname{Ind}_H^G W}(C) = \frac{1}{|H|} \sum_{\substack{x\in G \\ x^{-1}gx\in H}} \chi_W(x^{-1}gx) = \frac{|Z_G(g)|}{|H|} \sum_{y\in C\cap H} \chi_W(y),$$

[4] I follow the exposition in [2] for this proof.

where we made the change $y = x^{-1}gx$, and we had to account for the fact that if $x' \in Z_G(g)x$, then $(x')^{-1}gx' = y$ as well. By the orbit-stabilizer theorem, we have

$$|Z_G(g)| = |G|/|C|.$$

Finally, it is clear that $\displaystyle\sum_{y\in C\cap H} \chi_W(y) = \sum_{i=1}^{\ell} |D_i|\chi_W(D_i).$ □

Example 7.7. *In general, $C \cap H$ does not equal a single H-conjugacy class. For example, take $G = S_3$, $H = A_3$. Then the conjugacy class $C = \{(123), (132)\}$ in S_3 breaks up into $C \cap A_3 = \{(123)\} \cup \{(132)\}$ in A_3. Of course, A_3 is abelian, hence every A_3-conjugacy class is a singleton.*

7.3. **Frobenius reciprocity.** The main relation between induction and restriction is Frobenius reciprocity.

Proposition 7.8. *Let $H \leq G$ be a subgroup, V a G-representation and W an H-representation.*

(1) There is a natural linear isomorphism $\mathrm{Hom}_G(V, \mathrm{Ind}_H^G W) \cong \mathrm{Hom}_H(\mathrm{Res}_H^G V, W)$.

(2) $\langle \chi_V, \chi_{\mathrm{Ind}_H^G W}\rangle_G = \langle \chi_{\mathrm{Res}_H^G V}, \chi_W\rangle_H$.

Proof. (1) This is the type of abstract algebra nonsense proof that writes itself(and yet the proof is *non-examinable*). Let us denote for simplicity M the space on the left and N the space on the right. We define to maps $\Phi : M \to N$ and $\Psi : N \to M$ and prove that they are well defined, linear, and inverses to each other. The definitions are the only things that make sense naturally.

Firstly, for $\Phi : M \to N$, for every $\alpha \in M$, set

$$\Phi(\alpha)(v) = \alpha(v)(e) \in W, \quad v \in V,$$

where e is the identity element in G. Secondly, for $\Psi : N \to M$, for every $\beta \in N$, set

$$\Psi(\beta)(v)(x) = \beta(x^{-1} \cdot v), \quad v \in V,\ x \in G.$$

Check the following steps:

(i) $\Phi(\alpha)$ is an H-homomorphism:

$$\begin{aligned}\Phi(\alpha)(h \cdot v) &= \alpha(h \cdot v)(e) = (h \cdot \alpha(v))(e) = \alpha(v)(h^{-1}e)\\ &= h \cdot (\alpha(v)(e)) = h \cdot \Phi(\alpha)(v).\end{aligned}$$

(ii) $\Psi(\beta)(v)$ is an element of $\mathrm{Ind}_H^G W$:

$$(\Psi(\beta)(v))(xh) = \beta(h^{-1}x^{-1} \cdot v) = h^{-1} \cdot \beta(x^{-1} \cdot v) = h^{-1} \cdot (\Psi(\beta)(v))(x).$$

(iii) $\Psi(\beta)$ is a G-homomorphism:

$$(\Psi(\beta)(g \cdot v)(x) = \beta(x^{-1}g \cdot v) = \beta((g^{-1}x)^{-1} \cdot v) = (\Psi(\beta)(v))(g^{-1}x) = g \cdot (\Psi(\beta)(v))(x).$$

(iv) $\Phi \circ \Psi = \mathrm{Id}_N$:

$$\Phi(\Psi(\beta))(v) = (\Psi(\beta)(v))(e) = \beta(e^{-1} \cdot v) = \beta(v).$$

(v) $\Psi \circ \Phi = \mathrm{Id}_M$:

$$(\Psi(\Phi(\alpha))(v))(x) = \Phi(\alpha)(x^{-1} \cdot v) = \alpha(x^{-1} \cdot v)(e) = (x^{-1} \cdot \alpha(v))(e) = \alpha(v)(x).$$

(2) The character formula follows immediately from (1) just by taking dimensions of M and N. But we also give another direct proof involving characters. The left hand side equals

$$\begin{aligned}LHS &= \frac{1}{|G|}\sum_{g\in G} \overline{\chi_V(g)}\chi_{\mathrm{Ind}_H^G W}(g) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{|H|}\sum_{\substack{x\in G\\ x^{-1}gx\in H}} \overline{\chi_V(g)}\chi_W(x^{-1}gx)\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{\substack{g,x\in G\\ x^{-1}gx\in H}} \overline{\chi_V(x^{-1}gx)}\chi_W(x^{-1}gx),\end{aligned}$$

where we used that χ_V is a class function on G, hence $\chi_V(g) = \chi_V(x^{-1}gx)$. Now denote $x^{-1}gx = h \in H$, and write $g = xhx^{-1}$ and change the summation indices from g and x to h and x:

$$\begin{aligned} LHS &= \frac{1}{|G|}\frac{1}{|H|}\sum_{\substack{x\in G\\ h\in H}} \overline{\chi_V(h)}\chi_W(h) \\ &= \frac{1}{|H|}\sum_{h\in H} \overline{\chi_V(h)}\chi_W(h), \end{aligned}$$

which is exactly the RHS.

□

Example 7.9. *To illustrate Frobenius reciprocity, take $H = \{e\}$, $W = \mathsf{triv}$, the trivial representation of the trivial group. Then $\operatorname{Res}^G_{\{e\}} V = \dim V \cdot \mathsf{triv}$, hence the right hand side of the character form of Frobenius reciprocity equals $\dim V$. On the other hand, as we have seen already $\operatorname{Ind}^G_{\{e\}} \mathsf{triv} = \mathbb{C}G$. Therefore*

$$\langle \chi_V, \chi_{\mathbb{C}G}\rangle_G = \dim V. \tag{7.5}$$

In particular, if V is irreducible, this says that V appears in $\mathbb{C}G$ $\dim V$ times:

$$\mathbb{C}G = \bigoplus_{V \ irreducible} (\dim V)\ V, \tag{7.6}$$

which is something that we knew as a consequence of the Artin-Wedderburn Theorem.

7.4. **An interesting example.** To give a more subtle application of Frobenius reciprocity, let us assume that $H = N$ is a normal subgroup of G. Recall that S is a set of representatives for G/N (the latter is also a group now). From the character formula for induced representations (7.3), we have $\chi_{\operatorname{Ind}^G_N W}(g) = \sum_{\substack{s\in G/N\\ s^{-1}gs\in N}} \chi_W(s^{-1}gs)$.

Since N is normal, we have $s^{-1}gs \in N$ if and only if $g \in N$. This means that in this case

$$\chi_{\operatorname{Ind}^G_N W}(g) = \begin{cases} \sum_{s\in S} \chi^s_W(g), & \text{if } g \in N, \\ 0, & \text{if } g \notin N, \end{cases} \tag{7.7}$$

where we define for every $s \in S$,

$$\chi^s_W : N \to \mathbb{C}, \quad \chi^s_W(g) = \chi_W(s^{-1}gs), \quad g \in N.$$

Lemma 7.10. *The function χ^s_W is a class function on N. Moreover, $\langle \chi^s_W, \chi^s_W\rangle_N = \langle \chi_W, \chi_W\rangle_N$. In particular, if χ_W is an irreducible character, so is χ^s_W.*

Proof. For the first claim, let $n \in N$ and $g \in N$. Since N is normal $ns = sn'$ for some $n' \in N$. Calculate

$$\chi^s_W(n^{-1}gn) = \chi_W(s^{-1}n^{-1}gns) = \chi_W((n')^{-1}s^{-1}gsn').$$

Since χ_W is the character of an N-representation, it is a class function on N, hence we continue

$$\chi^s_W(n^{-1}gn) = \chi_W(s^{-1}gs) = \chi^s_W(g).$$

This proves that χ^s_W is a class function. For the second claim, compute

$$\langle \chi^s_W, \chi^s_W\rangle_N = \frac{1}{|N|}\sum_{n\in N} \overline{\chi^s_W(n)}\chi^s_W(n) = \frac{1}{|N|}\sum_{n\in N} \overline{\chi_W(s^{-1}ns)}\chi_W(s^{-1}ns).$$

Make the change $n' = s^{-1}ns \in N$ since N is normal. As n ranges over N so does n', hence

$$\langle \chi^s_W, \chi^s_W\rangle_N = \frac{1}{|N|}\sum_{n'\in N} \overline{\chi_W(n')}\chi_W(n') = \langle \chi_W, \chi_W\rangle_N.$$

