Leandro Vendramin

Representation theory of algebras

Notes

Thursday 9th March, 2023

Preface

The notes correspond to the master course *Representation theory of algebras* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into twelve two-hour lectures.

Most of the material is based on standard results of the representation theory of finite groups. Basic texts on representation theory are [2] and [21].

Thanks go to Wannes Malfait, Silvia Properzi.

This version was compiled on Thursday 9th March, 2023 at 14:53.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Artin–Wedderburn theorem

We first review the basic definitions concerning finite-dimensional semisimple algebras. Proofs can be found in the notes to the course *Associative Algebras*, see lectures 1, 2 and 3.

Our base field will be the field $\mathbb{C}$ of complex numbers.

A (complex) **algebra** A is a (complex) vector space with an associative multiplication $A \times A \to A$ such that

$$a(\lambda b + \mu c) = \lambda(ab) + \mu(ac), \quad (\lambda a + \mu b)c = \lambda(ac) + \mu(bc)$$

for all $a, b, c \in A$. If A contains an element $1_A \in A$ such that $1_A a = a 1_A = a$ for all $a \in A$, then A is a unitary algebra.

Our algebras will be finite-dimensional. Clearly, $\mathbb{C}$ is an algebra. Other examples of algebras are $\mathbb{C}[X]$ and $M_n(\mathbb{C})$.

A (left) **module** M (over a unitary algebra A) is an abelian group M together with a map $A \times M \to M$, $(a, m) \mapsto am$, such that $1_A m = m$ for all $m \in M$ and $a(bm) = (ab)m$ and $a(m + m_1) = am + am_1$ for all $a, b \in A$ and $m, m_1 \in M$. A **submodule** N of M is a subgroup N such that $an \in N$ for all $a \in A$ and $n \in N$.

Exercise 1.1. Let A be a finite-dimensional algebra. If M is an A-module, then M is a vector space with $\lambda m = (\lambda 1_A)m$ for $\lambda \in \mathbb{C}$ and $m \in M$. Moreover, M is finitely generated if and only if M is finite-dimensional.

A module M is said to be **simple** if $M \neq \{0\}$ and $\{0\}$ and M are the only submodules of M. A finite-dimensional module M is said to be **semisimple** if M is a direct sum of finitely many simple submodules. Clearly, simple modules are semisimple. Moreover, any finite direct sum of semisimples is semisimple.

A finite-dimensional algebra A is said to be **semisimple** if every finitely-generated A-module is semisimple.

Theorem 1.2 (Artin–Wedderburn). *Let A be a complex finite-dimensional semisimple algebra, say with k isomorphism classes of simple modules. Then*

$$A \simeq M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$$

for some $n_1, \ldots, n_k \in \mathbb{Z}_{>0}$.

We also give some basic facts on the Jacobson radical of finite-dimensional algebras. If A is a finite-dimensional algebra, the **Jacobson radical** is defined as

$$J(A) = \bigcap \{M : M \text{ is a maximal left ideal of } A\}.$$

It turns out that $J(A)$ is an ideal of A. If A is unitary, then Zorn's lemma implies that there a maximal left ideal of A and hence $J(A) \neq A$.

An ideal I of A is said to be **nilpotent** if $I^m = \{0\}$ for some m, that is $x_1 \cdots x_m = 0$ for all $x_1, \ldots, x_m \in I$. One proves that the Jacobson radical of A contains every nilpotent ideal of A. An important fact is that

$$\begin{aligned} A \text{ is semisimple} &\iff J(A) = \{0\} \\ &\iff A \text{ has no non-zero nilpotent ideals.} \end{aligned}$$

§2. Kolchin's theorem

In this section it will be useful to consider non-unitary algebras.

Definition 2.1. Let A be an algebra (possibly without one). An element $a \in A$ is said to be **nilpotent** if $a^n = 0$ for some $n \geq 1$. The algebra A is said to be **nil** if every element $a \in A$ is nilpotent.

Nilpotent elements are also called nil elements.

Example 2.2. Let $A = M_2(\mathbb{R})$. Then $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent.

Definition 2.3. An algebra A is said to be **nilpotent** if there exists $n \geq 1$ such that every product $a_1 a_2 \cdots a_n$ of n elements of A is zero.

Nilpotent algebras are trivially nil, whereas nil algebras may not be nilpotent.

Exercise 2.4. Give an example of a nil algebra that is not nilpotent.

Note that nil algebras cannot be unitary.

Proposition 2.5. *Let A be an algebra. There exists an algebra B with one 1_B and an ideal I of B such that $B/I \simeq \mathbb{C}$ and $I \simeq A$.*

Sketch of the proof. Let $B = \mathbb{C} \times A$. The multiplication

$$(\lambda, u)(\mu, v) = (\lambda\mu, \lambda v + \mu u + uv)$$

turns B into an algebra with identity $(1, 0)$. The subset $I = \{(0, a) : a \in A\}$ is an ideal of B. Then $I \simeq A$ and $B/I \simeq \mathbb{C}$. □

Exercise 2.6. Let $A_1, \dots, A_k$ be algebras. Prove that the ideals of $A_1 \times \cdots \times A_k$ are of the form $I_1 \times \cdots \times I_k$, where each I_j is an ideal of A_j.

Exercise 2.7. Prove that the non-zero ideals of $\prod_{i=1}^{k} M_{n_i}(\mathbb{C})$ are unitary algebras.

Proposition 2.8. *Let A be non-zero algebra (possibly without one). If A does not have non-zero nilpotent ideals, then A is a unitary algebra.*

Proof. Let B be a unitary algebra such that there exists an ideal I of B with $B/I \simeq \mathbb{C}$ and $I \simeq A$ (see Proposition 2.5). Let J be a nilpotent ideal of B. Since $J \cap I \subseteq I$ is a nilpotent ideal of A, $J \cap I = \{0\}$. Thus

$$J \simeq J/(J \cap I) \simeq (I+J)/I$$

is a nilpotent ideal of $B/I \simeq \mathbb{C}$. Thus $J = \{0\}$ and hence B is semisimple. By Artin–Wedderburn, $B \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C})$. Since A is isomorphic to an ideal of B, Exercise 2.7 shows that A is a unitary algebra. □

Now we prove another nice result of Wedderburn:

Theorem 2.9 (Wedderburn). *Let A be a complex finite-dimensional algebra. If A is generated (as a vector space) by nilpotent elements, then A is nilpotent.*

We shall need a lemma.

Lemma 2.10. *The vector space $M_n(\mathbb{C})$ does not have a basis of nilpotent matrices.*

Proof. If $\{A_1, \dots, A_{n^2}\}$ is a basis of $M_n(\mathbb{C})$ consisting of nilpotent matrices, then there exist $\lambda_1, \dots, \lambda_{n^2} \in \mathbb{C}$ such that

$$E_{11} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} = \sum_{i=1}^{n^2} \lambda_i A_i. \tag{1.1}$$

Note $\operatorname{trace}(A_i) = 0$ for all $i \in \{1, \dots, n\}$, as every A_i is nilpotent. Apply trace to (1.1) to obtain that $1 = \operatorname{trace}(E_{11}) = \sum \lambda_i \operatorname{trace}(A_i) = 0$, a contradiction. □

Now we prove Wedderburn's theorem. Note that the theorem can be extended to any algebraically closed field. We state and prove Wedderburn's theorem in the case of complex numbers to simplify the presentation.

Proof of Theorem 2.9. We proceed by induction on $\dim A$. If $\dim A = 1$ and there exists a nilpotent element $a \in A$ such that $\{a\}$ is a basis of A, then A is nilpotent, as every element of A is nilpotent, as it is of the form λa for some $\lambda \in \mathbb{C}$.

Assume now that $\dim A > 1$. Since $J(A)$ is nilpotent, $J(A)^n = \{0\}$ for some n.

If $J(A) = A$, the result trivially holds.

If $J(A) \neq \{0\}$, $\dim A/J(A) < \dim A$ and hence $A/J(A)$ is nilpotent by the inductive hypothesis, say $(A/J(A))^m = \{0\}$. Let $\pi\colon A \to A/J(A)$ be the canonical map

and $N = nm$. We claim that $A^N = \{0\}$. Let $a_1, \dots, a_N \in A$. Write $a_1 \cdots a_N = x_1 \cdots x_n$ for some $x_1 \cdots x_n \in A$. For example,

$$\begin{aligned} x_1 &= a_1 a_2 \cdots a_m, \\ x_2 &= a_{m+1} a_{m+2} \cdots a_{2m}, \\ &\vdots \end{aligned}$$

Since

$$\pi(x_1) = \pi(a_1 a_2 \cdots a_m) = \pi(a_1)\pi(a_2) \cdots \pi(a_m) = 0,$$

it follows that $x_1 \in J(A)$. Similarly, $\pi(x_j) \in J(A)$ for every $j \in \{1, \dots, n\}$. Thus,

$$a_1 a_2 \cdots a_N = x_1 x_2 \cdots x_n \in J(A)^n = \{0\}.$$

Thus A is nilpotent.

If $J(A) = \{0\}$, then A is semisimple. By Artin–Wedderburn, $A \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C})$, a contradiction to the previous lemma. □

Definition 2.11. Let $V = \mathbb{C}^n$ (column vectors). A **complete flag** in V is a sequence $(V_1, V_2, \dots, V_n)$ of vector spaces such that

$$\{0\} \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_n = V.$$

If $(V_1, \dots, V_n)$ is a complete flag, then $\dim V_i = i$ for all $i \in \{1, \dots, n\}$. Let $\{e_1, \dots, e_n\}$ be the standard basis of $\mathbb{C}^n$. The **standard flag** is the sequence $(E_1, \dots, E_n)$, where $E_i = \langle e_1, \dots, e_i \rangle$ for all $i \in \{1, \dots, n\}$.

Note that $\mathbf{GL}_n(\mathbb{C})$ acts on the set of complete flags of V by

$$g \cdot (V_1, \dots, V_n) = (T_g(V_1), \dots, T_g(V_n)),$$

where $T_g : V \to V$, $x \mapsto gx$.

The action is *transitive*, which means that if $(V_1, \dots, V_n)$ is a complete flag, then there exists $g \in \mathbf{GL}_n(\mathbb{C})$ such that $g \cdot (E_1, \dots, E_n) = (V_1, \dots, V_n)$. In fact, the matrix $g = (v_1 | v_2 | \cdots | v_n)$, where $\{v_1, \dots, v_n\}$ is a basis of V, satisfies $g e_i = v_i$ for all $i \in \{1, \dots, n\}$.

Let $B_n(\mathbb{C})$ be the stabilizer

$$G_{(E_1, \dots, E_n)} = \{g \in \mathbf{GL}_n(\mathbb{C}) : T_g(E_i) = E_i \text{ for all } i\} = \{(b_{ij}) : b_{ij} = 0 \text{ if } i > j\}$$

of the standard flag. Then $B_n(\mathbb{C})$ is known as the **Borel subgroup**.

Let $U_n(\mathbb{C})$ be the subgroup of $\mathbf{GL}_n(\mathbb{C})$ of matrices (u_{ij}) such that

$$u_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i > j. \end{cases}$$

Let $T_n(\mathbb{C})$ be the subgroup of $\mathbf{GL}_n(\mathbb{C})$ diagonal matrices.

Proposition 2.12. $B_n(\mathbb{C}) = U_n(\mathbb{C}) \rtimes T_n(\mathbb{C})$.

Proof. It is trivial that $U_n(\mathbb{C}) \cap T_n(\mathbb{C}) = \{I\}$, where I is the $n \times n$ identity matrix. Clearly, $U_n(\mathbb{C})$ is a subgroup of $B_n(\mathbb{C})$. To prove that $U_n(\mathbb{C})$ is normal in $B_n(\mathbb{C})$ note that $U_n(\mathbb{C})$ is the kernel of the group homomorphism

$$f\colon B_n(\mathbb{C}) \to T_n(\mathbb{C}), \quad (b_{ij}) \mapsto \begin{pmatrix} b_{11} & & & \\ & b_{22} & & \\ & & \ddots & \\ & & & b_{nn} \end{pmatrix}.$$

It remains to show that $B_n(\mathbb{C}) = U_n(\mathbb{C})T_n(\mathbb{C})$. Let us prove that $B_n(\mathbb{C}) \subseteq U_n(\mathbb{C})T_n(\mathbb{C})$, as the other inclusion is trivial. Let $b \in B_n(\mathbb{C})$. Then $bf(b)^{-1} \in \ker f = U_n(\mathbb{C})$ and therefore $b = (bf(b)^{-1})f(b) \in U_n(\mathbb{C})T_n(\mathbb{C})$. □

Definition 2.13. A matrix $a \in \mathbf{GL}_n(\mathbb{C})$ is said to be **unipotent** if its characteristic polynomial is of the form $(X-1)^n$.

The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is unipotent, as its characteristic polynomial is $(X-1)^2$.

Definition 2.14. A subgroup G of $\mathbf{GL}_n(\mathbb{C})$ is said to be **unipotent** if each $g \in G$ is unipotent.

Now an application of Wedderburn's theorem:

Proposition 2.15. *Let G be a unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$. Then there exists a non-zero $v \in \mathbb{C}^n$ such that $gv = v$ for all $g \in G$.*

Proof. Without loss of generality, we may assume that G is non-trivial. Let V be the subspace of $\mathbb{C}^{n\times n}$ generated by $\{g - I : g \in G\}$. If $g \in G$, then $(g-I)^n = 0$, as g is unipotent. Thus, every element of V is nilpotent. If $g, h \in G$, then

$$(g-I)(h-I) = (gh-I) - (g-I) - (h-I) \in V.$$

This means that V is closed under multiplication and hence V is an algebra generated (as a vector space) by nilpotent elements. By Wedderburn's theorem, V is nilpotent. Let m be minimal such that $(g_1 - I)\cdots(g_m - I) = 0$ for all $g_1, \ldots, g_m \in G$. The minimality of m implies that there exist $h_1, \ldots, h_{m-1} \in G$ such that

$$(h_1 - I)\cdots(h_{m-1} - I) \neq 0.$$

In particular, there exists a non-zero $w \in C^n$ such that $v = (h_1 - I)\cdots(h_{m-1} - I)w \neq 0$. For every $g \in G$,

$$(g-I)v = (g-I)(h_1 - I)\cdots(h_{m-1} - I)w = 0$$

and hence $gv = v$. □

Theorem 2.16 (Kolchin). *Every unipotent subgroup of* $\mathbf{GL}_n(\mathbb{C})$ *is conjugate to some subgroup of* $U_n(\mathbb{C})$.