The last claim is immediate since χ_W is irreducible if and only if $\langle \chi_W, \chi_W\rangle_N = 1$. □

This means that formula (7.7) can be rewritten in the following more elegant form:

$$\chi_{\operatorname{Res}^G_N \operatorname{Ind}^G_N(W)} = \sum_{s\in S} \chi^s_W. \tag{7.8}$$

Proposition 7.11. *Let N be a normal subgroup of G and W be an irreducible N-representation. Then $\mathrm{Ind}_N^G W$ is an irreducible G-representation if and only if $\chi_W^s \neq \chi_W$ for all $s \in S \setminus \{e\}$.*

Proof. Apply Frobenius reciprocity:

$$\langle \chi_{\mathrm{Ind}_N^G W}, \chi_{\mathrm{Ind}_N^G W}\rangle_G = \langle \chi_{\mathrm{Res}_N^G \mathrm{Ind}_N^G W}, \chi_W\rangle_N,$$

and then by (7.8)

$$\langle \chi_{\mathrm{Ind}_N^G W}, \chi_{\mathrm{Ind}_N^G W}\rangle_G = \sum_{s\in S}\langle \chi_W^s, \chi_W\rangle_N = 1 + \sum_{s\in S\setminus\{e\}}\langle \chi_W^s, \chi_W\rangle_N,$$

where the 1 comes from $\langle \chi_W, \chi_W\rangle_N$. The claim now follows from Lemma 7.10. □

Example 7.12. *(1) Suppose N is a proper normal subgroup of G. Then $\mathrm{Ind}_N^G \mathsf{triv}$ is always reducible. This is because when $W = \mathsf{triv}$, all $\chi^s_{\mathsf{triv}} = \chi_{\mathsf{triv}}$. In fact, the proof of Proposition 7.11 shows that*

$$\langle \chi_{\mathrm{Ind}_N^G \mathsf{triv}}, \chi_{\mathrm{Ind}_N^G \mathsf{triv}}\rangle_G = [G : N]. \tag{7.9}$$

(2) Let $N = A_3$ in $G = S_3$. Since $A_3 \cong C_3$, there are 3 one-dimensional irreducible A_3 representations μ_1, μ_ζ, μ_{ζ^2}, where ζ is a primitive 3-root of unity, defined by

$$\mu_{\zeta^i}((123)) = \zeta^i, \quad 0 \le i \le 2. \tag{7.10}$$

By the previous example, $\mathrm{Ind}_{A_3}^{S_3} \mu_1$ is reducible and it is 2-dimensional, hence it must be $\mathrm{Ind}_{A_3}^{S_3} \mu_1 = \mathsf{triv}_3 \oplus \mathsf{sgn}_3$.

On the other hand, taking $S = \{e, (12)\}$,

$$\mu_\zeta^{(12)}((123)) = \mu_\zeta((12)(123)(12)) = \mu_\zeta((132)) = \mu_\zeta((123)^2) = \zeta^2,$$

meaning that $\mu_\zeta^{(12)} = \mu_{\zeta^2}$ and similarly, $\mu_{\zeta^2}^{(12)} = \mu_\zeta$. By Proposition 7.11, both $\mathrm{Ind}_{A_3}^{S_3}(\mu_{\zeta^i})$, $i = 1, 2$, are irreducible. Since they are both two-dimensional, it follows that

$$\mathrm{Ind}_{A_3}^{S_3}(\mu_\zeta) \cong \mathrm{Ind}_{A_3}^{S_3}(\mu_{\zeta^2}) \cong \mathsf{St}_3. \tag{7.11}$$

We remark, that by Frobenius reciprocity, this implies that

$$\mathrm{Res}_{A_3}^{S_3} \mathsf{St}_3 = \mu_\zeta \oplus \mu_{\zeta^2}. \tag{7.12}$$

7.5. **An example: dihedral groups.** The dihedral group D_{2n} is the group of symmetries of the regular n-gon. It is defined in terms of generators and relations as:

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1,\ srs = r^{-1}\rangle. \tag{7.13}$$

We would like to describe the irreducible complex representations of D_{2n}. Firstly, let us determine the conjugacy classes. In addition to the trivial element 1, there are two types of elements: rotations $(r, r^2, \dots, r^{n-1})$ and reflections $(s, sr, \dots, sr^{n-1})$. Since $sr^is = r^{-i} = r^{n-i}$, we see that r^i and r^{n-i} are in the same conjugacy class. Moreover, $s \cdot sr^i \cdot s = r^is = s^{-i}$, so sr^i and sr^{-i} are in the same conjugacy class. Finally, $r \cdot sr^i \cdot r^{-1} = sr^{i-2}$, so sr^i and sr^{i-2} are conjugate. Since s and r generate D_{2n}, this discussion gives the following

Lemma 7.13. *If n is even, there are $\frac{n}{2} + 3$ conjugacy classes: $\{1\}$, $\{r^i, r^{n-i}\}$, $1 \le i < \frac{n}{2}$, $\{r^{n/2}\}$, $\{s, sr^2, sr^4, \dots, sr^{n-2}\}$ and $\{sr, sr^3, \dots, sr^{n-1}\}$.*

If n is odd, there are $\frac{n+1}{2} + 1$ conjugacy classes: $\{1\}$, $\{r^i, r^{n-i}\}$, $1 \le i \le \frac{n-1}{2}$, and $\{s, sr, sr^2, \dots, sr^{n-1}\}$.

Next, we can easily determine the one-dimensional representations. If $\rho : D_{2n} \to \mathbb{C}^\times$ is a one-dimensional representation, then we only need to determine the scalars by which r and s act, since everything else is determined by them. Suppose that λ_r and λ_s are these scalars. Then because of the relations in D_{2n}, the conditions they need to satisfy are:

$$\lambda_s^2 = 1,\ \lambda_r^n = 1,\ \lambda_r = \lambda_r^{-1}.$$

This means that if n is even, there are four one-dimensional representations given by $\lambda_s, \lambda_r \in \{\pm 1\}$. If n is odd on the other hand, there are only two one-dimensional representations: $\lambda_s \in \{\pm 1\}$ and $\lambda_r = 1$.

So it remains to determine $\frac{n}{2} - 1$ irreducible representations when n is even and $\frac{n-1}{2}$ irreducible representations, when n is odd.

Suppose n is even, of dimensions $d_i \geq 2$, $1 \leq i \leq \frac{n}{2} - 1$. Adding the squares of the dimensions, we see

$$\sum_{i=1}^{\frac{n}{2}-1} d_i^2 = 2n - 4,$$

which means that $d_i = 2$ for all i. Similarly, we see that also in the odd case, all of the remaining $\frac{n-1}{2}$ representations are two dimensional.

To determine these two-dimensional representations, all we need is to remember that D_{2n} acts on the plane as the symmetries of the regular n-gon. Motivated by this, define

$$\rho_k : D_{2n} \to GL(2, \mathbb{C}), \quad \rho_k(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \rho_k(r) = \begin{pmatrix} \cos k\theta & \sin k\theta \\ -\sin k\theta & \cos k\theta \end{pmatrix},$$

where $\theta = 2\pi/n$ and $1 \leq k \leq n - 1$.

Proposition 7.14. *The equivalence classes of irreducible representations of D_{2n} are given by the 4 (respectively 2) one-dimensional representations when n is even (respectively odd), and by the two-dimensional representations ρ_k, where $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$.*

Proof. It is easy to check that ρ_k are group homomorphisms, i.e., representations. We only need to check that the matrices written above satisfy the same relations as s and r. Next, notice that the number of ρ_k, where $1 \leq k \leq \lfloor \frac{n-1}{2} \rfloor$ is exactly the number of two dimensional representations that we need to find. This means that we only need to show that the ρ_k are inequivalent. For that, we look at their characters. In particular,

$$\chi_{\rho_k}(s) = 0, \quad \chi_{\rho_k}(r) = 2\cos k\theta.$$

Since $\cos k\theta \neq \cos k'\theta$ for $1 \leq k \neq k' \leq \lfloor \frac{n-1}{2} \rfloor$, we see that the characters are different. □

8. Exterior and symmetric powers

The construction of exterior and symmetric powers makes sense for vector spaces over an arbitrary field k. Recall that if V and W are two k-vector spaces, we defined their tensor product $V \otimes W$. The following lemma is easy to prove using the universal property of the tensor product.

Lemma 8.1. *Let U, V, W be k-vector spaces.*

(1) The assignment $v \otimes w \mapsto w \otimes v$ extends to a k-linear isomorphism $V \otimes W \cong W \otimes V$.
(2) The assignment $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$ extends to a k-linear isomorphism $(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$.

Because of the second part of this lemma, we may write $V^{\otimes n} = \underbrace{V \otimes V \otimes \cdots \otimes V}_{n}$ without ambiguity, and call it the n-fold tensor product of V.

Definition 8.2 (Exterior powers)**.** *Consider the subspace U of $V^{\otimes n}$ generated by all simple tensors of the form $v_1 \otimes v_2 \otimes \cdots \otimes v_n$, where $v_i = v_j$ for some $i \neq j$. Define the quotient vector space*

$$\bigwedge^n V = V^{\otimes n}/U.$$

Let $\pi : V^{\otimes n} \to \bigwedge^n V$ be the projection map, and denote the image of $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ in $\bigwedge^n V$ by $v_1 \wedge v_2 \wedge \cdots \wedge v_n$.

If σ is any permutation in S_n, then

$$v_{\sigma(1)} \wedge \cdots \wedge v_{\sigma(n)} = \mathsf{sgn}(\sigma)\ v_1 \wedge \cdots \wedge v_n. \tag{8.1}$$

To see this, recall that every permutation is a product of transpositions, so it is sufficient to prove this for a transposition (ij), $i < j$. The usual bilinearity trick is

$$(v_i + v_j) \otimes (v_i + v_j) - v_i \otimes v_i - v_j \otimes v_j = v_i \otimes v_j + v_j \otimes v_i.$$

Applying π to both sides, the left hand side is mapped to 0 and the right hand side gives

$$v_i \wedge v_j = -v_j \wedge v_i.$$

Suppose $\{e_i\}$ is a basis of V, then

$$\{e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_n} \mid i_1 < i_2 < \cdots < i_n\} \tag{8.2}$$

is a basis of $\bigwedge^n V$. In particular, if $\dim V = m$, then

$$\dim \bigwedge^n V = \begin{cases} \binom{m}{n}, & \text{if } n \leq m, \\ 0, & \text{if } n > m. \end{cases}$$

Definition 8.3 (Symmetric powers)**.** *Consider the subspace U' of $V^{\otimes n}$ generated by all expressions $v_1 \otimes v_2 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes v_{\sigma(2)} \otimes \cdots \otimes v_{\sigma(n)}$, $\sigma \in S_n$. Define the quotient vector space*

$$\mathrm{Sym}^n V = V^{\otimes n}/U'.$$

Let $\pi' : V^{\otimes n} \to \mathrm{Sym}^n V$ be the projection map, and denote the image of $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ in $\mathrm{Sym}^n V$ by $v_1 \cdot v_2 \cdots v_n$.

By definition, if σ is any permutation in S_n, then

$$v_{\sigma(1)} \cdot v_{\sigma(2)} \cdots v_{\sigma(n)} = v_1 \cdot v_2 \cdots v_n. \tag{8.3}$$

A basis of $\mathrm{Sym}^n V$ is

$$\{e_{i_1} \cdot e_{i_2} \cdot \cdots \cdot e_{i_n} \mid i_1 \leq i_2 \leq \cdots \leq i_n\}. \tag{8.4}$$

If the characteristic of the field k is 0, then we may think of the exterior and symmetric powers as subspaces of $V^{\otimes n}$. More precisely, define

$$\iota : \bigwedge^n V \to V^{\otimes n}, \qquad v_1 \wedge \cdots \wedge v_n \mapsto \frac{1}{n!} \sum_{\sigma \in S_n} \mathsf{sgn}(\sigma)\ v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}, \tag{8.5}$$

$$\iota' : \mathrm{Sym}^n V \to V^{\otimes n}, \qquad v_1 \cdot \cdots \cdot v_n \mapsto \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}. \tag{8.6}$$

It is easy to see that $\pi \circ \iota = \mathrm{Id}$ on $\bigwedge^n V$, and similarly $\pi \circ \iota' = \mathrm{Id}$ on $\mathrm{Sym}^n V$.

8.1. **Representations on symmetric and exterior powers.** Specialize again $\mathsf{k} = \mathbb{C}$. If V is a G-representation, then $V^{\otimes n}$ is also a G-representation via

$$g \cdot (v_1 \otimes \cdots \otimes v_n) = (g \cdot v_1) \otimes \cdots \otimes (g \cdot v_n).$$

It is clear that the subspaces U and U' used to define the exterior and symmetric powers, respectively, are subrepresentations, which means that so are the quotients $\bigwedge^n V$ and $\mathrm{Sym}^n V$.

Example 8.4. *If $n = 2$, then $V \otimes V = \mathrm{Sym}^2 V \oplus \bigwedge^2 V$ as $\mathbb{C}$-vector spaces. This is because every simple tensor can be written as*

$$v_1 \otimes v_2 = \frac{1}{2}(v_1 \otimes v_2 + v_2 \otimes v_1) + \frac{1}{2}(v_1 \otimes v_2 - v_2 \otimes v_1),$$

and the first component is in $\mathrm{Sym}^2 V$, while the second is in $\bigwedge^2 V$, and $\mathrm{Sym}^2 V \cap \bigwedge^2 V = \{0\}$.

If V is a G-representation, then this decomposition is one of G-representations.

Lemma 8.5. *If V is a G-representation, the characters of $\bigwedge^2 V$ and $\mathrm{Sym}^2 V$ are given by:*

$$\begin{aligned} \chi_{\bigwedge^2 V}(g) &= \frac{1}{2}(\chi_V(g)^2 - \chi_V(g^2)), \\ \chi_{\mathrm{Sym}^2 V}(g) &= \frac{1}{2}(\chi_V(g)^2 + \chi_V(g^2)). \end{aligned} \tag{8.7}$$

Proof. Since $\chi_{V \otimes V}(g) = \chi_V(g)^2$, it is sufficient to prove one of the formulas. Let $\rho : G \to GL(V)$ be the representation. Let $\lambda_1, \ldots, \lambda_m$ be the eigenvalues of $\rho(g)$. Since $\rho(g)$ is diagonalizable, there exists a basis of V given by eigenvectors $e_1, \ldots, e_m$ for these eigenvalues. Then

$$g \cdot (e_i \wedge e_j) = (g \cdot e_i) \wedge (g \cdot e_j) = \lambda_i \lambda_j (e_i \wedge e_j),$$

for all $i < j$. This means that the eigenvalues of the action of g on $\bigwedge^2 V$ are $\lambda_i \lambda_j$, $i < j$. So the character is

$$2\chi_{\bigwedge^2 V}(g) = 2 \sum_{i<j} \lambda_i \lambda_j = (\sum_i \lambda_i)^2 - \sum_i \lambda_i^2,$$

which proves the formula. $\square$

8.2. **The character table of S_5.** To illustrate one use of exterior and symmetric powers, we will use them to determine the character table of S_5. The group S_5 has 7 conjugacy classes, hence we need to find 7 irreducible characters. We already know 4 of them: the trivial and the sign representations, the standard representation St_5 and its tensor with sgn. So the first 4 lines of the table look like

S_5	e	(12)	(123)	(1234)	(12345)	$(12)(34)$	$(12)(345)$
size	1	10	20	30	24	15	20
χ_{triv}	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1	1	-1
χ_{St_5}	4	2	1	0	-1	0	-1
$\chi_{St_5 \otimes \mathsf{sgn}}$	4	-2	1	0	-1	0	1

We now consider the second exterior and symmetric powers of St_5. From Lemma 8.5, we see that the row of $\bigwedge^2 \mathsf{St}_5$ is

$$\chi_{\bigwedge^2 \mathsf{St}_5} = (6, 0, 0, 0, 1, -2, 0).$$

Computing the character pairing, we find

$$\langle \chi_{\bigwedge^2 \mathsf{St}_5}, \chi_{\bigwedge^2 \mathsf{St}_5} \rangle = \frac{1}{120}(36 + 24 + 15 \times 4) = 1,$$

which means that $\bigwedge^2 \mathsf{St}_5$ is irreducible. Now using the sum of squares of the degrees of representations, we find that

$$120 = 1^2 + 1^2 + 4^2 + 4^2 + 6^2 + d_1^2 + d_2^2, \text{ hence } d_1^2 + d_2^2 = 50,$$

where d_1 and d_2 are the degrees of the missing representations. We know that the only one-dimensional representations are the trivial and the sign, hence $d_1 = d_2 = 5$. Let us denote by W and W' these two 5-dimensional representations.