Proof. Let G be an unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$. Assume first that there exists a complete flag $(V_1, \dots, V_n)$ of $\mathbb{C}^n$ such that $G \subseteq G_{(V_1,\dots,V_n)}$. Let $g \in \mathbf{GL}_n(\mathbb{C})$ be such that $g \cdot (E_1, \dots, E_n) = (V_1, \dots, V_n)$. Then

$$G \subseteq G_{g\cdot(E_1,\dots,E_n)} = gG_{(E_1,\dots,E_n)}g^{-1} = gB_n(\mathbb{C})g^{-1}.$$

Since G is unipotent, it follows that

$$G \subseteq gB_n(\mathbb{C})g^{-1} \subseteq gU_n(\mathbb{C})g^{-1}.$$

We claim that $G \subseteq G_{(V_1,\dots,V_n)}$ for some complete flag $(V_1, \dots, V_n)$. We proceed by induction on n. If $n = 1$, the result is trivial. Assume the result holds for $n-1$. By the previous proposition, there exists a non-zero $v \in \mathbb{C}^n$ such that $gv = v$ for all $g \in G$. Let $Q = \mathbb{C}^n/\langle v\rangle$ and $\pi\colon \mathbb{C}^n \to Q$ be the canonical map. Then $\dim Q = n-1$. The group G acts on Q by

$$g \cdot (w + \langle v\rangle) = gw + \langle v\rangle.$$

The action is well-defined: if $w + \langle v\rangle = w_1 + \langle v\rangle$, then $w - w_1 = \lambda v$ for some $\lambda \in \mathbb{C}$. This implies that

$$gw - gw_1 = g(w - w_1) = \lambda(gv) = \lambda v \in \langle v\rangle$$

and hence $gw + \langle v\rangle = gw_1 + \langle v\rangle$.

By the inductive hypothesis, G stabilizes a complete flag $(Q_1, \dots, Q_{n-1})$, where

$$Q_1 = \langle \pi(v_1)\rangle, \quad Q_2 = \langle \pi(v_1), \pi(v_2)\rangle, \quad \dots \quad Q_{n-1} = \langle \pi(v_1), \dots, \pi(v_{n-1})\rangle.$$

Let

$$W_0 = \langle v\rangle, \quad W_1 = \langle v, v_1\rangle, \quad W_2 = \langle v, v_1, v_2\rangle, \quad \dots \quad W_{n-1} = \langle v, v_1, \dots, v_{n-1}\rangle.$$

Since $(Q_1, \dots, Q_{n-1})$ is a complete flag, the set $\{\pi(v_j) : 1 \le j \le n-1\}$ is linearly independent. We claim that $\{v, v_1, \dots, v_{n-1}\}$ is linearly independent. In fact, since $v \neq 0$, one obtains that

$$\sum_{i=1}^{n-1} \lambda_i v_i + \lambda v = 0 \implies \sum_{i=1}^{n-1} \lambda_i \pi(v_i) = 0 \implies \lambda_1 = \cdots = \lambda_{n-1} = 0 \implies \lambda = 0.$$

Thus $\dim W_i = i + 1$ for all i.

Let $g \in G$. Clearly, $gW_0 \subseteq W_0$, as $gv = v$. Let $j \in \{1, \dots, n-1\}$. There exist $\lambda_1, \dots, \lambda_j \in \mathbb{C}$ such that $\pi(gv_j) = \sum_{i \le j} \lambda_i \pi(v_i)$. This means that

$$gv_j - \sum_{i \le j} \lambda_i v_i = \lambda v \in \langle v\rangle$$

for some $\lambda \in \mathbb{C}$. In particular,

$$gv_j = \sum_{i \le j} \lambda_i v_i + \lambda v \in \langle v, v_1, \ldots, v_j \rangle = W_j.$$

Therefore, $G \subseteq G_{(W_0,\ldots,W_{n-1})}$. □

Some comments

The ideas behind the theorem are somewhat connected to Sylow's theory. The key is to consider an explicit version of Sylow's theorem for the group $\mathbf{GL}_n(p)$ of invertible matrices with coefficients in the field $\mathbb{F}_p$ with p elements.

A group G acts linearly on a vector space V if $g \cdot (v+w) = g \cdot v + g \cdot w$ for all $g \in G$ and $v, w \in V$. Proposition 2.15 has the following version:

Proposition 2.17. *Let P be a finite p-group acting on a finite-dimensional $\mathbb{F}_p$-vector space V linearly. Then there exists a non-zero $v \in V$ such that $x \cdot v = v$ for all $x \in P$.*

Proof. Let $n = \dim V$. There are $p^n - 1$ non-zero vectors in V. Since the action is linear, P acts on $X = V \setminus \{0\}$. We decompose V into orbits and collect those orbits with only one element, say

$$X = X_0 \cup O(v_1) \cup \cdots \cup O(v_m),$$

where $|O(v_j)| \ge 2$ for all $j \in \{1, \ldots, m\}$. Since p divides the order of each $O(v_j)$ and $|X| = p^n - 1$ is not divisible by p, it follows that $X_0 \neq \emptyset$. In particular, there exists $v \in V$ such that $x \cdot v = v$ for all $x \in G$. □

The analog of Kolchin's theorem is the following result:

Proposition 2.18. *Every p-subgroup of $\mathbf{GL}_n(p)$ is conjugate to a subgroup of the unipotent subgroup $U_n(p)$.*

Sketch of the proof. Let P be a p-subgroup of $\mathbf{GL}_n(p)$. Then P acts linearly on an n-dimensional $\mathbb{F}_p$-vector space V by left multiplication. The previous proposition implies that there exists a non-zero $v_1 \in V$ such that $xv_1 = v_1$ for all $x \in P$. Let $V_1 = \langle v_1 \rangle$. The group P acts on the $(n-1)$-dimensional vector space V/V_1 by

$$x \cdot (v + V_1) = xv + V_1.$$

This action is well-defined. As before, there exists a non-zero vector of V/V_1 fixed by P. Thus there exists $v_2 \in V \setminus V_1$ such that $xv_2 + V_1 = v_2 + V_1$. Note that $\{v_1, v_2\}$ is linearly independent, as applying the canonical map $V \to V/V_1$ to $\alpha v_1 + \beta v_2 = 0$ one obtains that $\beta = 0$ and therefore $\alpha = 0$. This process produces a basis $\{v_1, \ldots, v_n\}$ of V and a sequence $\{0\} \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_n = V$, where $V_j = \langle v_1, \ldots, v_j \rangle$ for all $j \in \{1, \ldots, n\}$. Moreover, $PV_j \subseteq V_j$ and $Pv_j = v_j + V_{j-1}$ for all j. This means precisely

that in the basis $\{v_1, \ldots, v_n\}$ every element of P is an upper triangular matrix with ones in the main diagonal. □

Proposition 2.18 is deeply connected to Sylow's theorems.

Exercise 2.19. Prove that the normalizer of $U_n(p)$ in $\mathbf{GL}_n(p)$ is the Borel subgroup $B_n(p)$ of upper triangular matrices.

Now we have the following explicit Sylow theory for $\mathbf{GL}_n(p)$. The first two Sylow theorems appear in the following result.

Exercise 2.20. Prove that $U_n(p)$ is a Sylow p-subgroup of $\mathbf{GL}_n(p)$.

What about the third Sylow's theorem? First, note that the number n_p of conjugates of $U_n(p)$ in $\mathbf{GL}_n(p)$ is the number of complete flags in $\mathbb{F}_p^n$.

Exercise 2.21. Prove that $n_p \equiv 1 \bmod p$.

Lecture 2

§3. Group algebras

Let G be a finite group. The (complex) **group algebra** $\mathbb{C}[G]$ is the $\mathbb{C}$-vector space with basis $\{g : g \in G\}$ and multiplication

$$\left(\sum_{g\in G} \lambda_g g\right)\left(\sum_{h\in G} \mu_h h\right) = \sum_{g,h\in G} \lambda_g \mu_h (gh).$$

Clearly, $\dim \mathbb{C}[G] = |G|$. Moreover, $\mathbb{C}[G]$ is commutative if and only if G is abelian.

If G is non-trivial, then $\mathbb{C}[G]$ contains proper non-trivial ideals. For example, the **augmentation ideal**

$$I(G) = \left\{ \sum_{g\in G} \lambda_g g \in \mathbb{C}[G] : \sum_{g\in G} \lambda_g = 0 \right\}$$

is a non-zero proper ideal of $\mathbb{C}[G]$.

Exercise 3.1. Let C_n be the cyclic group of order n (written multiplicatively). Prove that $\mathbb{C}[G] \simeq \mathbb{C}[X]/(X^n - 1)$.

Exercise 3.2. Let G be a finite non-trivial group. Prove that $\mathbb{C}[G]$ has zero divisors.

Exercise 3.3. Let G be a finite group. The set

$$\mathrm{Fun}(G, \mathbb{C}) = \{\alpha : G \to \mathbb{C}\}$$

is a complex vector space with the operations

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x), \quad (\lambda\alpha)(x) = \lambda\alpha(x),$$

for all $\alpha, \beta \in \mathrm{Fun}(G, \mathbb{C})$, $x \in G$ and $\lambda \in \mathbb{C}$. It is an algebra with the **convolution product**

$$(\alpha * \beta)(x) = \sum_{y \in G} \alpha(xy^{-1})\beta(y).$$

Let

$$\delta_x(y) = \begin{cases} 1 & \text{if } x = y, \\ 0 & \text{otherwise.} \end{cases}$$

Prove the following statements:

1) The set $\{\delta_x : x \in G\}$ is a basis of $\mathrm{Fun}(G, \mathbb{C})$.
2) The map $\mathbb{C}[G] \to \mathrm{Fun}(G, \mathbb{C})$, $g \mapsto \delta_g$, extends linearly to an algebra isomorphism.

Recall that a finite-dimensional module M is semisimple if and only if for every submodule S of M there is a submodule T of M such that $M = S \oplus T$.

Theorem 3.4 (Maschke). *Let G be a finite group and M be a finite-dimensional $\mathbb{C}[G]$-module. Then M is semisimple.*

Proof. We must show that every submodule S of M admits a complement. Since S is a subspace of M, there exists a subspace T_0 of M such that $M = S \oplus T_0$ (as vector spaces). We use T_0 to construct a submodule T of M that complements S. Since $M = S \oplus T_0$, every $m \in M$ can be written uniquely as $m = s + t_0$ for some $s \in S$ and $t_0 \in T$. Let

$$p_0 \colon M \to S, \quad p_0(m) = s,$$

where $m = s + t_0$ with $s \in S$ and $t_0 \in T$. If $s \in S$, then $p_0(s) = s$. In particular, $p_0^2 = p_0$, as $p_0(m) \in S$.

Generally, p_0 is not a $\mathbb{C}[G]$-modules homomorphism. Let

$$p \colon M \to S, \quad p(m) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot p_0(g \cdot m).$$

We claim that p is a homomorphism of $\mathbb{C}[G]$-modules. For that purpose, we need to show that $p(g \cdot m) = g \cdot p(m)$ for all $g \in G$ and $m \in M$. In fact,

$$p(g \cdot m) = \frac{1}{|G|} \sum_{h \in G} h^{-1} \cdot p_0(h \cdot (g \cdot m)) = \frac{1}{|G|} \sum_{h \in G} (gh^{-1}) \cdot p_0(h \cdot m) = g \cdot p(m).$$

We now claim that $p(M) = S$. The inclusion $\subseteq$ is trivial to prove, as S is a submodule of M and $p_0(M) \subseteq S$. Conversely, if $s \in S$, then $g \cdot s \in S$, as S is a submodule. Thus $s = g^{-1} \cdot (g \cdot s) = g^{-1} \cdot p_0(g \cdot s)$ and hence

$$s = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (g \cdot s) = \frac{1}{|G|} \sum_{g \in G} g^{-1} \cdot (p_0(g \cdot s)) = p(s).$$

Since $p(m) \in S$ for all $m \in M$, it follows that $p^2(m) = p(m)$, so p is a projector onto S. Hence S admits a complement in M, that is $M = S \oplus \ker(p)$. □

Exercise 3.5. Let $G = \langle g \rangle$ be the cyclic group of order four and $\rho_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Let $M = \mathbb{C}^{2\times 1}$ as an $\mathbb{C}[G]$-module with

$$g \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -v \\ u \end{pmatrix}.$$

Prove that M is a semisimple non-simple $\mathbb{C}[G]$-module.

Exercise 3.6. Let $G = \langle g \rangle$ be the cyclic group of order four and $\rho_g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Let $M = \mathbb{R}^{2\times 1}$ as an $\mathbb{R}[G]$-module with

$$g \cdot \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -v \\ u \end{pmatrix}.$$

Prove that M is a simple $\mathbb{R}[G]$-module.

If G is a finite group, then $\mathbb{C}[G]$ is semisimple. By Artin–Wedderburn theorem,

$$\mathbb{C}[G] \simeq \prod_{i=1}^{r} M_{n_i}(\mathbb{C}),$$

where r is the number of isomorphism classes of simple modules of $\mathbb{C}[G]$. Moreover, $|G| = \dim \mathbb{C}[G] = \sum_{i=1}^{r} n_i^2$. By convention, we always assume that $n_1 = 1$. This corresponds, of course, to the **trivial module**.

Theorem 3.7. *Let G be a finite group. The number of simple modules of $\mathbb{C}[G]$ coincides with the number of conjugacy classes of G.*

Proof. By Artin–Wedderburn theorem, $\mathbb{C}[G] \simeq \prod_{i=1}^{r} M_{n_i}(\mathbb{C})$. Thus

$$Z(\mathbb{C}[G]) \simeq \prod_{i=1}^{r} Z(M_{n_i}(\mathbb{C})) \simeq \mathbb{C}^r.$$

In particular, $\dim Z(\mathbb{C}[G]) = r$. If $\alpha = \sum_{g\in G} \lambda_g g \in Z(\mathbb{C}[G])$, then $h^{-1}\alpha h = \alpha$ for all $h \in G$. Thus

$$\sum_{g\in G} \lambda_{hgh^{-1}} g = \sum_{g\in g} \lambda_g h^{-1} g h = \sum_{g\in G} \lambda_g g$$

and hence $\lambda_g = \lambda_{hgh^{-1}}$ for all $g, h \in G$. A basis for $Z(\mathbb{C}[G])$ is given by elements of the form

$$\sum_{g\in K} g,$$

where K is a conjugacy class of G. Therefore $\dim Z(\mathbb{C}[G])$ equals the number of conjugacy classes of G. □

Exercise 3.8. Let G be a finite group of order n with k conjugacy classes. Let $m = (G : [G, G])$. Prove that $n + 3m \geq 4k$.