The character of $\mathrm{Sym}^2 \mathsf{St}_5$ is

$$\chi_{\mathrm{Sym}^2 \mathsf{St}_5} = (10, 4, 1, 0, 0, 2, 1).$$

Computing the character pairing, we find

$$\langle \chi_{\mathrm{Sym}^2 \mathsf{St}_5}, \chi_{\mathrm{Sym}^2 \mathsf{St}_5} \rangle = \frac{1}{120}(100 + 160 + 20 + 60 + 20) = 3.$$

Hence $\mathrm{Sym}^2 \mathsf{St}_5$ is the sum of three inequivalent irreducible representations. Indeed, we check easily that

$$\langle \chi_{\mathrm{Sym}^2 \mathsf{St}_5}, \chi_{\mathsf{triv}} \rangle = 1 \text{ and } \langle \chi_{\mathrm{Sym}^2 \mathsf{St}_5}, \chi_{\mathsf{St}_5} \rangle = 1.$$

So $\mathrm{Sym}^5 \mathsf{St}_5$ is the direct sum of the trivial, the standard, and one of the 5-dimensional representations, say W:

$$\mathrm{Sym}^5 \mathsf{St}_5 = \mathsf{triv} \oplus \mathsf{St}_5 \oplus W.$$

In particular, the character of W is

$$\chi_W = (5, 1, -1, -1, 0, 1, 1).$$

Since $\chi_{W \otimes \mathsf{sgn}} = (5, -1, -1, 1, 0, 1, -1) \neq \chi_W$, it follows that $W' = W \otimes \mathsf{sgn}$. This completes the character table.

S_5	e	(12)	(123)	(1234)	(12345)	$(12)(34)$	$(12)(345)$
size	1	10	20	30	24	15	20
χ_{triv}	1	1	1	1	1	1	1
χ_{sgn}	1	-1	1	-1	1	1	-1
χ_{St_5}	4	2	1	0	-1	0	-1
$\chi_{St_5 \otimes \mathsf{sgn}}$	4	-2	1	0	-1	0	1
χ_W	5	1	-1	-1	0	1	1
$\chi_{W \otimes \mathsf{sgn}}$	5	-1	-1	1	0	1	-1

Exercise 8.6. *Let $\mathcal{S}_5$ denote the set of Sylow 5-subgroups of S_5. The elements of order 5 in S_5 are precisely the 5-cycles and there are 24 of them. This means that $|\mathcal{S}_5| = 6$ and each Sylow 5-subgroup is cyclic. The group S_5 acts by conjugation of $\mathcal{S}_5$. Check that this action is 2-transitive, i.e., if (H_1, H_2) and (H_1', H_2') are pairs of Sylow 5-subgroups, then there exists a permutation $\sigma \in S_5$ such that $\sigma(H_1) = H_1'$ and $\sigma(H_2) = H_2'$.*

From this, deduce that the permutation representation $\mathbb{C}\mathcal{S}_5$ decomposes as the direct sum of the trivial representation with one irreducible 5-dimensional representations. (Which 5-dimensional?)

9. Characters and algebraic integers

In this section, we study more closely the character values of irreducible complex representations of a finite group G. Suppose $\rho : G \to GL(V)$ is such a representation with character χ. Recall that for every $g \in G$, since $g^m = e$ for some m, the minimal polynomial of $\rho(g)$ divide $x^m - 1$, hence the minimal polynomial has no repeated factors. Therefore, $\rho(g)$ is diagonalizable and

$$\chi(g) = \mathrm{tr}_V(g) = \sum_{i=1}^{n} \lambda_i,$$

where λ_i are the eigenvalues, which are n-th roots of 1. Here $n = \dim V$.

The question we want to answer first is what kind of complex numbers are the λ_i's.

9.1. **Algebraic integers.**

Definition 9.1. *An number $\alpha \in \mathbb{C}$ is called an* algebraic integer *if α is a root of a monic polynomial $f(x) = x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$ with integer coefficients. Let $\mathbb{A}$ denote the set of all algebraic integers in $\mathbb{C}$.*

Example 9.2. *(1) Every integer is an algebraic integer. (This is clear: if $\alpha \in \mathbb{Z}$, then α is the root of $x - \alpha$.)*
(2) Every root of 1 is an algebraic integer. (If α is an n-th root of 1, then α is a root of $x^n - 1$.)

Lemma 9.3. *If α is a rational number, then α is an algebraic integer if and only if $\alpha \in \mathbb{Z}$. In other words, $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$.*

Proof. Suppose $\alpha = \frac{a}{b}$, where a and b are coprime integers. If $f(\frac{a}{b}) = 0$, we clear denominators and find that

$$a^m + a_1a^{m-1}b + \cdots + a_{m-1}ab^{m-1} + a_mb^m = 0.$$

If p is a prime and p divides b, then from this equation, it follows that p divides a^m, hence a, and this is a contradiction unless $b = 1$. □

We need a criterion to check is a complex number is an algebraic integer.

Proposition 9.4. *Let $(A, +)$ be a nonzero finitely generated subgroup of $(\mathbb{C}, +)$. If $\alpha \in \mathbb{C}$ is such that $\alpha A \subseteq A$, then $\alpha \in \mathbb{A}$.*

Proof. Since A is a finitely generated torsion-free abelian group,

$$A = \mathbb{Z}x_1 \oplus \cdots \oplus \mathbb{Z}x_n,$$

for some $x_i \in \mathbb{C}$. Consider the map

$$m_\alpha : A \to A, \quad m_\alpha(a) = \alpha \cdot a.$$

The condition $\alpha A \subseteq A$ means that the map is well defined. On the other hand, it is clearly a group homomorphism. For every j, $m_\alpha(x_j) = \sum_{i=1}^n a_{ij}x_i$, for some $a_{ij} \in \mathbb{Z}$. Let M be the matrix $M = (a_{ij})$. Then M is the matrix of m_α with respect to $\{x_1, \ldots, x_n\}$. Let $f_M(x) = x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m$ be the characteristic polynomial of M. Since M has integer coefficients, $f_M(x)$ is a monic polynomial with integer coefficients. By the Cayley-Hamilton Theorem

$$f_M(m_\alpha) = 0.$$

Hence $f_M(m_\alpha)a = 0$ for all $a \in A$, which means that $(\alpha^m + a_1\alpha^{m-1} + \cdots + a_{m-1}\alpha + a_m) \cdot a = 0$. Take a to be any nonzero element of A, then it follows that α is a root of $f_M(x)$, hence an algebraic integer.

□

Example 9.5. *If α is any complex number, then we may form*

$$A = \mathbb{Z}[\alpha] = \{\sum_{i=0}^{m} a_i \alpha^i \mid m \in \mathbb{Z}_{\geq 0},\ a_i \in \mathbb{Z}\}.$$

One can show easily that Proposition 9.4 implies that

$$\alpha \text{ is an algebraic integer if and only if } \mathbb{Z}[\alpha] \text{ is a finitely generated subgroup of } (\mathbb{C}, +). \tag{9.1}$$

The first important result about algebraic numbers is the following

Theorem 9.6. *If α and β are algebraic integers, then so are $\alpha + \beta$ and $\alpha\beta$. In other words, $(\mathbb{A}, +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$.*

Proof. Let α, β be algebraic integers with corresponding polynomials $p(x)$ and $q(x)$ of degrees n and m, respectively. Set

$$\mathbb{Z}[\alpha, \beta] = \{ \sum_{0 \leq i < n,\ 0 \leq j < m} a_{ij} \alpha^i \beta^j \mid a_{ij} \in \mathbb{Z}\}.$$

Then $(\mathbb{Z}[\alpha, \beta], +)$ is a subgroup of $(\mathbb{C}, +)$. Notice that in fact $\mathbb{Z}[\alpha, \beta]$ is in fact a nonzero subring of $(\mathbb{C}, +, \cdot)$. This is because any power of α higher than n can be expressed in terms of lower powers, and similarly for β. Also $\mathbb{Z}[\alpha, \beta]$ is clearly finitely generated by $\{\alpha^i \beta^j\}$. Since $\alpha + \beta$ and $\alpha\beta$ belong to $\mathbb{Z}[\alpha, \beta]$, we may apply Proposition 9.4, and deduce that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

Corollary 9.7. *If χ is the character of a representation of G, then $\chi(g) \in \mathbb{A}$.*

Proof. This is because $\chi(g)$ is a sum of algebraic integers (roots of 1). □

9.2. **Frobenius-Burnside divisibility.** To investigate closer the relation between character values and algebraic integers, we need first a result about the ring structure of the centre $Z(\mathbb{C}G)$ of the group algebra $\mathbb{C}G$. Suppose $C_1, \ldots, C_k$ are the conjugacy classes of G. Define

$$z_i = \sum_{g \in C_i} g \in Z(\mathbb{C}G).$$

As seen before, $\{z_i\}$ form a $\mathbb{C}$-basis of $Z(\mathbb{C}G)$.

Lemma 9.8. *There exist nonnegative integers $\mu_{i,j,s}$ such that, in $Z(\mathbb{C}G)$, we have:*

$$z_i \cdot z_j = \sum_{s=1}^{k} \mu_{i,j,s} z_s,$$

for every $1 \leq i, j \leq k$.

Proof. In the proof, we will find a precise formula for the integers $\mu_{i,j,s}$ in fact. Notice that since z_i and z_j are in $Z(\mathbb{C}G)$, then so is $z_i \cdot z_j$. Given that $\{z_i\}$ is a $\mathbb{C}$-basis of $Z(\mathbb{C}G)$, it is then automatic that

$$z_i \cdot z_j = \sum_{s=1}^{k} \mu'_{i,j,s} z_s,$$

for some complex numbers $\mu'_{i,j,s}$, so the content of the lemma is that these numbers can be chosen to be integers. We calculate

$$z_i \cdot z_j = \sum_{g \in C_i,\ h \in C_j} gh = \sum_{x \in G} \mu_{i,j,x} x,$$

where

$$\mu_{i,j,x} = |\{(g, h) \mid g \in C_i,\ h \in C_j,\ gh = x\} \in \mathbb{Z}.$$

If x and x' are conjugate in G, then $\mu_{i,j,x} = \mu_{i,j,x'}$. This is because if $x' = yxy^{-1}$ and $x = gh$, then $x' = (ygy^{-1})(yhy^{-1})$. So we may denote $\mu_{i,j,s} = \mu_{i,j,x}$ for any $x \in C_s$ and rewrite the formula as in the statement of the lemma. □

Recall that, as a consequence of Schur's Lemma, if V is any simple $\mathbb{C}G$-module, every $z \in Z(\mathbb{C}G)$ acts by a scalar $\lambda_z \in \mathbb{C}$. If we denote by λ_i the scalar by which z_i acts, then Lemma 9.8 implies

$$\lambda_i \lambda_j = \sum_{s=1}^{k} \mu_{i,j,s} \lambda_s. \tag{9.2}$$

Lemma 9.9. *The numbers λ_i are algebraic integers.*

Proof. Let A denote the abelian subgroup of $(\mathbb{C}, +)$ generated by $\lambda_1, \ldots, \lambda_k$. Formula (9.2) says that for every i, $\lambda_i \cdot A \subseteq A$. (In fact, a better way is to say that $(A, +, \cdot)$ is a subring of $(\mathbb{C}, +, \cdot)$.) The claim follows by Proposition 9.4. $\square$

Proposition 9.10. *Let C be a conjugacy class of G, $g \in C$, and let χ be an irreducible character of G. Then*

$$\frac{|C|\chi(g)}{\chi(e)}$$

is an algebraic integer.

Proof. This follows from computing λ_i from before in terms of the characters. Let (ρ, V) be the irreducible representation with character χ and think of V as a simple $\mathbb{C}G$-module. Let z_i be the central element given by the sum of elements of our fixed conjugacy class C. Since z_i acts by $\lambda_i \cdot \mathrm{Id}$ on V, we see that

$$\mathrm{tr}_V\, \rho(z_i) = \lambda_i \dim V.$$

On the other hand,

$$\mathrm{tr}_V\, \rho(z_i) = \sum_{x \in C} \mathrm{tr}_V\, \rho(x) = \sum_{x \in G} \chi(x) = |C|\chi(g).$$

Hence

$$\lambda_i = \frac{|C|\chi(g)}{\dim V},$$

and the claim follows from Lemma 9.9. $\square$

Theorem 9.11. *Let χ be an irreducible character of G. Then $\chi(e)$ divides $|G|$.*

Proof. Since χ is irreducible, $\langle \chi, \chi \rangle = 1$, which means

$$\frac{1}{|G|} \sum_{i=1}^{k} |C_i| \overline{\chi}(g_i) \chi(g_i) = 1,$$

where g_i is a representative of C_i. We rewrite this as

$$\sum_{i=1}^{k} \frac{|C_i|\chi(g_i)}{\chi(e)} \chi(g_i^{-1}) = \frac{|G|}{\chi(e)}.$$

By Proposition 9.10, the left hand side is a sum of products of algebraic integers, hence an algebraic integer. Thus $\frac{|G|}{\chi(e)}$ is an algebraic integer. But it is also a rational number, hence an integer. $\square$

While Theorem 9.11 seems at first that it might be useful in getting concrete information about the irreducible representations of a finite group, in practice this isn't so much the case. For example, we know that when G is abelian, then every irreducible representation is one dimensional, so in that case the result would say that 1 divides $|G|$. On the other hand, if $G = S_n$, then $|G| = n!$, so again we can't infer much from the fact that $\chi(e)$ divides $n!$. But the interesting thing about Theorem 9.11 is the proof, the fact that it links algebraic integers to character values in a perhaps surprising way.

Remark 9.12. *It is worth remarking that there exists a refinement of Theorem 9.11, namely that the degree of every irreducible representation divides the index $|G : Z(G)|$, where $Z(G)$ is the centre of G. See* [3, Section 6.5, Proposition 17] *for a clever proof of this fact.*

9.3. **Burnside's p^aq^b Theorem.** We begin by recalling the Orbit-Stabiliser Theorem. If G is a group acting on a set Ω, then, for every $\omega \in \Omega$, there is a natural bijection

$$G/\mathrm{Stab}(\omega) \longleftrightarrow \mathcal{O}_\omega, \quad g\mathrm{Stab}(\omega) \mapsto g\cdot\omega, \tag{9.3}$$

where $\mathrm{Stab}(\omega) = \{g \in G \mid g\cdot\omega = \omega\}$ is the stabiliser and $\mathcal{O}_\omega = \{g\cdot\omega \mid g \in G\}$ is the orbit. In particular, if we apply this to the action of G on itself given by conjugation, we see that

$$|G/C_G(x)| = |C_x|,$$

where $C_G(x) = \{g \in G \mid gxg^{-1} = x\}$ is the centraliser of x, and C_x is the conjugacy class of x.

Ig G is a finite p-group, $G| = p^a$, this means that every conjugacy class in G has order equal to a power of p. Let $C_1, \dots, C_\ell$ be the conjugacy classes in G. Then

$$|C_1| + |C_2| + \cdots + |C_\ell| = |G|.$$

Separate the conjugacy classes into the ones with one element and the ones with more:

$$\sum_{|C_i|=1} |C_i| + \sum_{|C_j|>1} |C_j| = |G|.$$

Notice that an element is its own conjugacy class if and only if it is in the centre $Z(G)$ of G. Using that the order of every conjugacy class is a power of p, we see that

$$|Z(G)| \equiv 0 \pmod p.$$

Since $e \in Z(G)$, this implies that $|Z(G)| \geq p$.

Lemma 9.13. *A finite p-group G with $|G| = p^a$ has a normal subgroup of order p^m for every $0 \leq m \leq a$. In particular, a finite p-group is simple if and only if it is isomorphic to C_p.*

Proof. The second claim follows directly from the first. The first claim can be proved by induction. Assumes it is true for all p-groups of order less than p^a. Suppose $|Z(G)| = p^k \geq p$. Since $|G/Z(G)| = p^{a-k}$, by induction there exists a normal subgroup N of $G/Z(G)$ of order p^{m-k}. But then $NZ(G)$ is a normal subgroup of G of order p^m. □

The main result[5] of the subsection is the following

Theorem 9.14 (Burnside)**.** *A group G of order p^aq^b, where p and q are prime numbers, is simple if and only if G is isomorphic to C_p or to C_q.*

To prove it, we need some preliminary results. Firstly, we need to record some easy facts from Galois theory. Suppose μ is a primitive m-th root of 1. Define $\mathbb{Q}(\mu)$ to be the *cyclotomic field* generated by μ, i.e., the subfield of $\mathbb{C}$ generated by $\mathbb{Q}$ and μ. The minimal polynomial of μ (the m-th cyclotomic polynomial) over $\mathbb{Q}$ divides $x^m - 1$, which means in particular that $\mathbb{Q}(\mu)$ is a finite field extension over $\mathbb{Q}$ (of degree less than n). Define the Galois group

$$\mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) = \{\sigma : \mathbb{Q}(\mu) \to \mathbb{Q}(\mu) \text{ field isomorphism} \mid \sigma(\alpha) = \alpha, \text{ for all } \alpha \in \mathbb{Q}\}. \tag{9.4}$$

This is a group with respect to composition. For every $1 \leq k \leq m$ such that $\mathrm{hcf}(k, m) = 1$, define

$$\sigma_k : \mathbb{Q}(\mu) \to \mathbb{Q}(\mu), \quad \sigma_k \mid_{\mathbb{Q}} = \mathrm{Id},\ \sigma_k(\mu) = \mu^k\}.$$

Since σ_k maps μ to another primitive m-th root of 1, it is easy to see that

$$\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) \text{ and } \sigma_k \circ \sigma_\ell = \sigma_{k\ell}.$$

In fact, it isn't difficult to prove the following

Proposition 9.15. $\mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) = \{\sigma_k \mid 1 \leq k \leq m,\ \mathrm{hcf}(k, m) = 1\} \cong ((\mathbb{Z}/m\mathbb{Z})^\times, \cdot)$. *Moreover, if $\alpha \in \mathbb{Q}(\mu)$ is such that $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$, then $\alpha \in \mathbb{Q}$.*

Now we can prove a lemma about the average of roots of unity.