If G is a finite group, then

$$\mathbb{C}[G] \simeq \prod_{i=1}^{k} M_{n_i}(\mathbb{C}),$$

where k is the number of conjugacy classes of G. In particular,

$$|G| = \dim \mathbb{C}[G] = \sum_{i=1}^{k} n_i^2.$$

For $n \in \mathbb{Z}_{\geq 2}$, we write C_n to denote the (multiplicative) cyclic group of order n.

Exercise 3.9. Prove that $\mathbb{C}[C_4] \simeq \mathbb{C}^4$.

For $n \geq 1$, let $\mathbb{S}_n$ denote the symmetric group in n letters.

Example 3.10. The group $\mathbb{S}_3$ has three conjugacy classes: $\{\mathrm{id}\}$, $\{(12), (13), (23)\}$ and $\{(123), (132)\}$. Since $6 = 1^2 + a^2 + b^2$, it follows that $\mathbb{C}[G] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.

Open problem 3.1 (Brauer). Which algebras are group algebras?

This question might be impossible to answer, but it is extremely interesting.

Example 3.11. The algebra $\mathbb{C}^2 \times M_2(\mathbb{C}) \times M_3(\mathbb{C})$ is not complex group algebra, as all groups of order 15 are abelian.

Some comments

There is a multiplicative version of Maschke's theorem. A group G acts by automorphisms on A if there is a group homomorphism $\lambda\colon G \to \mathrm{Aut}(A)$. In this case, a subgroup B of A is said to be G-invariant if $\lambda(B) \subseteq B$.

Theorem 3.12. *Let K be a finite group of order m. Assume that K acts by automorphisms on $V = U \times W$, where U and W are subgroups of V and U is abelian and K-invariant. If the map $U \to U$, $u \mapsto u^m$, is bijective, then there exists a normal K-invariant subgroup N of V such that $V = U \times N$.*

Proof. Let $\theta\colon U \times W \to U$, $(u, w) \mapsto u$. Then θ is a group homomorphism such that $\theta(u) = u$ for all $u \in U$. Since U is K-invariant,

$$k^{-1} \cdot \theta(k \cdot v) \in U$$

for all $k \in K$ and $v \in V$. Since K is finite and U is abelian, the map

$$\varphi\colon V \to U, \quad v \mapsto \prod_{k \in K} k^{-1} \cdot \theta(k \cdot v),$$

is well-defined. We claim that φ is a group homomorphism. If $x, y \in V$, then

$$\begin{aligned}\varphi(xy) &= \prod_{k\in K} k^{-1}\cdot\theta(k\cdot(xy)) \\ &= \prod_{k\in K} k^{-1}\cdot(\theta(k\cdot x)\theta(k\cdot y)) \\ &= \prod_{k\in K} k^{-1}\cdot\theta(k\cdot x)\prod_{k\in K} k^{-1}\cdot\theta(k\cdot y) = \varphi(x)\varphi(y),\end{aligned}$$

since U is abelian and K acts by automorphisms on V.

We claim that $N = \ker\varphi$ is K-invariant. We need to show that $\varphi(l\cdot x) = l\cdot\varphi(x)$ for all $l \in K$ and $x \in V$. If $l \in K$ and $x \in V$, then

$$l^{-1}\cdot\varphi(l\cdot x) = l^{-1}\cdot\left(\prod_{k\in K} k^{-1}\cdot\theta(k\cdot(l\cdot x))\right) = \prod_{k\in K}(kl)^{-1}\cdot\theta((kl)\cdot x) = \varphi(x),$$

since kl runs over all the elements of K whenever k runs over all the elements of K. In conclusion, $\ker\varphi$ is K-invariant.

It remains to show that V is the direct product of U and N. By assumption, U is normal in V. We first prove that $U \cap N = \{1\}$. If $u \in U$, then $k\cdot u \in U$ for all $k \in K$. This implies that $k^{-1}\cdot\theta(k\cdot u) = k^{-1}\cdot(k\cdot u) = u$. Hence $\varphi(u) = u^m$. Since this map is bijective by assumption,

$$U \cap N = U \cap \ker\varphi = \{1\}.$$

We now show that $V \subseteq UN$, as the other inclusion is trivial. Since $N = \ker\varphi$,

$$\varphi(V) \subseteq U = \varphi(U) = \varphi(U)\varphi(N) = \varphi(UN)$$

and hence $V \subseteq (UN)N = UN$. Therefore V is the direct product of U and N, as N is normal in V. □

Corollary 3.13. *Let p be a prime number and K be a finite group with order not divisible by p. Let V be a p-elementary abelian group. Assume that K acts by automorphism on V. If U be a K-invariant subgroup of V, then there exists a K-invariant subgroup N of V such that $V = U \times N$.*

Proof. Let $m = |K|$. Since m and $|U|$ are coprime, the map $u \mapsto u^m$ is bijective in U. Since V is a vector space over the field $\mathbb{Z}/p$, it follows that $V = U \times W$ for some subgroup W of V. Now the claim follows from the previous theorem. □

§4. Representations

Unless we state differently, we will always work with finite groups. All our vector spaces will be complex vector spaces.

Definition 4.1. Let G be a finite group. A **representation** of G is a group homomorphism $\rho\colon G \to \mathbf{GL}(V)$, where V is a finite-dimensional vector space. The **degree** (or dimension) of the representation is the integer $\deg\rho = \dim V$.

Let $G \to \mathbf{GL}(V)$ be a representation. If we fix a basis of V, then we obtain a **matrix representation** of G, that is a group homomorphism

$$\rho\colon G \to \mathbf{GL}(V) \simeq \mathbf{GL}_n(\mathbb{C}), \quad g \mapsto \rho_g,$$

where $n = \dim V$.

Example 4.2. Since $\mathbb{S}_3 = \langle (12), (123) \rangle$, the map $\rho\colon \mathbb{S}_3 \to \mathbf{GL}_3(\mathbb{C})$,

$$(12) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

is a representation of $\mathbb{S}_3$.

Example 4.3. Let $G = \langle g \rangle$ be cyclic of order six. The map $\rho\colon G \to \mathbf{GL}_2(\mathbb{C})$,

$$g \mapsto \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

is a representation of G.

Example 4.4. Let $G = \langle g \rangle$ be cyclic of order four. The map $\rho\colon G \to \mathbf{GL}_2(\mathbb{C})$,

$$g \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

is a representation of G.

Example 4.5. Let $G = \langle a, b : a^2 = b^3 = (ab)^3 = 1 \rangle$. The map

$$a \mapsto \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & -1 \\ 0 & 0 & -1 \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

defines a representation $G \to \mathbf{GL}_3(\mathbb{C})$.

Example 4.6. Let $Q_8 = \{-1, 1, i, -i, j, -j\}$ be the quaternion group. Recall that

$$i^2 = j^2 = k^2 = -1, \quad ijk = -1.$$

The group Q_8 is generated by $\{i, j\}$ and the map $\rho\colon Q_8 \to \mathbf{GL}_2(\mathbb{C})$,

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

is a representation.

Example 4.7. Let G be a finite group that acts on a finite set X. Let $V = \mathbb{C}X$ the complex vector space with basis $\{x : x \in X\}$. The map

$$\rho\colon G \to \mathbf{GL}(V), \quad \rho_g\left(\sum_{x\in X} \lambda_x x\right) = \sum_{x\in X} \lambda_x \rho_g(x) = \sum_{x\in X} \lambda_{g^{-1}\cdot x} x,$$

is a representation of degree $|X|$.

Example 4.8. The sign $\operatorname{sign}\colon \mathbb{S}_n \to \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ is a representation of $\mathbb{S}_n$.

An important fact is that there exists a bijective correspondence between representations of a finite group G and finite-dimensional modules over $\mathbb{C}[G]$. The correspondence is given as follows. If $\rho\colon G \to \mathbf{GL}(V)$ is a representation, then V is a $\mathbb{C}[G]$-module with

$$\left(\sum_{g\in G} \lambda_g g\right)\cdot v = \sum_{g\in G} \lambda_g \rho_g(v).$$

Conversely, if V is a $\mathbb{C}[G]$-module, then $\rho\colon G \to \mathbf{GL}(V)$, $\rho_g\colon V \to V$, $v \mapsto g\cdot v$, is a representation.

Exercise 4.9. Let G be a finite group and $\rho\colon G \to \mathbf{GL}(V)$ be a representation. Prove that each ρ_g is diagonalizable.

The previous exercise uses properties of the minimal polynomial. We will see a different proof later.

Definition 4.10. Let G be a group and $\phi\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations of G. We say that ϕ and ψ are **equivalent** if there exists a linear isomorphism $T\colon V \to W$ such that

$$\psi_g T = T\phi_g$$

for all $g \in G$. In this case, we write $\phi \simeq \psi$.

Note that $\phi \simeq \psi$ if and only if V and W are isomorphic as $\mathbb{C}[G]$-modules.

Example 4.11. The representation

$$\phi\colon \mathbb{Z}/n \to \mathbf{GL}_2(\mathbb{C}), \quad \phi(m) = \begin{pmatrix} \cos(2\pi m/n) & -\sin(2\pi m/n) \\ \sin(2\pi m/n) & \cos(2\pi m/n) \end{pmatrix},$$

is equivalent to the representation

$$\psi\colon \mathbb{Z}/n \to \mathbf{GL}_2(\mathbb{C}), \quad \psi(m) = \begin{pmatrix} e^{2\pi i m/n} & 0 \\ 0 & e^{-2\pi i m/n} \end{pmatrix}.$$

The equivalence is obtained with the matrix $T = \begin{pmatrix} i & -i \\ 1 & 1 \end{pmatrix}$, as a direct calculation shows that $\phi_m T = T\psi_m$ for all m.

Exercise 4.12. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. Fix a basis of V and consider the corresponding matrix representation ϕ of ρ. Prove that ρ and ϕ are equivalent.

Definition 4.13. Let $\phi\colon G \to \mathbf{GL}(V)$ be a representation. A subspace $W \subseteq V$ is said to be G**-invariant** if $\phi_g(W) \subseteq W$ for all $g \in G$.

Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. If W is a G-invariant subspace of V, then the restriction $\rho|_W\colon G \to \mathbf{GL}(W)$ is a representation. In particular, W is a submodule (over $\mathbb{C}[G]$) of V.

Definition 4.14. A representation $\rho\colon G \to \mathbf{GL}(V)$ is said to be **irreducible** if $\{0\}$ and V are the only G-invariant subspaces of V.

Note that a representation $\rho\colon G \to \mathbf{GL}(V)$ is irreducible if and only if V is simple.

Example 4.15. Degree-one representations are irreducible.

Exercise 4.16. Let G be a finite group. Prove that there exists a bijective correspondence between degree-one representations of G and degree-one representations of $G/[G,G]$.

In the following example, we work over the real numbers.

Example 4.17. Let $G = \langle g \rangle$ be the cyclic group of three elements and

$$\rho\colon G \to \mathbf{GL}(\mathbb{R}^3), \quad \rho_g(x,y,z) = (y,z,x).$$

The set

$$N = \{(x,y,z) \in \mathbb{R}^3 : x+y+z = 0\}$$

is a G-invariant subspace of $\mathbb{R}^3$.

We claim that N is irreducible. If N contains a non-zero G-invariant subspace S, let $(x_0,y_0,z_0) \in S \setminus \{(0,0,0)\}$. Since S is G-invariant,

$$(y_0,z_0,x_0) = g \cdot (x_0,y_0,z_0) \in S.$$

We claim that $\{(x_0,y_0,z_0),(y_0,z_0,x_0)\}$ is linearly independent. If there exists $\lambda \in \mathbb{R}$ such that $\lambda(x_0,y_0,z_0) = (y_0,z_0,x_0)$, then $x_0 = \lambda^3 x_0$. Since $x_0 = 0$ implies $y_0 = z_0 = 0$, it follows that $\lambda = 1$. In particular, $x_0 = y_0 = z_0$, a contradiction, as $x_0 + y_0 + z_0 = 0$. Hence $\dim S = 2$ and therefore $S = N$.

What happens in the previous example if we consider complex numbers?

Exercise 4.18. Let $\phi\colon G \to \mathbf{GL}(V)$, $g \mapsto \phi_g$, be a degree-two representation. Prove that ϕ is irreducible if and only if there is no common eigenvector for all the ϕ_g.

Example 4.19. Recall that $\mathbb{S}_3$ is generated by (12) and (23). The map

$$(12) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

defines a representation ϕ of $\mathbb{S}_3$. Exercise 4.18 shows that ϕ is irreducible.

Lecture 3

We now describe three crucial examples of representations.

Example 4.20 (The trivial representation). The map $\rho\colon G \to \mathbb{C}^\times$, $g \mapsto 1$, is a representation, that is $\mathbb{C}$ is a $\mathbb{C}[G]$-module with $g \cdot \lambda = \lambda$ for all $g \in G$ and $\lambda \in \mathbb{C}^\times$.

Example 4.21. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations. The **direct sum** $\rho \oplus \psi\colon G \to \mathbf{GL}(V \oplus W)$, $g \mapsto (\rho_g, \psi_g)$, is a representation. This is equivalent to say that the vector space $V \oplus W$ is a $\mathbb{C}[G]$-module with

$$g \cdot (v, w) = (g \cdot v, g \cdot w), \quad g \in G,\ v \in v,\ w \in W.$$

Let V be a vector space with basis $\{v_1, \ldots, v_k\}$ and W be a vector space with basis $\{w_1, \ldots, w_l\}$. A **tensor product** of V and W is a vector space X with together with a bilinear map

$$V \times W \to X, \quad (v, w) \mapsto v \otimes w,$$

such that $\{v_i \otimes w_j : 1 \le i \le k, 1 \le j \le l\}$ is a basis of X. The tensor product of V and W is unique up to isomorphism and it is denoted by $V \otimes W$. Note that

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

Example 4.22. Let V and W be $\mathbb{C}[G]$-modules. The **tensor product** $V \otimes W$ is a $\mathbb{C}[G]$-module with

$$g \cdot v \otimes w = g \cdot v \otimes g \cdot w, \quad g \in G,\ v \in V,\ w \in W.$$

Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be representations. The **tensor product** of ρ and ψ is the representation of G given by

$$\rho \otimes \psi\colon G \to \mathbf{GL}(V \otimes W), \quad g \mapsto (\rho \otimes \psi)_g,$$

where

$$(\rho \otimes \psi)_g(v \otimes w) = \rho_g(v) \otimes \psi_g(w)$$

for $v \in V$ and $w \in W$.