[5]The proof of the theorem is not examinable

Lemma 9.16. *If $\lambda_1, \dots, \lambda_n$ are roots of unity such that their average*

$$a = \frac{\lambda_1 + \cdots + \lambda_n}{n}$$

is an algebraic integer, then either $a = 0$ or $\lambda_1 = \lambda_2 = \cdots = \lambda_n$.

Proof. Without loss of generality, we may assume that all λ_i are m-th roots of 1. Let μ be a primitive m-th root of 1, as before. Then $\lambda_i \in \mathbb{Q}(\mu)$ for all i. Define

$$\alpha = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})} \sigma(a) \in \mathbb{Q}(\mu).$$

It is clear from the definition that $\sigma(\alpha) = \alpha$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$, which by Proposition 9.15, means that $\alpha \in \mathbb{Q}$.

On the other hand, every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$ maps roots of unity to roots of unity, hence $\sigma(\alpha)$ is an algebraic number (because α is) for all σ. Hence α is an algebraic number and a rational number, so it is an integer.

Finally, $|a| \leq 1$, which means that $|\sigma(a)| \leq 1$ for all σ. Thus $|\alpha| \leq 1$ and α is an integer. There are two cases: if $\alpha = 0$, then one of the $\sigma(a) = 0$, but then $a = 0$, as well. Or, if $|\alpha| = 1$, we must have $|\sigma(a)| = 1$ for all σ, so $|a| = 1$. But this implies that $\lambda_1 = \cdots = \lambda_n$. □

This lemma can be rephrased as follows.

Lemma 9.17. *Let χ be the character of a representation $\rho : G \to GL(V)$ of a finite group G. Suppose $g \in G$ is such that $\frac{\chi(g)}{\chi(e)}$ is an algebraic integer. Then one of the following holds:*

(1) either $\chi(g) = 0$,
(2) or $\rho(g)$ is a scalar multiple of the identity in $GL(V)$.

In particular, suppose that G is a nonabelian simple group, $g \neq e$, and χ is an irreducible nontrivial character. If $\frac{\chi(g)}{\chi(e)}$ is an algebraic integer, then $\chi(g) = 0$.

Proof. If $\lambda_1, \dots, \lambda_n$ are the eigenvalues of $\rho(g)$, then we see that the condition is just the same as in the previous lemma: $\frac{\lambda_1 + \cdots + \lambda_n}{n}$ is an algebraic integer. The two cases are exactly the ones from before.

For the second part, we need to show that $\rho(g)$ can't be a multiple of the identity. Suppose it is, e.g., $\rho(g) = \lambda \,\mathrm{Id}_V$ for some $\lambda \in \mathbb{C}$. By assumption, ρ is an irreducible nontrivial G-representation. Since G is a simple group, ρ must be faithful, and therefore, by the first isomorphism theorem, $\rho(G) \cong G$. This means that $\rho(G)$ is a simple group too. But $\rho(g)$ is a central element of $\rho(G)$, which means that $\rho(G)$ must be abelian simple group (cyclic of prime order), and this is a contradiction with the assumption. □

Proposition 9.18. *Let G be a nonabelian simple group and let C be a conjugacy class in G, $C \neq \{e\}$. Then $|C|$ is not a prime power.*

Proof. Suppose $|C| = q^k$ for some prime number q and $k \in \mathbb{Z}_{\geq 0}$. Fix a representative $g \in C$. Using the column orthogonality of characters, $g \neq e$,

$$\sum_{\chi \in \mathrm{Irr}\ G} \chi(g)\chi(e) = 0,$$

which implies

$$1 + \sum_{\chi \in \mathrm{Irr}\ G \setminus \{\chi_{\mathsf{triv}}\}} \chi(g)\chi(e) = 0. \tag{9.5}$$

We claim that for every $\chi \neq \chi_{\mathsf{triv}}$, either $q \mid \chi(e)$ or $\chi(g) = 0$. Suppose q does not divide $\chi(e)$. Then $\mathrm{hcf}(|C|, \chi(e)) = 1$, since $|C| = q^k$. So there exist integers $a, b \in \mathbb{Z}$ such that $a|C| + b\chi(e) = 1$. Multiply by $\frac{\chi(g)}{\chi(e)}$ and get

$$a\frac{|C|\chi(g)}{\chi(e)} + b\chi(g) = \frac{\chi(g)}{\chi(e)}.$$

All the elements in the left hand side are algebraic integers (the difficult bit was done in Proposition 9.10), hence $\frac{\chi(g)}{\chi(e)}$ is also an algebraic integer. By Lemma 9.17, it follows that $\chi(g) = 0$, so the claim is proved.

Returning to (9.5), taking mod q, we now see that we may write $\sum_{\chi\in\mathrm{Irr}\ G\setminus\{\chi_{\mathrm{triv}}\}}\chi(g)\chi(e) = q\alpha$ for some algebraic integer α. But then $\frac{1}{q} = -\alpha$ is an algebraic integer and this is a contradiction, since $\frac{1}{q}$ is rational but not an integer.

□

We can now finally prove Theorem 9.14.

Proof of Theorem 9.14. If $a = 0$ (or $b = 0$), then Lemma 9.13 gives the statement in the theorem. Suppose $a \geq 1$ and $b \geq 1$. Applying Sylow's Theorem, we see that G has a Sylow subgroup H of order $p^a > 1$. By Lemma 9.13 again, $Z(H) \neq \{e\}$. Let $g \in Z(H)$ be an element, $g \neq e$. Let C be the conjugacy class of g in G.

Since $g \in Z(H)$, we have $H \subseteq C_G(H)$. But then

$$|G : H| = |G : C_G(g)| \cdot |C_G(g) : H|.$$

Since $|G : H| = q^b$ and $|C| = |G : C_G(g)|$, we have that the order of C is a power of q. But this is a contradiction with Proposition 9.18. □

Appendix A. Unitary representations

In this appendix, we will work with the field $\mathsf{k} = \mathbb{C}$.

A.1. Inner products.

Definition A.1. *Let V be a $\mathbb{C}$-vector space. An inner product on V is a pairing $(\ ,\ ) : V \times V \to \mathbb{C}$ which is:*

(i) sesquilinear: $(\lambda_1 v_1 + \lambda_2 v_2, u) = \overline{\lambda}_1(v_1, u) + \overline{\lambda}_2(v_2, u)$, $v_1, v_2, u \in V$, $\lambda \in \mathbb{C}$;
(ii) hermitian: $(v, u) = \overline{(u, v)}$;
(iii) positive-definite: $(v, v) \geq 0$ for all $v \in V$, and if $(v, v) = 0$ then $v = 0$.

A subset $\{v_i : i \in I\}$ of V is called orthogonal if $(v_i, v_j) = 0$ for all $i \neq j$. It is called orthonormal if, in addition, $(v_i, v_i) = 1$ for all i.

Example A.2. *(1) Let $V = \mathbb{C}^n$ be the standard n-dimensional $\mathbb{C}$-vector space. Set $(v, u) = \sum_{i=1}^n \overline{v}_i u_i$, where $v = (v_i)_{1\leq i\leq n}$ and $u = (u_i)_{1\leq i\leq n}$ are vectors in V. This is the standard inner product on V.*

(2) [6] Suppose X is a measure space with measure μ. Let $L^2(X)$ denote the space of integrable functions $f : X \to \mathbb{C}$ such that

$$||f||_2 := (\int_X |f(x)|^2\ d\mu(x) < \infty)^{1/2}. \tag{A.1}$$

The space $L^2(X)$ is a metric space with the metric $d_2(f, g) = ||f - g||_2$. An inner product on $L^2(X)$ is defined by

$$(f, g)_2 = \int_X \overline{f(x)} g(x)\ d\mu(x). \tag{A.2}$$

Hölder's inequality says that $|(f, g)_2| \leq ||f||_2||g||_2$, so this pairing takes finite values indeed. It is moreover true that $L^2(X)$, just as $\mathbb{C}^n$, is a complete metric space; such spaces are called Hilbert spaces.

Lemma A.3. *Let V be a $\mathbb{C}$-vector space with an inner product $(\ ,\ )$ and let U be a subspace. Then*

$$U^\perp = \{v \in V \mid (v, u) = 0, \text{ for all } u \in U\}$$

is a subspace of V and $U \cap U^\perp = 0$. If V is finite dimensional, then $V = U \oplus U^\perp$.