Exercise 4.23. Let G be a finite group and V and W be $\mathbb{C}[G]$-modules. Prove that the set $\mathrm{Hom}(V,W)$ of complex linear maps $V \to W$ is a $\mathbb{C}[G]$-module with

$$(g \cdot f)(v) = g f(g^{-1}v), \quad f \in \mathrm{Hom}(V,W),\ v \in V,\ g \in G.$$

If, moreover, V and W are finite-dimensional, then

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

as $\mathbb{C}[G]$-modules.

The previous exercise shows, in particular, that the dual V^* of a $\mathbb{C}[G]$-module V is a $\mathbb{C}[G]$-module with

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

Definition 4.24. A representation $\rho\colon G \to \mathbf{GL}(V)$ is said to be **completely reducible** if ρ can be decomposed as $\rho = \rho_1 \oplus \cdots \oplus \rho_n$ for some irreducible representations $\rho_1, \ldots, \rho_n$ of G.

Note that if $\rho\colon G \to \mathbf{GL}(V)$ is completely reducible and $\rho = \rho_1 \oplus \cdots \oplus \rho_n$ for some irreducible representations $\rho_i\colon G \to \mathbf{GL}(V_i)$, $i \in \{1, \ldots, n\}$, then each V_i is an invariant subspace of V and $V = V_1 \oplus \cdots V_n$. Moreover, in some basis of V, the matrix ρ_g can be written as

$$\rho_g = \begin{pmatrix} (\rho_1)_g & & & \\ & (\rho_2)_g & & \\ & & \ddots & \\ & & & (\rho_n)_g \end{pmatrix}.$$

Definition 4.25. A representation $\rho\colon G \to \mathbf{GL}(V)$ is **decomposable** if V can be decomposed as $V = S \otimes T$ where S and T are non-zero invariant subspaces of V.

A representation is **indecomposable** if it is not decomposable.

Exercise 4.26. Let $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ be equivalent representations. Prove the following facts:

1) If ρ is irreducible, then ψ is irreducible.
2) If ρ is decomposable, then ψ is decomposable.
3) If ρ is completely reducible, then ψ is completely reducible.

§5. Characters

Fix a finite group G and consider (matrix) representations of G. We use linear algebra to study these representations.

Definition 5.1. Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation. The **character** of ρ is the map $\chi_\rho\colon G \to \mathbb{C}$, $g \mapsto \operatorname{trace}\rho_g$.

If a representation ρ is irreducible, its character is said to be an **irreducible character**. The **degree** of a character is the degree of the affording representation.

Example 5.2. We can compute the character of the representation

$$(12) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (23) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix},$$

of Example 4.19. Since

$$\rho_{(132)} = \rho_{(23)(12)} = \rho_{(23)}\rho_{(12)} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},$$

we conclude that $\rho_{(132)} = -1$. Similar calculations show that

$$\chi_{\mathrm{id}} = 2, \quad \chi_{(12)} = \chi_{(13)} = \chi_{(23)} = 0, \quad \chi_{(123)} = \chi_{(132)} = -1.$$

Proposition 5.3. *Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation, χ be its character and $g \in G$. The following statements hold:*

1) $\chi(1) = \dim V$.
2) $\chi(g) = \chi(hgh^{-1})$ *for all* $h \in G$.
3) $\chi(g)$ *is the sum of* $\chi(1)$ *roots of one of order* $|g|$.
4) $\chi(g^{-1}) = \overline{\chi(g)}$.
5) $|\chi(g)| \le \chi(1)$.

Proof. The first statement is trivial. To prove 2) note that

$$\chi(hgh^{-1}) = \operatorname{trace}(\rho_{hgh^{-1}}) = \operatorname{trace}(\rho_h\rho_g\rho_h^{-1}) = \operatorname{trace}\rho_g = \chi(g).$$

Statement 3) follows from the fact that the trace of ρ_g is the sum of the eigenvalues of ρ_g and these numbers are roots of the polynomial $X^{|g|} - 1 \in \mathbb{C}[X]$. To prove 4) write $\chi(g) = \lambda_1 + \cdots + \lambda_k$, where the λ_j are roots of one. Then

$$\overline{\chi(g)} = \sum_{j=1}^{k} \overline{\lambda_j} = \sum_{j=1}^{k} \lambda_j^{-1} = \operatorname{trace}(\rho_g^{-1}) = \operatorname{trace}(\rho_{g^{-1}}) = \chi(g^{-1}).$$

Finally, we prove 5). Use 3) to write $\chi(g)$ as the sum of $\chi(1)$ roots of one, say $\chi(g) = \lambda_1 + \cdots + \lambda_k$ for $k = \chi(1)$. Then

$$|\chi(g)| = |\lambda_1 + \cdots + \lambda_k| \le |\lambda_1| + \cdots + |\lambda_k| = \underbrace{1 + \cdots + 1}_{k\text{-times}} = k. \qquad \square$$

If two representations are equivalent, their characters are equal.

Definition 5.4. Let G be a group and $f\colon G \to \mathbb{C}$ be a map. Then f is a **class function** if $f(g) = f(hgh^{-1})$ for all $g, h \in G$.

Characters are class functions. If G is a finite group, we write

$$\mathrm{cf}(G) = \{f\colon G \to \mathbb{C} : f \text{ is a class function}\}.$$

One proves that $\mathrm{cf}(G)$ is a complex vector space.

Exercise 5.5. Let G be a finite group. For a conjugacy class K of G let

$$\delta_K : G \to \mathbb{C}, \quad \delta_K(g) = \begin{cases} 1 & \text{if } g \in K, \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $\{\delta_K : K \text{ is a conjugacy class of } G\}$ is a basis of $\mathrm{cf}(G)$. In particular, $\dim \mathrm{cf}(G)$ is the number of conjugacy classes of G.

Proposition 5.6. *If $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are representations, then $\chi_{\rho\oplus\psi} = \chi_\rho + \chi_\psi$.*

Proof. For $g \in G$, it follows that $(\rho \oplus \psi)_g = \begin{pmatrix} \rho_g & 0 \\ 0 & \psi_g \end{pmatrix}$. Thus

$$\chi_{\rho\oplus\psi}(g) = \mathrm{trace}((\rho \oplus \phi)_g) = \mathrm{trace}(\rho_g) + \mathrm{trace}(\psi_g) = \chi_\rho(g) + \chi_\psi(g). \qquad \square$$

Proposition 5.7. *If $\rho\colon G \to \mathbf{GL}(V)$ and $\psi\colon G \to \mathbf{GL}(W)$ are representations, then*

$$\chi_{\rho\otimes\psi} = \chi_\rho \chi_\psi.$$

Proof. For each $g \in G$, the map ρ_g is diagonalizable. Let $\{v_1, \ldots, v_n\}$ be a basis of eigenvectors of ρ_g and let $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ be such that $\rho_g(v_i) = \lambda_i v_i$ for all $i \in \{1, \ldots, n\}$. Similarly, let $\{w_1, \ldots, w_m\}$ be a basis of eigenvectors of ψ_g and $\mu_1, \ldots, \mu_m \in \mathbb{C}$ be such that $\psi_g(w_j) = \mu_j w_j$ for all $j \in \{1, \ldots, m\}$. Each $v_i \otimes w_j$ is eigenvector of $(\rho \otimes \psi)_g$ with eigenvalue $\lambda_i \mu_j$, as

$$(\rho \otimes \psi)_g(v_i \otimes w_j) = \rho_g v_i \otimes \psi_g w_j = \lambda_i v_i \otimes \mu_j v_j = (\lambda_i \mu_j) v_i \otimes w_j.$$

Thus $\{v_i \otimes w_j : 1 \le i \le n, 1 \le j \le m\}$ is a basis of eigenvectors and the $\lambda_i \mu_j$ are the eigenvalues of $(\rho \otimes \psi)_g$. It follows that

$$\chi_{\rho\otimes\psi}(g) = \sum_{i,j} \lambda_i \mu_j = \left(\sum_i \lambda_i\right)\left(\sum_j \mu_j\right) = \chi_\rho(g)\chi_\psi(g). \qquad \square$$

We know that it is also possible to define the dual $\rho^*\colon G \to \mathbf{GL}(V^*)$ of a representation $\rho\colon G \to \mathbf{GL}(V)$ by the formula

$$(\rho_g^* f)(v) = f(\rho_g^{-1} v), \quad g \in G,\ f \in V^* \text{ and } v \in V.$$

We claim that the character of the dual representation is then $\overline{\chi_\rho}$. Let $\{v_1, \dots, v_n\}$ be a basis of V and $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ be such that $\rho_g v_i = \lambda_i v_i$ for all $i \in \{1, \dots, n\}$. If $\{f_1, \dots, f_n\}$ is the dual basis of $\{v_1, \dots, v_n\}$, then

$$(\rho_g^* f_i)(v_j) = f_i(\rho_g^{-1} v_j) = \overline{\lambda_j} f_i(v_j) = \overline{\lambda_j}\delta_{ij}$$

and the claim follows.

Let G be a finite group. If $\chi, \psi \colon G \to \mathbb{C}$ are characters of G and $\lambda \in \mathbb{C}$, we define

$$(\chi + \psi)(g) = \chi(g) + \psi(g), \quad (\chi\psi)(g) = \chi(g)\psi(g), \quad (\lambda\chi)(g) = \lambda\chi(g).$$

Note that these functions might not be characters!

Theorem 5.8. *Let G be a finite group. Then irreducible characters of G are linearly independent.*

Proof. Let $S_1, \dots, S_k$ be a complete set of representatives of classes of simple $\mathbb{C}[G]$-modules. Let $\operatorname{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. By Artin–Wedderburn theorem, there is an algebra isomorphism $f \colon \mathbb{C}[G] \to M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$, where $\dim S_j = n_j$ for all j. Moreover,

$$M_{n_j}(\mathbb{C}) \simeq \underbrace{S_j \oplus \cdots \oplus S_j}_{n_j\text{−times}}$$

for all j. For each j let $e_j = f^{-1}(I_j)$, where I_j is the identity matrix of $M_{n_j}(\mathbb{C})$. We claim that

$$\chi_i(e_j) = \begin{cases} \dim S_i & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

In fact, $\chi_i(g)$ is the trace of the action of g on S_j. Since $e_i e_j = 0$ if $i \neq j$, it follows that $\chi_i(e_j) = 0$ if $i \neq j$. Moreover, e_j acts as the identity on S_j, thus $\chi_j(e_j) = \dim S_j$.

Now if $\sum \lambda_i \chi_i = 0$ for some $\lambda_1, \dots, \lambda_k \in \mathbb{C}$, then

$$(\dim S_j)\lambda_j = \sum \lambda_i \chi_i(e_j) = 0$$

and hence $\lambda_j = 0$, as $\dim S_j \neq 0$. □

Theorem 5.9. *Let G be a finite group and $S_1, \dots, S_k$ be the simple $\mathbb{C}[G]$-modules (up to isomorphism). If $V = \oplus_{i=1}^k a_j S_j$, then $\chi_V = \sum a_i \chi_i$, where $\chi_i = \chi_{S_i}$ for all i. Moreover, if U and V are $\mathbb{C}[G]$-modules,*

$$U \simeq V \iff \chi_U = \chi_V.$$

Proof. The first part is left as an exercise.

It is also an exercise to prove that $U \simeq V$ implies $\chi_U = \chi_V$. Let us prove the converse. Assume that $\chi_U = \chi_V$. Since $\mathbb{C}[G]$ is semisimple, $U \simeq \oplus_{i=1}^k a_i S_i$ and $V \simeq \oplus_{i=1}^k b_i S_i$ for some integers $a_1, \dots, a_k \geq 0$ and $b_1, \dots, b_k \geq 0$. Since

$$0 = \chi_U - \chi_V = \sum_{i=1}^{k} (a_i - b_i)\chi_i$$

and the χ_i are linearly independent, it follows that $a_i = b_i$ for all i. Hence $U \simeq V$. □

Exercise 5.10. Let G be a finite group and U be a $\mathbb{C}[G]$-module. Prove $\chi_{U^*} = \overline{\chi_U}$.

We will use the following exercise later:

Exercise 5.11. Prove that if G is a finite group and U and V are $\mathbb{C}[G]$-modules, then

$$\chi_{\mathrm{Hom}_G(U,V)} = \overline{\chi_U}\chi_V\,.$$

For a finite group G we write $\mathrm{Irr}(G)$ to denote the complete set of isomorphism classes of characters of irreducible representations of G.

Exercise 5.12. Let G be a finite group. Prove that the set $\mathrm{Irr}(G)$ is a basis of $\mathrm{cf}(G)$.

Let G be a finite group and U be a $\mathbb{C}[G]$-module. Let

$$U^G = \{u \in U : g \cdot u = u \text{ for all } g \in G\}.$$

Then U^G is a subspace of U. The following lemma is important:

Lemma 5.13. $\dim U^G = \frac{1}{|G|} \sum_{x \in G} \chi_U(x)$

Proof. Let ρ be the representation associated with U and let

$$\alpha = \frac{1}{|G|} \sum_{x \in G} \rho_x \colon U \to U.$$

We claim that $\alpha^2 = \alpha$. Let $g \in G$. Then

$$\rho_g(\alpha) = \frac{1}{|G|} \sum_{x \in G} \rho_g \rho_x = \frac{1}{|G|} \sum_{x \in G} \rho_{gx} = \alpha.$$

Thus

$$\alpha(\alpha(u)) = \frac{1}{|G|} \sum_{x \in G} \rho_x(\alpha(u)) = \alpha(u)$$

for all $u \in U$. This means that α has eigenvalues 0 and 1.

Let V be the eigenspace of eigenvalue 1. We now claim that $V = U^G$. Let us first prove that $V \subseteq U^G$. For that purpose, let $v \in V$ and $g \in G$. Then

$$\begin{aligned} g \cdot v &= \rho_g(v) = \rho_g(\alpha(v)) \\ &= \frac{1}{|G|} \sum_{x \in G} \rho_g \rho_x(v) = \frac{1}{|G|} \sum_{y \in G} \rho_y(v) = \alpha(v) = v. \end{aligned}$$

Now we prove that $V \supseteq U^G$. Let $u \in U^G$, so $\rho_g(u) = u$ for all $g \in G$. Then

$$\alpha(u) = \frac{1}{|G|} \sum_{x \in G} \rho_x(u) = \frac{1}{|G|} \sum_{x \in G} u = u.$$

Thus

$$\dim U^G = \dim V = \operatorname{trace} \alpha = \frac{1}{|G|} \sum_{x \in G} \operatorname{trace} \rho_x = \frac{1}{|G|} \sum_{x \in G} \chi_U(x). \qquad \square$$

One proves that the operation

$$\langle \chi_U, \chi_V \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_U(g) \overline{\chi_V(g)}$$

defines an inner product.