Proof. The fact that $U^\perp$ is a subspace follows immediately from the conjugate-linearity of $(\ ,\ )$ with respect to the first variable. For the second claim, suppose $u \in U \cap U^\perp$. Then $(u, u) = 0$, hence $u = 0$.

For the last claim, let $\{u_1, \ldots, u_m\}$ be an orthonormal basis of U. (This exists by the Gram-Schmidt procedure.) Then we may extend this to a basis $\{u_1, \ldots, u_m, w_1, \ldots, w_l\}$ of V. Again by Gram-Schmidt, we make this into an orthonormal basis $\{u_1, \ldots, u_m, w'_1, \ldots, w'_l\}$. The span of $\{w'_1, \ldots, w'_l\}$ is in $U^\perp$ (since the elements are orthogonal to U), and since $U \cap U^\perp = 0$, we have that they form a basis of $U^\perp$. The claim follows. □

---

[6] If you took Part A Integration.

A better way to phrase the last part of the proof is to define the projection onto U by

$$p : V \to U, \quad p(v) = \sum_{i=1}^{m} (v, u_i) u_i.$$

Notice that $p(u) = u$ for all $u \in U$, hence $p(p(v)) = p(v)$ for all $v \in V$. For every $v \in V$, $v = p(v) + (v - p(v))$, and $v - p(v) \in \ker p_U = U^\perp$.

This means that if we have a well-defined projection onto U even if V is infinite dimensional, then we can still conclude that $V = U \oplus U^\perp$. This is precisely why for infinite dimensional inner product spaces, one needs to assume completeness. The basic result is the following.

Theorem A.4 (See Part A Metric Spaces)**.** *Let V be a Hilbert space with metric d and let U be a closed subspace of V. Then for every $v \in V$,*

$$d(v, U) = \inf\{d(v, u) : u \in U\} \geq 0$$

is attained at some point in U. Define $p_U(v)$ to be the point of U where $d(v, U)$ is attained. Then $p_U : V \to U$ is a projection of V onto U and $U^\perp = \ker p_U$. Moreover,

$$V = U \oplus U^\perp.$$

A.2. **Algebras with star operations.** The goal of this subsection is to explain how semisimple modules occur naturally in representation theory.

Let A be a $\mathbb{C}$-algebra (not necessarily finite dimensional). A star operation on A is a ring anti-automorphism $\kappa : A \to A$, meaning that

(i) $\kappa(a + b) = \kappa(a) + \kappa(b)$;
(ii) $\kappa(ab) = \kappa(b)\kappa(a)$, $a, b \in A$,

and in addition

(iii) κ is conjugate-linear, $\kappa(\lambda a) = \overline{\lambda}\kappa(a)$, $\lambda \in \mathbb{C}$, $a \in A$, and
(iv) κ is an involution $\kappa^2 = \mathrm{Id}_A$.

This definition looks a bit complicated at first, but there are natural examples.

Example A.5. *(i) If A is an abelian algebra, then we would like to say that $\kappa = \mathrm{Id}_A$ is a star operation. But this doesn't quite work because of the conjugate-linear property. One non-canonical way to fix it is to take a $\mathbb{C}$-basis $\{a_i : i \in I\}$ of A and define $\kappa(\sum_{finite} \lambda_i a_i) = \sum_{finite} \overline{\lambda} a_i$.*

(ii) Let $A = M_n(\mathbb{C})$. Then we may take

$$\kappa(X) = \overline{X}^t$$

for all matrices $X \in M_n(\mathbb{C})$.

(iii) Let $A = \mathbb{C}G$, for a group G. The natural star operation is

$$\kappa(\sum \lambda_g g) = \sum \overline{\lambda}_g g^{-1}.$$

Definition A.6. *Let A be a $\mathbb{C}$-algebra with a star operation κ and let M be an A-module. We say that M is κ-preunitary if M has a positive-definite inner product $(\ ,\ )_M$ which is κ-invariant, i.e.:*

$$(a \cdot m_1, m_2)_M = (m_1, \kappa(a) \cdot m_2)_M, \quad a \in A,\ m_1, m_2 \in M. \tag{A.3}$$

We say that M is (κ-)unitary if M is a Hilbert space.

We see from the definition why we need κ to be an anti-automorphism:

$$((ab)\cdot m_1, m_2)_M = (a\cdot(b\cdot m_1), m_2)_M = (b\cdot m_1, \kappa(a)\cdot m_2)_M = (m_1, \kappa(b)\cdot(\kappa(a)\cdot m_2)_M = (m_1, (\kappa(b)\kappa(a))\cdot m_2)_M.$$

On the other hand, this has to equal $(m_1, \kappa(ab) \cdot m_2)_M$. This justifies the condition $\kappa(ab) = \kappa(b)\kappa(a)$.

The main first property of preunitary modules is the following observation.

Proposition A.7. *Suppose that M is a preunitary A-module. If N is a submodule of M, then $N^\perp$ is also a submodule of M and $N \cap N^\perp = 0$.*

Proof. We need to prove that $N^\perp$ is a submodule, the rest following from the statements for vector spaces. Let $m \in N^\perp$ and $a \in A$. Then

$$(a \cdot m, n)_M = (m, \kappa(a) \cdot n = 0, \text{ for all } n \in N.$$

By definition, this means that $a \cdot m \in N^\perp$ as well. □

Corollary A.8. *Suppose M is a unitary A-module and N a closed submodule of M. Then $M = N \oplus N^\perp$ as A-modules.*

Proof. This is immediate from the previous proposition and the decomposition of Hilbert spaces from before. □

Remark A.9. *The decomposition in Corollary A.8 applies in particular whenever M is a finite dimensional (pre)unitary A-module and N is any submodule of M. Corollary A.8 says that unitary modules are completely reducible, and in fact more, since we have a canonical complement for any (closed) submodule.*

Proposition A.10. *Let M be a finite dimensional A-module. Then M is semisimple if and only if it is completely reducible.*

Proof. We proved this in the lectures. □

A.3. **Finite groups.** Let G be a finite group and $A = \mathbb{C}G$ with $\kappa(g) = g^{-1}$ as in Example A.5. The following result can be viewed as an easy, conceptual proof of Maschke's Theorem in this setting.

Theorem A.11. *Every finite dimensional $\mathbb{C}G$-module is unitary. Therefore $\mathbb{C}G$ is a semisimple finite-dimensional $\mathbb{C}$-algebra.*

Proof. Let V be a finite dimensional $\mathbb{C}G$-module and let $(\ ,\ )$ be any positive definite inner product on V. Such an inner product exists, because as a $\mathbb{C}$-vector space V is isomorphic to $\mathbb{C}^n$ for $n = \dim V$, and we can just take the standard inner product on $\mathbb{C}^n$. We make $(\ ,\ )$ G-invariant by averaging, i.e., define

$$(u, v)_V := \frac{1}{|G|} \sum_{g \in G} (g \cdot u, g \cdot v). \tag{A.4}$$

Then $(\ ,\ )_V$ is indeed G-invariant: for $h \in G$,

$$\begin{aligned}(h \cdot u, v)_V &= \frac{1}{|G|} \sum_{g \in G} (gh \cdot u, g \cdot v) = \frac{1}{|G|} \sum_{g' \in G} (g' \cdot u, g' h^{-1} \cdot v) \quad (g' = gh) \\ &= (u, h^{-1} \cdot v)_V.\end{aligned}$$

Since $(\ ,\ )_V$ is G-invariant, it is easy to see that it is also A-invariant. Moreover $(\ ,\ )_V$ is sesquilinear since $(\ ,\ )$ is. Finally,

$$(u, u)_V = \frac{1}{|G|} \sum_{g \in G} (g \cdot u, g \cdot u) \geq 0,$$

and it is 0 if and only if $(g \cdot u, g \cdot u) = 0$ for all g, but then $(u, u) = 0$ hence $u = 0$. So indeed V is unitary with respect to $(\ ,\ )_V$. □

A.4. **L^2-spaces.** This part is non-examinable, but I hope you may still find it interesting. We will look at two examples, $G = S^1$ and $G = (\mathbb{R}, +)$. Recall, that in general, if a group G acts on a set X, then it acts on the space of functions $\mathcal{F}(X) = \{f : X \to \mathbb{C}\}$ by the left-regular representation

$$(g \cdot f)(x) = f(g^{-1}x), \quad g \in G,\ x \in X. \tag{A.5}$$

This is a representation of G. If X is a measure space with a measure μ and the action of G preserves the measure, i.e.,

$$\mu(g \cdot B) = \mu(B), \text{ for every measurable set } B \subseteq X, \tag{A.6}$$

then G acts on $L^2(X)$. In other words, if $f \in L^2(X)$, then $g \cdot f \in L^2(X)$. In this way, $L^2(X)$ becomes a unitary representation of G.