Theorem 5.14. *Let G be a finite group and U and V be $\mathbb{C}[G]$-modules. Then*

$$\langle \chi_U, \chi_V \rangle = \dim \operatorname{Hom}_G(U, V).$$

Proof. We claim that

$$\operatorname{Hom}_G(U, V) = \operatorname{Hom}(U, V)^G.$$

Let us first prove that $\operatorname{Hom}_G(U,V) \subseteq \operatorname{Hom}(U,V)^G$. Let $f \in \operatorname{Hom}_G(U,V)$ and $g \in G$. Then

$$(g \cdot f)(u) = g \cdot f(g^{-1} \cdot u) = g \cdot (g^{-1} \cdot f(u)) = f(u)$$

for all $u \in U$. Now we prove that $\operatorname{Hom}_G(U,V) \supseteq \operatorname{Hom}(U,V)^G$. Let $f \in \operatorname{Hom}(U,V)^G$. Then $f \colon U \to U$ is a linear such that $g \cdot f = f$ for all $g \in G$. Then we compute

$$\begin{aligned} (g \cdot f)(u) = f(u) &\implies g \cdot f(g^{-1} \cdot u) = f(u) \\ &\implies f(g^{-1} \cdot u) = g^{-1} \cdot f(u) \quad \text{for all } g \in G \text{ and } u \in U \end{aligned}$$

This means that one has

$$f(g \cdot u) = g \cdot f(u)$$

for all $g \in G$ and $u \in U$.

Using Exercise 5.11,

$$\begin{aligned} \dim \operatorname{Hom}_G(U,V) &= \dim \operatorname{Hom}(U,V)^G \\ &= \frac{1}{|G|} \sum_{g \in G} \chi_{\operatorname{Hom}(U,V)}(g) \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{\chi_U(g)} \chi_V(g) \\ &= \langle \chi_V, \chi_U \rangle. \end{aligned}$$

Since $\dim \mathrm{Hom}_G(U,V) \in \mathbb{R}$, one has $\langle \chi_U, \chi_V \rangle = \overline{\langle \chi_V, \chi_U \rangle} = \langle \chi_V, \chi_U \rangle$ and the claim follows. □

Let G be a finite group and $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. Note that k is the number of conjugacy classes of G. Let $g_1, \ldots, g_k$ be representatives of conjugacy classes of G. The **matrix of characters** of G is $X = (X_{ij})$, where

$$X_{ij} = \chi_i(g_j)$$

for $i, j \in \{1, \ldots, k\}$.

Example 5.15. Let $G = \mathbb{S}_3$. The group G has three conjugacy classes, so $|\mathrm{Irr}(G)| = 3$. Let $g_1 = \mathrm{id}$, $g_2 = (12)$ and $g_3 = (123)$. We know that $6 = n_1^2 + n_2^2 + n_3^2$. We know two degree-one (irreducible) representations of G, the trivial one and the sign. This implies that $n_1 = n_2 = 1$ and $n_3 = 2$. The matrix of characters is then

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	?	?

Lecture 4

§6. Schur's orthogonality relations

We start with a crucial exercise. It is known as Schur's lemma.

Exercise 6.1. If G is a group and U and V are simple $\mathbb{C}[G]$-modules, then a non-zero module homomorphism $U \to V$ is an isomorphism.

We now discuss a handy application of Schur's lemma. Let G be a finite group and S be a simple $\mathbb{C}[G]$-module. We claim that $\mathrm{Hom}_G(S,S) \simeq \mathbb{C}$. Let $f \in \mathrm{Hom}_G(S,S)$ and $\lambda \in \mathbb{C}$ be an eigenvalue of f. Then $f - \lambda\,\mathrm{id}\colon S \to S$ is not invertible. By Schur's lemma, $f - \lambda\,\mathrm{id} = 0$ and hence $f = \lambda\,\mathrm{id}$.

Theorem 6.2 (Schur). *Let G be a finite group and $\chi, \psi \in \mathrm{Irr}(G)$. Then*

$$\langle \chi, \psi \rangle = \begin{cases} 1 & \text{if } \chi = \psi, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $S_1, \ldots, S_k$ be the simples of $\mathbb{C}[G]$. For each j, let χ_j be the irreducible character of S_j. Then

$$\langle \chi_i, \chi_j \rangle = \dim \mathrm{Hom}_G(S_i, S_j) = \begin{cases} 1 & \text{if } S_i \simeq S_j, \\ 0 & \text{otherwise.} \end{cases}$$

But we know that $S_i \simeq S_j$ if and only if $\chi_i = \chi_j$. □

With the theorem, one can construct the character table of $\mathbb{S}_3$. For example, this can be done using that $\langle \chi_3, \chi_3 \rangle = 1$ and that $\langle \chi_1, \chi_3 \rangle = 0$. As an exercise, check that the character table of $\mathbb{S}_3$ is given by

	1	(12)	(123)
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	-1

Exercise 6.3. Let G be a finite group. Prove that $\mathrm{Irr}(G)$ is an orthonormal basis of $\mathrm{cf}(G)$.

The previous exercise has some consequences. Let G be a finite group and assume that $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. If $\alpha = \sum a_i \chi_i$, then $\alpha = \sum \langle \alpha, \chi_i \rangle \chi_i$.

Theorem 6.4. *Let G be a finite group and $S_1, \ldots, S_k$ be the simples of G. Then the left regular $\mathbb{C}[G]$-module decomposes as*

$$\mathbb{C}[G] \simeq \bigoplus_{i=1}^{k} (\dim S_i) S_i.$$

Proof. Let $n = |G|$. Assume that $G = \{g_1, \ldots, g_n\}$. Decompose the $\mathbb{C}[G]$-module corresponding to the left regular representation as

$$\mathbb{C}[G] \simeq a_1 S_1 \oplus \cdots \oplus a_k S_k$$

for some integers $a_1, \ldots, a_k \geq 0$. Let $L \colon G \to \mathbb{S}_G$, $g \mapsto L_g$, where $L_g(g_j) = g g_j$ for all j. Since the matrix of L_g in the basis $\{g_1, \ldots, g_n\}$ is

$$(L_g)_{ij} = \begin{cases} 1 & \text{if } g_i = g g_j, \\ 0 & \text{otherwise,} \end{cases}$$

one obtains that

$$\chi_L(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover,

$$\chi_L = \sum_{i=1}^{k} a_i \chi_i = \sum_{i=1}^{k} \langle \chi_L, \chi_i \rangle \chi_i$$

and

$$a_i = \langle \chi_L, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_L(g) \overline{\chi_i(g)} = \frac{1}{|G|} |G| \overline{\chi_i(1)} = \dim S_i.$$

Thus $\mathbb{C}[G] \simeq \bigoplus_{i=1}^{k} (\dim S_i) S_i$. □

If G is a finite group, let $\mathrm{Char}(G)$ be the set of characters of G.

Exercise 6.5. Let $n \in \{1, 2, 3\}$. Let G be a finite group and $\alpha \in \mathrm{Char}(G)$. Prove that α is the sum of n irreducible characters if and only if $\langle \alpha, \alpha \rangle = n$.

We now prove Schur's second orthogonality relation.

Theorem 6.6 (Schur). *Let G be a finite group and $g, h \in G$. Then*

$$\sum_{\chi\in\mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |C_G(g)| & \text{if } g \text{ and } h \text{ are conjugate,} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $g_1,\dots,g_r$ be the representatives of the conjugacy classes of G. Assume that $\mathrm{Irr}(G) = \{\chi_1,\dots,\chi_r\}$. For each $k \in \{1,\dots,r\}$, let $c_k = (G : C_G(g_k))$ denote the size of the conjugacy class of g_k. Then

$$\langle \chi_i, \chi_j \rangle = \frac{1}{|G|}\sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = \frac{1}{|G|}\sum_{k=1}^{r} c_k \chi_i(g_k)\overline{\chi_j(g_k)}.$$

We write this as $I = \frac{1}{|G|} XDX^*$, where I denotes the identity matrix, $X_{ij} = \chi_i(g_j)$, $X^* = \overline{X}^T$ and

$$D = \begin{pmatrix} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_r \end{pmatrix}.$$

Since, in matrices, $AB = I$ implies $BA = I$, it follows that $I = \frac{1}{|G|} X^*XD$. Thus, using that $|G| = c_k|C_G(g_k)|$ holds for all k,

$$(|G|D^{-1})_{ij} = (X^*X)_{ij} = \sum_{k=1}^{r} \overline{\chi_k(g_i)}\chi_k(g_j) = \begin{cases} |C_G(g_j)| & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases} \qquad \square$$

Theorem 6.7 (Solomon). *Let G be a finite group and $\mathrm{Irr}(G) = \{\chi_1,\dots,\chi_r\}$. If $g_1,\dots,g_r$ are the representatives of the conjugacy classes of G and $i \in \{1,\dots,r\}$, then*

$$\sum_{j=1}^{r} \chi_i(g_j) \in \mathbb{Z}_{\geq 0}.$$

Proof. Let $n = |G|$. Assume that $G = \{g_1, g_2, \dots, g_r, g_{r+1}, \dots, g_n\}$. Let V be the complex vector space with basis $\{g_1,\dots,g_n\}$. The action of G on G by conjugation induces a group homomorphism $\rho\colon G \to \mathbf{GL}(V)$, $g \mapsto \rho_g$, where $\rho_g(h) = ghg^{-1}$. The matrix of ρ_g in the basis $\{g_1,\dots,g_n\}$ is

$$(\rho_g)_{ij} = \begin{cases} 1 & \text{if } g_jg = gg_i, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\chi_\rho(g) = \operatorname{trace}\rho_g = \sum_{k=1}^{|G|} (\rho_g)_{kk} = |\{k : g_kg = gg_k\}| = |C_G(g)|.$$

Write $\chi_\rho = \sum_{i=1}^{r} m_i\chi_i$ for $m_1,\dots,m_r \geq 0$. For each j let $c_j = (G : C_G(g_j))$. Then

$$m_i = \langle \chi_\rho, \chi_i \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_\rho(g) \overline{\chi_i(g)}$$
$$= \frac{1}{|G|} \sum_{j=1}^{r} c_j |C_G(g_j)| \overline{\chi_i(g_j)} = \sum_{j=1}^{r} \overline{\chi_i(g_j)}. \qquad \square$$

§7. Algebraic integers and characters

Definition 7.1. Let $\alpha \in \mathbb{C}$. We say that α is **algebraic integer** if $f(\alpha) = 0$ for some monic polynomial $f \in \mathbb{Z}[X]$.

Let $\mathbb{A}$ be the set of algebraic integers. Note that $\mathbb{Z} \subseteq \mathbb{A}$.

Example 7.2. Every root of one is an algebraic integer.

Proposition 7.3. $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

Proof. Let $m/n \in \mathbb{Q}$ with $\gcd(m,n) = 1$ and $n > 0$. If $f(m/n) = 0$ for some

$$f = X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$$

of degree $k \geq 1$, then

$$0 = n^k f(m/n) = m^k + a_{k-1}m^{k-1}n + \cdots + a_1 m n^{k-1} + a_0 n^k.$$

This implies that

$$m^k = -n\left(a_{k-1}m^{k-1} + \cdots + a_1 m n^{k-2} + a_0 n^{k-1}\right)$$

and hence n divides m^k. Thus $n \in \{-1, 1\}$ and therefore $m/n \in \mathbb{Z}$. $\square$

Proposition 7.4. *Let $x \in \mathbb{C}$. Then $x \in \mathbb{A}$ if and only if x is an eigenvalue of an integer matrix.*

Proof. Let us prove the non-trivial implication. Let

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$$

be such that $f(x) = 0$. Then x is an eigenvalue of the companion matrix of f, that is the matrix

$$C(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix} \in \mathbb{Z}^{n \times n}. \qquad \square$$

Theorem 7.5. *$\mathbb{A}$ is a subring of $\mathbb{C}$.*

Proof. Let $\alpha, \beta \in \mathbb{A}$. By the previous proposition, α is an eigenvalue of an integer matrix $A \in \mathbb{Z}^{n\times n}$, say $Av = \alpha v$ for some $v \neq 0$, β is an eigenvalue of an integer matrix $B \in \mathbb{Z}^{m\times m}$, say $Bw = \beta w$ for some $w \neq 0$. Then

$$(A \otimes I_{m\times m} + I_{n\times n} \otimes B)(v \otimes w) = (\alpha + \beta)(v \otimes w),$$

where $I_{k\times k}$ denotes the $(k \times k)$ identity matrix, and

$$(A \otimes B)(v \otimes w) = (\alpha\beta)v \otimes w.$$

This implies that $\alpha + \beta \in \mathbb{A}$ and $\alpha\beta \in \mathbb{A}$, again by the previous proposition. □

Theorem 7.6. *Let G be a finite group. If $\chi \in \mathrm{Char}(G)$ and $g \in G$, then $\chi(g) \in \mathbb{A}$.*

Proof. Let φ be a representation of G such that $\chi_\varphi = \chi$. Since φ_g is diagonalizable with eigenvalues $\lambda_1, \ldots, \lambda_k \in \mathbb{A}$ (because G is finite and the λ_j are roots of one),

$$\chi(g) = \operatorname{trace} \varphi_g = \sum_{i=1}^{k} \lambda_i \in \mathbb{A}.$$ □

Lecture 5

Theorem 7.7. *Let G be a finite group, $\chi \in \mathrm{Irr}(G)$ and $g \in G$. If K is the conjugacy class of g in G, then*

$$\frac{\chi(g)}{\chi(1)}|K| \in \mathbb{A}.$$

To prove the theorem, we need a lemma.

Lemma 7.8. *Let $x \in \mathbb{C}$. Then $x \in \mathbb{A}$ if and only if there exist $z_1, \dots, z_k \in \mathbb{C}$ not all zero such that $xz_i = \sum_{j=1}^{k} a_{ij} z_j$ for some $a_{ij} \in \mathbb{Z}$ and all $i \in \{1, \dots, k\}$.*

Proof. Let us first prove $\implies$. Let $f = X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$ be such that $f(x) = 0$. For $i \in \{1, \dots, k\}$ let $z_i = x^{i-1}$. Then $xz_i = x^i = z_{i+1}$ for all $i \in \{1, \dots, k-1\}$. Moreover, $xz_k = x^k = -a_0 - a_1 x - \cdots - a_{k-1}x^{k-1}$.

We now prove $\impliedby$. Let $A = (a_{ij}) \in \mathbb{Z}^{k \times k}$ and Z be the column vector $Z = \begin{pmatrix} z_1 \\ \vdots \\ z_k \end{pmatrix}$.

Note that Z is non-zero. Moreover, $AZ = xZ$, as

$$(AZ)_i = \sum_{j=1}^{k} a_{ij} z_j = xz_i = (xZ)_i$$

for all i. Thus x is an eigenvalue of $A \in \mathbb{Z}^{k \times k}$ and hence $x \in \mathbb{A}$. □

We now prove the theorem. We will use the following notation: if χ is a character of a group G and C is a conjugacy class of G, then $\chi(g) = \chi(xgx^{-1})$ for all $x \in G$. We write $\chi(C)$ to denote the value $\chi(g)$ for any $g \in C$.

Proof of Theorem 7.6. Let φ be a representation of G with character χ. Let $C_1, \dots, C_r$ be the conjugacy classes of G and for every $i \in \{1, \dots, r\}$ let

$$T_i = \sum_{x \in C_i} \varphi_x.$$

Claim. $T_i = \left(\frac{|C_i|}{\chi(1)}\chi(C_i)\right)\mathrm{id}$.

We proceed in several steps. First, we prove that $T_i = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{C}$. We prove that T_i is a morphism of representations:

$$\varphi_g T_i \varphi_g^{-1} = \sum_{x\in C_i} \varphi_g \varphi_x \varphi_g^{-1} = \sum_{x\in C_i} \varphi_{gxg^{-1}} = \sum_{y\in C_i} \varphi_y = T_i.$$

Now Schur's lemma implies that $T_i = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{C}$.

We now prove that

$$\lambda = \frac{|C_i|\chi(C_i)}{\chi(1)}.$$

To prove this we compute λ:

$$\lambda\chi(1) = \operatorname{trace}(\lambda\,\mathrm{id}) = \operatorname{trace} T_i = \sum_{x\in C_i} \operatorname{trace}\varphi_x = \sum_{x\in C_i} \chi(x) = |C_i|\chi(C_i).$$

Then the claim follows.

Now we claim that

$$T_i T_j = \sum_{k=1}^{r} a_{ijk} T_k$$

for some $a_{ijk} \in \mathbb{Z}_{\geq 0}$. In fact,

$$T_i T_j = \sum_{x\in C_i}\sum_{y\in C_j} \varphi_x\varphi_y = \sum_{x\in C_i}\sum_{y\in C_j} \varphi_{xy} = \sum_{g\in G} a_{ijg}\varphi_g,$$

where a_{ijg} is the number of elements $g \in G$ that can be written as $g = xy$ for $x \in C_i$ and $y \in C_j$.

Claim. The a_{ijg} depend only on the conjugacy class of g.

Let $X_g = \{(x,y) \in C_i \times C_j : g = xy\}$. If $h = kgk^{-1}$, the map

$$X_g \to X_h, \quad (x,y) \mapsto (kxk^{-1}, kyk^{-1}),$$

is well-defined. It is bijective with inverse

$$X_h \to X_g, \quad (a,b) \mapsto (k^{-1}ak, k^{-1}bk).$$

Hence $|X_g| = |X_h|$.

Now

$$T_i T_j = \sum_{g\in G} a_{ijg}\varphi_g = \sum_{k=1}^{r}\sum_{g\in C_k} a_{ijg}\varphi_g = \sum_{k=1}^{r} a_{ijg} \sum_{g\in C_k} \varphi_g = \sum_{k=1}^{r} a_{ijk} T_k.$$

Therefore

$$\left(\frac{|C_i|}{\chi(1)}\chi(C_i)\right)\left(\frac{|C_j|}{\chi(1)}\chi(C_j)\right) = \sum_{k=1}^{r} a_{ijk}\left(\frac{|C_k|}{\chi(1)}\chi(C_k)\right). \tag{5.1}$$

By the previous lemma, $x = \frac{|C_j|}{\chi(1)}\chi(C_j) \in \mathbb{A}$. □

§8. Frobenius' theorem

Theorem 8.1 (Frobenius). *Let G be a finite group and $\chi \in \mathrm{Irr}(G)$. Then $\chi(1)$ divides $|G|$.*

Proof. Let φ be an irreducible representation with character χ. Since $\langle \chi, \chi \rangle = 1$,

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

Let $C_1, \ldots, C_r$ be the conjugacy classes of G. Then

$$\frac{|G|}{\chi(1)} = \sum_{i=1}^{r} \sum_{g \in C_i} \frac{\chi(g)}{\chi(1)}\overline{\chi(g)} = \sum_{i=1}^{r} \left(\frac{|C_i|}{\chi(1)}\chi(C_i)\right)\overline{\chi(C_i)} \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z},$$

as $\overline{\chi(C_i)} \in \mathbb{A}$. This implies that $\chi(1)$ divides $|G|$. □

The character table gives information on the structure of the group. For example, with the previous result, one can easily prove that groups of order p^2 (where p is a prime number) are abelian.

Exercise 8.2. Let p and q be prime numbers such that $p < q$. If $q \not\equiv 1 \bmod p$, then a group of order pq is abelian.

Another application:

Theorem 8.3. *Let G be a finite simple group. Then $\chi(1) \neq 2$ for all $\chi \in \mathrm{Irr}(G)$.*

Proof. Let $\chi \in \mathrm{Irr}(G)$ be such that $\chi(1) = 2$. Let $\rho\colon G \to \mathbf{GL}_2(\mathbb{C})$ be an irreducible representation of G with character χ. Since G is simple, $\ker\rho = \{1\}$. Since $\chi(1) = 2$, G is non-abelian and hence $[G, G] = G$. Since G has $(G : [G, G]) = 1$ degree-one characters, it follows that G has only one degree-one character, the trivial one. The composition

$$G \xhookrightarrow{\rho} \mathbf{GL}_2(\mathbb{C}) \xrightarrow{\det} \mathbb{C}^\times$$

is a degree-one representation, which means that $\det\rho_g = 1$ for all $g \in G$. By Frobenius' theorem, $|G|$ is even (because $2 = \chi(1)$ divides $|G|$). Let $x \in G$ be such that $|x| = 2$ (Cauchy's theorem). Then $|\rho_x| = 2$, as ρ is injective. Since ρ_x is diagonalizable, there exists $C \in \mathbf{GL}_2(\mathbb{C})$ such that

$$C\rho_x C^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

for some $\lambda, \mu \in \{-1, 1\}$. Since $1 = \det \rho_x = \lambda\mu$ and ρ is non-trivial, $\lambda = \mu = -1$. In particular, $C\rho_x C^{-1}$ is central and hence ρ_x is central. Since ρ is injective, x is central and thus $Z(G) \neq \{1\}$, a contradiction. □

Theorem 8.4 (Schur). *Let G be a finite group and $\chi \in \mathrm{Irr}(G)$. Then $\chi(1)$ divides $(G : Z(G))$.*

We need a lemma.

Lemma 8.5. *Let G and G_1 be finite groups. If ρ is an irreducible representation of G and ρ_1 is an irreducible representation of G_1, then $\rho \otimes \rho_1$ is an irreducible representation of $G \times G_1$.*

Proof. Write $\chi = \chi_\rho$ and $\chi_1 = \chi_{\rho_1}$. Since χ is irreducible, $\langle \chi, \chi \rangle = 1$. Similarly, $\langle \chi_1, \chi_1 \rangle = 1$. Now $\rho \otimes \rho_1$ is irreducible, as

$$\begin{aligned}
\langle \chi\chi_1, \chi\chi_1 \rangle &= \frac{1}{|G \times G_1|} \sum_{(g,g_1) \in G \times G_1} (\chi\chi_1)(g, g_1)\overline{(\chi\chi_1)(g, g_1)} \\
&= \frac{1}{|G||G_1|} \sum_{g \in G} \sum_{g_1 \in G} \chi(g)\chi_1(g_1)\overline{\chi(g)\chi_1(g_1)} \\
&= \frac{1}{|G||G_1|} \sum_{g \in G} \overline{\chi(g)} \sum_{g_1 \in G} \chi(g)\chi_1(g_1)\overline{\chi_1(g_1)} \\
&= \langle \chi, \chi \rangle \langle \chi_1, \chi_1 \rangle = 1.
\end{aligned}$$

□

Exercise 8.6. Let G and G_1 be finite groups. Prove that irreducible characters of $G \times G_1$ are of the form $\chi \otimes \chi_1$ for $\chi \in \mathrm{Irr}(G)$ and $\chi_1 \in \mathrm{Irr}(G_1)$.

We now prove Schur's theorem. The proof goes back to Tate, it uses the *tensor power trick*. See Tao's blog `https://terrytao.wordpress.com` for other applications of this powerful trick.

Proof of Theorem 8.4. Let $\rho \colon G \to \mathbf{GL}(V)$ be an irreducible representation with character χ. Let $z \in Z(G)$. Then ρ_z commutes with ρ_g for all $g \in G$. By Schur's lemma, $\rho_z(v) = \lambda(z)v$ for all $v \in V$. Note that $\lambda \colon Z(G) \to \mathbb{C}^\times$, $z \mapsto \lambda(z)$, is a well-defined group homomorphism, as

$$\lambda(z_1 z_2)v = \rho_{z_1 z_2}(v) = \rho_{z_1}\rho_{z_2}(v) = \lambda(z_2)\rho_{z_1}(v) = \lambda(z_1)\lambda(z_2)v$$

for all $v \in V$ and $z_1, z_2 \in Z(G)$.

Let $n \in \mathbb{Z}_{\geq 1}$. Write $G^n = G \times \cdots \times G$ (n-times). Let

$$\sigma \colon G^n \to \mathbf{GL}(V^{\otimes n}), \quad (g_1, \ldots, g_n) \mapsto \rho_{g_1} \otimes \cdots \otimes \rho_{g_n}.$$

The character of σ is χ^n. Moreover, by the previous lemma, σ is irreducible. We compute:

$$\begin{aligned}\sigma(z_1,\dots,z_n)(v_1\otimes\cdots\otimes v_n) &= z_1v_1\otimes\cdots\otimes z_nv_n\\ &= \lambda(z_1)\cdots\lambda(z_n)v_1\otimes\cdots\otimes v_n\\ &= \lambda(z_1\cdots z_n)v_1\otimes\cdots\otimes v_n.\end{aligned}$$

Let

$$H=\{(z_1,\dots,z_n)\in Z(G)^n : z_1\cdots z_n=1\}\subseteq G^n.$$

The central subgroup H acts trivially on $V^{\otimes n}$, so there exists a representation

$$\tau\colon G^n/H\to \mathbf{GL}(V^{\otimes n}).$$

Since σ is irreducible, so is τ. By Frobenius' theorem, $\chi(1)$ divides $|G|$ and $\chi(1)^n$ divides $|G^n/H|=\frac{|G|^n}{|Z(G)|^{n-1}}$. Write $|G|=\chi(1)s$ and $|G|(G:Z(G))^{n-1}=\chi(1)^nr$ for some $r,s\in\mathbb{Z}$. Let a and b be such that $\gcd(a,b)=1$ and $\frac{a}{b}=\frac{(G:Z(G))}{\chi(1)}$. Then

$$s\left(\frac{a}{b}\right)^{n-1}=s\frac{(G:Z(G))^{n-1}}{\chi(1)^{n-1}}=\frac{|G|}{\chi(1)}\frac{(G:Z(G))^{n-1}}{\chi(1)^{n-1}}=r\in\mathbb{Z}.$$

Thus b^{n-1} divides s and hence $b=1$ (because n is arbitrary). □

§9. Examples of character tables

Let G be a finite group and $\chi_1,\dots,\chi_r$ be the irreducible characters of G. Without loss of generality we may assume that χ_1 is the trivial character, i.e. $\chi_1(g)=1$ for all $g\in G$. Recall that r is the number of conjugacy classes of G. Each χ_j is constant on conjugacy classes. The **character table** of G is given by

	1	k_2	$\cdots$	k_r
	1	g_2	$\cdots$	g_r
χ_1	1	1	$\cdots$	1
χ_2	n_2	$\chi_2(g_2)$	$\cdots$	$\chi_2(g_r)$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
χ_r	n_r	$\chi_r(g_2)$	$\cdots$	$\chi_r(g_r)$

where the n_j are the degrees of the irreducible representations of G and each k_j is the size of the conjugacy class of the element g_j. By convention, the character table contains not only the values of the irreducible characters of the group.

Example 9.1. Sea $G=\langle g : g^4=1\rangle$ be the cyclic group of order four. The character table of G is given by

	1	1	1	1
	1	g	g^2	g^3
χ_1	1	1	1	1
χ_2	1	λ	λ^2	λ^3
χ_3	1	λ^2	λ^4	λ^2
χ_4	1	λ^3	λ^2	λ

Let us see how to see this calculation in the computer:

```
julia> G = cyclic_group(4);

julia> T = character_table(G)
<pc group of size 4 with 2 generators>

  2  2    2  2    2

    1a   4a 2a   4b

X_1  1    1  1    1
X_2  1  z_4 -1 -z_4
X_3  1   -1  1   -1
X_4  1 -z_4 -1  z_4
```

Some remarks:

1) The symbol `z_4` denotes a primitive fourth root of 1.
2) The function `character_table` computes more information, not only the character table of the group. The function computes other stuff:

```
julia> orders_class_representatives(T)
4-element Vector{Int64}:
 1
 4
 2
 4

julia> class_lengths(T)
4-element Vector{fmpz}:
 1
 1
 1
 1

julia> orders_centralizers(T)
4-element Vector{fmpz}:
 4
 4
 4
 4
```

Example 9.2. The character table of the group $C_2 \times C_2 = \{1, a, b, ab\}$ is

	1	1	1	1
	1	a	b	ab
χ_1	1	1	1	1
χ_2	1	1	-1	-1
χ_3	1	-1	1	-1
χ_4	1	-1	-1	1

Let us do this by computer:

```
julia> A = abelian_group(PcGroup, [2,2]);

julia> character_table(A)
<pc group of size 4 with 2 generators>

  2  2  2  2  2

    1a 2a 2b 2c

X_1  1  1  1  1
X_2  1 -1  1 -1
X_3  1  1 -1 -1
X_4  1 -1 -1  1
```

Exercise 9.3. Let A and B be abelian groups. We write $\mathrm{Irr}(A) = \{\rho_1, \ldots, \rho_r\}$ and $\mathrm{Irr}(B) = \{\phi_1, \ldots, \phi_s\}$. Prove that the maps

$$\varphi_{ij} \colon A \times B \to \mathbb{C}^\times, \quad (a, b) \mapsto \rho_i(a)\phi_j(b),$$

where $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, s\}$, are the irreducible representations of $A \times B$.