Let $\mu_{\mathbb{R}}$ denote the Lebesgue measure on $\mathbb{R}$. This measure is translation invariant, namely B is a measurable set if and only $B+x$ is a measurable set for all $x \in \mathbb{R}$ and moreover

$$\mu_{\mathbb{R}}(B) = \mu(B+x).$$

If $G = (\mathbb{R}, +)$, then this says exactly that $\mu_{\mathbb{R}}$ is G-invariant. Hence $L^2(\mathbb{R})$ is naturally a unitary representation of $(\mathbb{R}, +)$.

Using again that $\mu_{\mathbb{R}}$ is translation invariant, it is clear that $\mu_{\mathbb{R}}$ defines a well-defined measure on

$$S^1 \cong \mathbb{R}/\mathbb{Z}, \quad (x \in \mathbb{R}/\mathbb{Z} \mapsto e^{2\pi i x} \in S^1),$$

which we denote by μ_{S^1}. Similarly $G = S^1$ acts on $L^2(S^1)$ and this is a unitary S^1-representation.

Notice that both S^1 and $\mathbb{R}$ carry natural topologies, but the difference is that S^1 is compact, whereas $\mathbb{R}$ is non-compact. This difference will be reflected in the decompositions of $L^2(G)$.

Since S^1 and $\mathbb{R}$ are abelian groups, we are interested first in the description of the one-dimensional representations. To account for the topology of these groups, we look at continuous group homomorphisms $\rho : G \to \mathbb{C}^\times$. Finally, since we are interested in the decomposition of $L^2(G)$, we restrict to unitary representations, which means that the image of ρ is in S^1. This makes no difference for S^1: a similar argument to that in Theorem A.11 shows that every finite dimensional representation of S^1 is unitary. (Instead of averaging using a sum as for finite groups, we average using an integral for a compact group.) But it makes a difference for $\mathbb{R}$ which has one-dimensional non-unitary representations.

Similarly to the case of finite abelian groups, we may define the Pontrijagin dual of $G = S^1$ or $\mathbb{R}$, by setting

$$\widehat{G} = \{\rho : G \to S^1 \mid \rho \text{ continuous group homomorphism}\}.$$

Lemma A.12. *(1) The irreducible unitary continuous representations of S^1 over $\mathbb{C}$ are the (one-dimensional) group homomorphisms*

$$\rho_n : S^1 \to S^1, \quad \rho_n(z) = z^n, \quad z \in S^1,$$

for every $n \in \mathbb{Z}$. In other words, $\widehat{S^1} \cong (\mathbb{Z}, +)$.

(2) The irreducible unitary continuous representations of $(\mathbb{R}, +)$ over $\mathbb{C}$ are the (one-dimensional) group homomorphisms

$$\rho_x : (\mathbb{R}, +) \to S^1, \quad \rho_x(y) = e^{ixy},$$

for every $x \in \mathbb{R}$. In other words, $\widehat{(\mathbb{R}, +)} \cong (\mathbb{R}, +)$.

Proof. Left as an exercise for now. □

We need a generalization of the notion of direct sums for Hilbert spaces.

Definition A.13. *Suppose that V_i, $i \in I$ is a family of Hilbert spaces with inner products $(\ ,\ )_{V_i}$ and norms $||\ ||_{V_i}$ indexed by a countable set I. The Hilbert space direct sum is*

$$\widehat{\bigoplus}_{i\in I} V_i = \{(v_i)_{i\in I} \in \prod_{i\in I} V_i \mid \sum_{i\in I} ||v_i||_{V_i} < \infty\}.$$

One endows $\widehat{\bigoplus}_{i\in I} V_i$ with a an inner product

$$((v_i), (u_i)) := \sum_{i\in I} (v_i, u_i)_{V_i}.$$

This makes $\widehat{\bigoplus}_{i\in I} V_i$ into a Hilbert space.

When the set I is finite, the Hilbert space direct sum is the same as the usual notion of a direct sum.

Theorem A.14. *As a representation of S^1,*

$$L^2(S^1) \cong \widehat{\bigoplus_{n\in\mathbb{Z}}} \rho_n,$$

where ρ_n is as in Lemma A.12.

Proof. This is nothing but the main result of Fourier series, namely that a periodic L^2-function can be decomposed uniquely into a Fourier series. □

Now we turn to $(\mathbb{R},+)$. To simplify notation, we write dx in place of $d\mu_B(x)$ in the integration with respect to the Lebesgue measure. Suppose $f:\mathbb{R}\to\mathbb{C}$ is an integrable function. Recall the Fourier transform of f:

$$\hat{f}:\mathbb{R}\to\mathbb{C},\quad \hat{f}(\xi)=\int_{\mathbb{R}} f(y)e^{-iy\xi}\,dy,\quad \xi\in\mathbb{R}. \tag{A.7}$$

The translation property of the Fourier transform says, in our notation, that

$$\widehat{(x_0\cdot f)}(\xi)=e^{-ix_0\xi}\hat{f}(\xi),\quad x_0\in\mathbb{R},\ \xi\in\mathbb{R}. \tag{A.8}$$

We recall that $(x_0\cdot f)(y)=f(y-x_0)$ is the left regular action of $\mathbb{R}$ on $L^2(\mathbb{R})$ (or any functions on $\mathbb{R}$).

Remark A.15. *Let ρ_x, $x\in\mathbb{R}$ be an irreducible unitary representation of $(\mathbb{R},+)$. We can think of $\widehat{\rho}_x$ as the delta function supported at x, a "function" which is nonzero only at x ("supported at x) with "infinite value" at x. (This leads to the notion of distribution in analysis.)*

The Fourier inversion theorem says that

$$f(x)=\int_{\mathbb{R}}\hat{f}(\xi)e^{ix\xi}\,d\xi. \tag{A.9}$$

In representation theoretic terms, you want to think of this formula as saying that there exists a measure $\hat{\mu}$ on $\widehat{\mathbb{R}}=\widehat{(\mathbb{R},+)}$ (which can be seen concretely here by identifying $\widehat{(\mathbb{R},+)}$ with $\mathbb{R}$ as in Lemma A.12) such that

$$f(x)=\int_{\widehat{\mathbb{R}}}\hat{f}(\xi)\,d\hat{\mu}(\rho_x(\xi)). \tag{A.10}$$

The question is to describe the $\mathbb{R}$-invariant subspaces (the subrepresentations) of $L^2(\mathbb{R})$. Let S be a measurable subset of $\mathbb{R}$. Consider

$$L^2(\mathbb{R})_S=\{f\in L^2(\mathbb{R})\mid \hat{f}=0\text{ almost everywhere on }\mathbb{R}\setminus S\}. \tag{A.11}$$

The subspace $L^2(\mathbb{R})$ is nonzero if and only if S has positive measure.

Theorem A.16. *The $\mathbb{R}$-invariant closed subspaces of $L^2(\mathbb{R})$ are precisely $L^2(\mathbb{R})_S$ for all measurable sets S in $\mathbb{R}$.*

Proof. Later. □

In a measure space (X,μ), one says that a measurable set $S\subset X$ is an atom if $\mu(S)>0$ and whenever S' is measurable and $\mu(S')<\mu(S)$, necessarily $\mu(S')=0$.

Lemma A.17. *The Lebesgue measure on $\mathbb{R}$ does not have atoms.*

Proof. Left as an exercise. □

Corollary A.18. *As a representation of $(\mathbb{R},+)$, the unitary representation $L^2(\mathbb{R})$ is completely reducible, but not semisimple.*

Proof. As a unitary representation, we already know that $L^2(\mathbb{R})$ is completely reducible (in the Hilbert space sense, i.e., with closed subspaces). On the other hand, from Theorem A.16, we know that the subrepresentations are $L^2(\mathbb{R})_S$, for measurable sets S. Notice that if $S_1\subseteq S_2$, then $L^2(\mathbb{R})_{S_1}\subseteq L^2(\mathbb{R})_{S_2}$. But since $\mathbb{R}$ does not have atoms, it follows that every nonzero $L^(\mathbb{R})_S$ has a proper nonzero subrepresentation. This means that $L^2(\mathbb{R})$ doesn't have any simple subrepresentations, and therefore, it cannot be semisimple. □

Thus the representation $L^2(\mathbb{R})$ does not decompose as a (Hilbert) direct sum of irreducible representations. However, the Fourier inversion formula (A.10) indicates that there is a "continuous", integral decomposition into the one-dimensional irreducible unitary representations ρ_x, $x\in\mathbb{R}$.

References

[1] K. Erdmann, *Algebras*, Oxford notes.
[2] P. Etingof et al, *Introduction to representation theory*, MIT, online notes.
[3] J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics **42**, Springer-Verlag New York, 1977.

(D. Ciubotaru) Mathematical Institute, University of Oxford
E-mail address: `dan.ciubotaru@maths.ox.ac.uk`