Example 9.4. The character table of $\mathbb{S}_3$ is given by

	1	3	2
	1	(12)	(123)
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

Let us recall one possible way to compute this table. Degree-one irreducibles were easy to compute. To compute the third row of the table, one possible approach is to use the irreducible representation

$$(12) \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad (123) \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Then

$$\chi_3((12)) = \mathrm{trace}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = 0,$$

$$\chi_3((123)) = \chi_3((12)(23)) = \mathrm{trace}\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = -1.$$

We should remark that the irreducible representation mentioned is not needed to compute the third row of the character table.

```
julia> S3 = symmetric_group(3);

julia> T = character_table(S3)
Sym( [ 1 .. 3 ] )

  2  1  1  .
  3  1  .  1
```

```
    1a 2a 3a
 2P 1a 1a 3a
 3P 1a 2a 1a

X_1  1 -1  1
X_2  2  . -1
X_3  1  1  1
```

As we did before, some extra information was computed:

```
julia> orders_class_representatives(T)
3-element Vector{Int64}:
 1
 2
 3

julia> class_lengths(T)
3-element Vector{fmpz}:
 1
 3
 2

julia> orders_centralizers(T)
3-element Vector{fmpz}:
 6
 2
 3
```

Exercise 9.5. Compute the character table of $\mathbb{S}_4$.

Exercise 9.6. Compute the character table of $\mathbb{A}_4$.

Exercise 9.7. Compute the character table of the quaternion group Q_8.

Exercise 9.8. Compute the character table of the dihedral group of eight elements.

Lecture 6

§10. McKay's conjecture

Let G be a finite group and let p be a prime number dividing $|G|$. Write $\mathrm{Syl}_p(G)$ to denote the (non-empty) set of Sylow p-subgroups of G. Recall that the *normalizer* of P is the subgroup

$$N_G(P) = \{g \in G : gPg^{-1} = P\}.$$

The following conjecture was made by McKay for the prime $p = 2$ and simple groups and later generalized by Alperin in [1] and independently by Isaacs en [20].

Conjecture 10.1 (McKay). Let p be a prime. If G is a finite group and $P \in \mathrm{Syl}_p(G)$, then

$$|\{\chi \in \mathrm{Irr}(G) : p \nmid \chi(1)\}| = |\{\psi \in \mathrm{Irr}(N_G(P))| : p \nmid \psi(1)\}|.$$

McKay's conjecture is still open and is an important problem in representation theory. The conjecture was proved for several classes of groups. Isaacs proved the conjecture for solvable groups, see for example [20, 23]. Malle and Späth prove the conjecture for $p = 2$.

Theorem 10.2 (Malle–Späth). *If G is finite and $P \in \mathrm{Syl}_2(G)$, then*

$$|\{\chi \in \mathrm{Irr}(G) : 2 \nmid \chi(1)\}| = |\{\psi \in \mathrm{Irr}(N_G(P))| : 2 \nmid \psi(1)\}|.$$

The proof appears in [32] and uses the classification of finite simple groups. It uses a deep result of Isaacs, Malle and Navarro [24].

We cannot prove Malle–Späth theorem here. However, we can use the computer to prove some particular cases with the following cuntion:

```
gap> McKay := function(G, p)
> local N, n, m;
> N := Normalizer(G, SylowSubgroup(G, p));
> n := Number(Irr(G), x->Degree(x) mod p <> 0);
> m := Number(Irr(N), x->Degree(x) mod p <> 0);
> if n = m then
> return true;
```

```
> else
> return false;
> fi;
> end;
function( G, p ) ... end
```

As a concrete example, let us verify McKay's conjecture for the Mathieu simple group M_{11} of order 7920.

```
gap> M11 := MathieuGroup(11);;
gap> PrimeDivisors(Order(M11));
[ 2, 3, 5, 11 ]
gap> McKay(M11,2);
true
gap> McKay(M11,3);
true
gap> McKay(M11,5);
true
gap> McKay(M11,11);
true
```

The following conjecture refines McKay's conjecture. It was formulated by Isaacs and Navarro:

Conjecture 10.3 (Isaacs–Navarro). Let p be a prime and $k \in \mathbb{Z}$. If G is a finite group and $P \in \mathrm{Syl}_p(G)$, then

$$|\{\chi \in \mathrm{Irr}(G) : p \nmid \chi(1) \text{ y } \chi(1) \equiv \pm k \bmod p\}| = |\{\psi \in \mathrm{Irr}(N_G(P)) | : p \nmid \psi(1) \text{ y } \psi(1) \equiv \pm k \bmod p\}|.$$

Isaacs–Navarro conjecture is still open. However, it is known to be true for solvable groups, sporadic simple groups and symmetric groups, see [25].

```
gap> IsaacsNavarro := function(G, k, p)
> local mG, mN, N;
> N := Normalizer(G, SylowSubgroup(G, p));
> mG := Number(Filtered(Irr(G), x->Degree(x)\
> mod p <> 0), x->Degree(x) mod p in [-k,k] mod p);
> mN := Number(Filtered(Irr(N), x->Degree(x)\
> mod p <> 0), x->Degree(x) mod p in [-k,k] mod p);
> if mG = mN then
> return mG;
> else
> return false;
> fi;
> end;
function( G, k, p ) ... end
```

It is an exercise to verify Isaacs–Navarro conjecture in some small cases, for example Mathieu simple group M_{11}.

§11. Commutators

Let G be a finite group with conjugacy classes $C_1, \ldots, C_s$. For $i \in \{1, \ldots, s\}$ and $\chi \in \mathrm{Irr}(G)$ let

$$\omega_\chi(C_i) = \frac{|C_i|\chi(C_i)}{\chi(1)} \in \mathbb{A}.$$

In the proof of Theorem 7.6, Equality (5.1), we obtained that

$$\omega_\chi(C_i)\omega_\chi(C_j) = \sum_{k=1}^{k} a_{ijk}\omega_\chi(C_k), \tag{6.1}$$

where a_{ijk} is the number of solutions of $xy = z$ with $x \in C_i$, $y \in c_j$ and $z \in C_k$.

Theorem 11.1 (Burnside). *Let G be a finite group with conjugacy classes $C_1, \ldots, C_s$. Then*

$$a_{ijk} = \frac{|C_i||C_j|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C_i)\chi(C_j)\overline{\chi(C_k)}}{\chi(1)}.$$

Proof. By (6.1),

$$\frac{|C_i||C_j|}{\chi(1)}\chi(C_i)\chi(C_j) = \sum_{k=1}^{s} a_{ijk}|C_k|\chi(C_k).$$

Multiply by $\overline{\chi(C_l)}$ and sum over all $\chi \in \mathrm{Irr}(G)$ to obtain

$$\begin{aligned}
|C_i||C_j| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\overline{\chi(C_l)}}{\chi(1)}\chi(C_i)\chi(C_j) &= \sum_{\chi \in \mathrm{Irr}(G)} \sum_{k=1}^{s} a_{ijk}|C_k|\chi(C_k)\overline{\chi(C_l)} \\
&= \sum_{k=1}^{s} a_{ijk}|C_k| \sum_{\chi \in \mathrm{Irr}(G)} \chi(C_k)\overline{\chi(C_l)} \\
&= a_{ijk}|G|,
\end{aligned}$$

because

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(C_k)\overline{\chi(C_l)} = \begin{cases} \frac{|G|}{|C_l|} & \text{if } k = l, \\ 0 & \text{otherwise.} \end{cases}$$

□

Theorem 11.2 (Burnside). *Let G be a finite group and $g, x \in G$. Then g and $[x, y]$ are conjugate for some $y \in G$ if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(x)|^2\chi(g)}{\chi(1)} > 0.$$

Proof. Let $C_1, \ldots, C_s$ be the conjugacy classes of G. Assume that $x \in C_i$ and $g \in C_k$ for some i and k. Then $C_i^{-1} = \{z^{-1} : z \in C_i\} = C_j$ for some j. By Burnside's theorem,

$$a_{ijk} = \frac{|C_i|^2}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{|\chi(C_i)|^2\overline{\chi(C_k)}}{\chi(1)}$$

We first prove $\Longleftarrow$. Since $a_{ijk} > 0$, there exist $u \in C_i$ and $v \in C_j$ such that $g = uv$ (since $zgz^{-1} = u_1v_1$ for some $u_1 \in C_i$ and $v_1 \in C_j$, it follows that $g = (z^{-1}u_1z)(z^{-1}v_1z)$, so take $u = z^{-1}u_1z \in C_i$ and $v = z^{-1}v_1z \in C_j$). If x and u are conjugate, say $u = zxz^{-1}$ for some z, then x^{-1} and v are conjugate, as

$$zxz^{-1} = u \implies zx^{-1}z^{-1} = u^{-1} \in C_i^{-1} = C_j.$$

Let $z_2 \in G$ be such that $z_2x^{-1}z_2 = v$. If $y = z^{-1}z_2$, then g and $[x, y]$ are conjugate, as

$$g = uv = (zxz^{-1})(z_2x^{-1}z_2^{-1}) = (zxyx^{-1}y^{-1})yz_2^{-1} = z[x, y]z^{-1}.$$

We now prove $\Longrightarrow$. Let $y \in G$ be such that g and $[x, y]$ are conjugate, say $g = z[x, y]z^{-1}$ for some $z \in G$. Let $v = yxy^{-1}$. Then g and $xv^{-1} = xyx^{-1}y^{-1} = [x, y]$ are conjugate. In particular, since $g \in C_iC_j$, $a_{ijk} > 0$. □

Exercise 11.3. Let G be a finite group, $g \in G$ and $\chi \in \mathrm{Irr}(G)$. Prove that

$$\sum_{h \in G} \chi([g, h]) = \frac{|G|}{\chi(1)}|\chi(g)|^2.$$

Prove also that

$$\chi(g)\chi(h) = \frac{\chi(1)}{|G|} \sum_{z \in G} \chi(zgz^{-1}h)$$

holds for all $h \in G$.

We now prove a theorem of Frobenius that uses character tables to recognize commutators. For that purpose, let

$$\tau(g) = |\{(x, y) \in G \times G : [x, y] = g\}|.$$

Theorem 11.4 (Frobenius). *Let G be a finite group. Then*

$$\tau(g) = |G| \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)}.$$

Proof. Let $\chi \in \mathrm{Irr}(G)$. Since χ is irreducible,

$$1 = \langle \chi, \chi \rangle = \frac{1}{|G|} \sum_{z \in G} \chi(z)\overline{\chi(z)} = \frac{1}{|G|} \sum_{C} |C|\chi(C)\overline{\chi(C)},$$

where the last sum is taken over all conjugacy classes of G. Let $g \in G$ and C be the conjugacy class of g. The equation $xu^{-1} = g$ with $x \in C$ and $u \in C^{-1}$ has

$$\frac{|C||C|^{-1}}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(C)\chi(C^{-1})\chi(g^{-1})}{\chi(1)}$$

solutions. If (x,u) is a solution of $xu^{-1} = g$, then there are $|C_G(x)|$ elements y such that $yxy^{-1} = u$. ($yxy^{-1} = u = y_1xy_1^{-1}$ implies that $y_1^{-1}y \in C_G(x)$ which implies $yC_G(x) = y_1C_G(x)$.) Now $[x,y] = (xyx^{-1})y^{-1} = g$ has

$$|C| \sum_{\chi} \frac{\chi(C)\chi(C^{-1})\chi(g^{-1})}{\chi(1)}$$

solutions, where the sum is taken over all irreducible characters of G. Now we sum over all conjugacy classes of G:

$$\begin{aligned}\sum_{C}\sum_{\chi} \frac{\chi(C)\chi(C^{-1})\chi(g^{-1})}{\chi(1)} &= \sum_{\chi} \frac{\chi(g^{-1})}{\chi(1)} \left(\sum_{C} |C|\chi(C)\chi(C^{-1}) \right) \\ &= |G| \sum_{\chi} \frac{\chi(g^{-1})}{\chi(1)}.\end{aligned}$$

From this the formula follows. □

Application:

Corollary 11.5. *Let G be a finite group and $g \in G$. Then g is a commutator if and only if*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0.$$

§12. Ore's conjecture

In 1951 Ore and independently Ito proved that every element of any alternating simple group is a commutator. Ore also mentioned that "it is possible that a similar theorem holds for any simple group of finite order, but it seems that at present we do not have the necessary methods to investigate the question".

Conjecture 12.1 (Ore). Let G be a finite simple non-abelian group. Then every element of G is a commutator.

Ore's conjecture was proved in 2010:

Theorem 12.2 (Liebeck–O'Brien–Shalev–Tiep). *Every element of a non-abelian finite simple group is a commutator.*

The proof appears in [30]. It needs about 70 pages and uses the classification of finite simple groups (CFSG) and character theory. See [31] for more information on Ore's conjecture and its proof a [31].

Despite the fact that the proof of Ore's conjecture is too complicated for this course, we can use the computer to prove the conjecture in some particular cases:

Proposition 12.3. *Ore's conjecture is true for sporadic simple groups.*

Proof. Let G be a finite simple group. We now that $g \in G$ is a commutator if and only if $\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0$. Let us write a computer script to check whether every element in a group is a commutator. Our function needs the character table of a group and returns `true` if every element of the group is a commutator and `false` otherwise.

```
gap> Ore := function(char)
> local s,f,k;
> for k in [1..NrConjugacyClasses(char)] do
> s := 0;
> for f in Irr(char) do
> s := s+f[k]/Degree(f);
> od;
> if s<=0 then
> return false;
> fi;
> od;
> return true;
> end;
function( char ) ... end
```

Now we check Ore's conjecture for Mathieu simple groups and for the Monster group:

```
gap> Ore(CharacterTable("M11"));
true
gap> Ore(CharacterTable("M12"));
true
gap> Ore(CharacterTable("M22"));
true
gap> Ore(CharacterTable("M23"));
true
gap> Ore(CharacterTable("M24"));
true
gap> Ore(CharacterTable("M"));
true
```

It is an exercise to check the conjecture for the other finite sporadic simple groups McL, Ru, Ly, Suz, He, HN, Th, Fi_{22}, Fi_{23}, Fi'_{24}, B, M □

See [29] for other applications of character theory.

§13. Cauchy–Frobenius–Burnside theorem

Theorem 13.1 (Cauchy–Frobenius–Burnside). *Let G be a finite group that acts on a finite set X. If m is the number of orbits, then*

$$m = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}(g)|,$$

where $\operatorname{Fix}(g) = \{x \in X : g \cdot x = x\}$.

Proof. Let $n = |X|$ and V be the complex vector space with basis $\{x : x \in X\}$. Let $\rho \colon G \to \mathbf{GL}_n(\mathbb{C})$, $g \mapsto \rho_g$, be the representation

$$(\rho_g)_{ij} = \begin{cases} 1 & \text{if } g \cdot x_j = x_i, \\ 0 & \text{otherwie.} \end{cases}$$

In particular, $(\rho_g)_{ii} = 1$ if $x_i \in \operatorname{Fix}(g)$ and $(\rho_g)_{ij} = 0$ if $i \neq j$. Thus

$$\chi_\rho(g) = \operatorname{trace} \rho_g = \sum_{i=1}^{n} (\rho_g)_{ii} = |\operatorname{Fix}(g)|.$$

Recall that

$$V^G = \{v \in V : g \cdot v = v \text{ for all } g \in G\}$$

and that

$$\dim V^G = \frac{1}{|G|} \sum_{z \in G} \chi_\rho(z) = \langle \chi_\rho, \chi_1 \rangle$$

where χ_1 is the trivial character of G.

Let $x_1, \ldots, x_m$ be the representatives of the orbits of G on X. For $i \in \{1, \ldots, m\}$, let $v_i = \sum_{x \in G \cdot x_i} x$.

Claim. $\{v_1, \ldots, v_m\}$ is a basis of V^G.

If $g \in G$, then $g \cdot v_i = \sum_{x \in G \cdot x_i} g \cdot x = \sum_{y \in G \cdot x_i} y = v_i$. Hence $\{v_1, \ldots, v_m\} \subseteq V^G$. Moreover, $\{v_1, \ldots, v_m\}$ is linearly independent because the v_j are orthogonal and non-zero:

$$\langle v_i, v_j \rangle = \begin{cases} |G \cdot x_i| & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

We now prove that $V^G = \langle v_1, \ldots, v_m \rangle$. Let $v \in V^G$. Then $v = \sum_{x \in X} \lambda_x$ for some coefficients $\lambda_x \in \mathbb{C}$. If $g \in G$, then $g \cdot v = v$. Since

$$\sum_{x \in X} \lambda_x x = v = g \cdot v = \sum_{x \in X} \lambda_x (g \cdot x) = \sum_{x \in X} \lambda_{g^{-1} \cdot x} x,$$

it follows that $\lambda_x = \lambda_{g^{-1} \cdot x}$ for all $x \in X$ and $g \in G$. This means that if $y, z \in X$ and $g \in G$ is such that $g \cdot y = z$, then $\lambda_y = \lambda_z$. Thus

$$v = \sum_{x \in X} \lambda_x x = \sum_{i=1}^{m} \lambda_{x_i} \sum_{y \in G \cdot x_i} y = \sum_{i=1}^{m} \lambda_{x_i} v_i.$$

Hence

$$m = \dim V^G = \langle \chi_\rho, \chi_1 \rangle = \frac{1}{|G|} \sum_{z \in G} \chi_\rho(z) = \frac{1}{|G|} \sum_{z \in G} |\operatorname{Fix}(z)|. \qquad \square$$

It is possible to give a very short proof of the theorem. For example, for transitive actions (i.e. $m = 1$), we proceed as follows:

$$\sum_{g\in G}|\mathrm{Fix}(g)| = \sum_{g\in G}\sum_{\substack{x\in X\\ g\cdot x=x}} 1 = \sum_{x\in X}\sum_{\substack{g\in G\\ g\cdot x=x}} 1 = \sum_{x\in X}|G_x| = |G_x||X| = |G|.$$

Exercise 13.2. Use the previous idea to prove Theorem 13.1.

Let G act on a finite set X. Then G acts on $X\times X$ by

$$g\cdot(x,y) = (g\cdot x, g\cdot y). \tag{6.2}$$

The orbits of this action are called the **orbitals** of G on X. The **rank** of G on X is the number of orbitals.

Proposition 13.3. *Let G be a group that acts on a finite set X. The rank of G on X is*

$$\frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|^2.$$

Proof. The action (6.2) has $\mathrm{Fix}(g)\times\mathrm{Fix}(g)$ as fixed points, as

$$\begin{aligned} g\cdot(x,y) = (x,y) &\iff (g\cdot x, g\cdot y) = (x,y)\\ &\iff g\cdot x = x \text{ and } g\cdot y = y \iff (x,y)\in \mathrm{Fix}(g)\times\mathrm{Fix}(g). \end{aligned}$$

Now the claim follows from Cauchy–Frobenius–Burnside theorem. □

Definition 13.4. Let G acts on a finite set X. We say that G is **2-transitive** on X if given $x,y\in X$ with $x\neq y$ and $x_1,y_1\in X$ with $x_1\neq y_1$ there exists $g\in G$ such that $g\cdot x = y$ and $g\cdot x_1 = y_1$.

The symmetric group $\mathbb{S}_n$ acts 2-transitively on $\{1,\dots,n\}$.

Proposition 13.5. *If G is 2-transitive on X, then the rank of G on X is two.*

Proof. The set $\Delta = \{(x,x) : x\in X\}$ is an orbital. The complement $X\times X\setminus\Delta$ is another orbital: if $x,x_1,y,y_1\in X$ are such that $x\neq y$ and $x_1\neq y_1$, then there exists $g\in G$ such that $g\cdot x = y$ and $g\cdot x_1 = y_1$, so $g\cdot(x,y) = (x_1,y_1)$. □

Lecture 7

Cauchy–Frobenius–Burnside theorem is useful to find characters.

Proposition 13.6. *Let G be 2-transitive on X with character $\chi(g) = |\mathrm{Fix}(g)|$. Then $\chi - \chi_1$ is irreducible.*

Proof. In particular, G is transitive on X. Since the trivial character χ_1 is irreducible, $\langle \chi_1, \chi_1 \rangle = 1$. By Cauchy–Frobenius–Burnside, the rank of G on X is

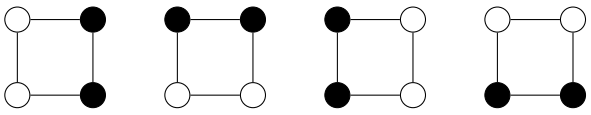
$$2 = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|^2 = \langle \chi, \chi \rangle.$$

Thus $\langle \chi - \chi_1, \chi - \chi_1 \rangle = \langle \chi, \chi \rangle - 1 - 1 + 1 = 1$. □

Example 13.7. The symmetric group $\mathbb{S}_n$ is 2-transitive on $\{1, \ldots, n\}$. The alternating group $\mathbb{A}_n$ is 2-transitive on $\{1, \ldots, n\}$ if $n \geq 4$. These groups then have an irreducible character χ given by $\chi(g) = |\mathrm{Fix}(g)| - 1$.

Example 13.8. Let p be a prime number and let $q = p^m$. Let V be the vector space of dimension m over the finite field of q elements. The group $G = \mathbf{GL}_2(q)$ acts 2-transitively on the set X of one-dimensional subspaces of V. In fact, if $\langle v \rangle \neq \langle v_1 \rangle$ and $\langle w \rangle \neq \langle w_1 \rangle$, then $\{v, v_1\}$ and $\{w, w_1\}$ are bases of V. The matrix g that corresponds to the linear map $v \mapsto w$, $v_1 \mapsto w_1$, is invertible. Thus $g \in \mathbf{GL}_2(q)$. The previous proposition produces the irreducible character $\chi(g) = |\mathrm{Fix}(g)| - 1$.

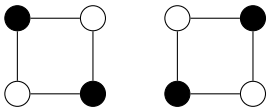
Example 13.9. In how many ways can we color (in black and white) the vertices of a square? We will count colorings up to symmetric. This means that, for example, the colorings



(7.1)

will be considered as equivalent. Let $G = \langle g \rangle$ the cyclic group of order four. Let X be the set of colorings of the square. Then $|X| = 16$.

Let G acts on X by anti-clockwise rotations of 90°. All the colorings of (7.1) belong to the same orbit. Another orbit of X is

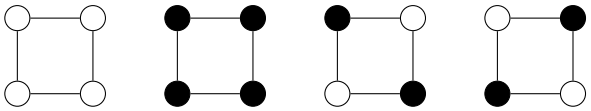


Cauchy–Frobenius–Burnside theorem states that there are

$$\frac{1}{|G|}\sum_{x\in G}|\mathrm{Fix}(x)|$$

orbits.

For each $x \in G = \{1, g, g^2, g^3\}$ we compute $\mathrm{Fix}(x)$. The identity fixes the 16 elements of X, both g and g^3 fix only two elements of X and g^2 fixes four elements of X. For example, the elements of X fixed by g^2 are



Thus X is union of

$$\frac{1}{|G|}\sum_{x\in G}|\mathrm{Fix}(x)| = \frac{1}{4}(16+2+4+2) = 6$$

orbits.

Exercise 13.10. In how many ways (up to symmetry) can you arrange eight non-attacking rooks on a chessboard? Symmetries are given by the dihedral group $\mathbb{D}_4$ of eight elements.

§14. Commuting probability

For a finite group G let $\mathrm{cp}(G)$ be the probability that two random elements of G commute. This number is also known as the **commutativity** of G. As an application of Cauchy–Frobenius–Burnside theorem we prove that $\mathrm{cp}(G) = k/|G|$, where k is the number of conjugacy classes of G. In fact, let

$$C = \{(x, y) \in G \times G : xy = yx\}.$$

We claim that

$$\mathrm{cp}(G) = \frac{|C|}{|G|^2} = \frac{k}{|G|}.$$

Let G act on G by conjugation. By Cauchy–Frobenius–Burnside theorem,

$$k = \frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}(g)| = \frac{1}{|G|}\sum_{g\in G}|C_G(g)| = \frac{|C|}{|G|},$$

as $\operatorname{Fix}(g) = \{x \in G : gxg^{-1} = x\} = C_G(g)$ and $\sum_{g\in G}|C_G(g)| = |C|$.

Theorem 14.1. *If G is a non-abelian finite group, then* $\operatorname{cp}(G) \le 5/8$.

Proof. Let $y_1, \dots, y_m$ the representatives of conjugacy classes of G of size ≥ 2. By the class equation,

$$|G| = |Z(G)| + \sum_{i=1}^{m}(G : C_G(y_i)) \ge |Z(G)| + 2m.$$

Thus $m \le (1/2)(|G| - |Z(G)|)$ and hence

$$k = |Z(G)| + m \le |Z(G)| + \frac{1}{2}(|G| - |Z(G)|) = \frac{1}{2}(|Z(G)| + |G|).$$

Since G is non-abelian, $G/Z(G)$ is not cyclic. In particular, $(G : Z(G)) \ge 4$. Therefore

$$k \le \frac{1}{2}(|Z(G)| + |G|) \le \frac{1}{2}\left(\frac{1}{4} + 1\right)|G|,$$

that is $k/|G| \le 5/8$. □

Exercise 14.2.

1) Prove that $\operatorname{cp}(Q_8) = 5/8$.
2) Prove that $\operatorname{cp}(\mathbb{A}_5) = 1/12$.

Exercise 14.3. Let G be a finite non-abelian group and p be the smallest prime number dividing $|G|$. Prove that $\operatorname{cp}(G) \le (p^2 + p - 1)/p^3$. Moreover, the equality holds if and only if $(G : Z(G)) = p^2$.

Exercise 14.4. Let G be a finite group and H be a subgroup of G.

1) $\operatorname{cp}(G) \le \operatorname{cp}(H)$.
2) If H is normal in G, then $\operatorname{cp}(G) \le \operatorname{cp}(G/H)\operatorname{cp}(H)$.

Degrees of irreducible characters give a lower bound:

Proposition 14.5. *If G is a finite group, then*

$$\operatorname{cp}(G) \ge \left(\frac{\sum_{\chi\in\operatorname{Irr}(G)}\chi(1)}{|G|}\right)^2.$$

Proof. Let k be the number of conjugacy classes of G. By Cauchy–Schwarz inequality,

$$\left(\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\right)^2 \le \left(\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)^2\right)\left(\sum_{\chi\in\mathrm{Irr}(G)}1\right)^2 = \left(\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)^2\right)k = |G|k.$$

From this the claim follows. □

Using basic facts about irreducible characters, we obtain a generalization of Theorem 14.1.

Theorem 14.6. *Let G be a finite group with $\mathrm{cp}(G) > 1/4$. Then*

$$|[G,G]| \le 3/(4\,\mathrm{cp}(G) - 1).$$

Proof. For $n \in \mathbb{Z}_{>0}$, let ρ_n be the number of irreducible characters of degree n. Then $k(G) = \sum_{i\ge1}\rho_i$ and $|G| = \sum_{i\ge1} i^2\rho_i$. It follows that

$$|G| - \rho_1 = \sum_{i\ge2} i^2\rho_i \ge 4\sum_{i\ge2}\rho_i = 4(k(G) - \rho_1) = 4(|G|\,\mathrm{cp}(G) - \rho_1).$$

Since $\rho_1 = (G : [G,G])$,

$$\mathrm{cp}(G) \le \frac{1}{4} + \frac{3}{4}\frac{\rho_1}{|G|} = \frac{1}{4} + \frac{3}{4|[G,G]|}.$$ □

Exercise 14.7. Use Theorem 14.6 to prove Theorem 14.1.

Theorem 14.6 can also be used to prove similar statements.

Exercise 14.8. Let G be a finite group. Prove the following statements:

1) If $\mathrm{cp}(G) > 1/2$, then G is nilpotent.
2) If $\mathrm{cp}(G) > 21/80$, then G is solvable.

In the following exercise we will discuss the notion of isoclinic groups. We first need a preliminary result:

Exercise 14.9. Let G be a group. Prove that the commutator map

$$c_G : G/Z(G)\times G/Z(G) \to [G,G], \quad c_G(xZ(G), yZ(G)) = [x,y],$$

is well-defined.

The idea is that two groups are said to be isoclinic if their commutator functions are somewhat equal.

Exercise 14.10. Let G and H be groups. A pair (σ,τ) of maps is an **isoclinism** between G and H if $\sigma\colon G/Z(G)\to H/Z(H)$ and $\tau\colon [G,G]\to[H,H]$ are group isomorphisms and the diagram

$$\begin{array}{ccc} G/Z(G)\times G/Z(G) & \xrightarrow{\sigma\times\tau} & H/Z(H)\times H/Z(H) \\ {\scriptstyle c_G}\downarrow & & \downarrow{\scriptstyle c_H} \\ [G,G] & \xrightarrow[\tau]{} & [H,H] \end{array} \tag{7.2}$$

commutes. We write $G\sim H$ when there exists an isoclinism between G and H.

Prove the following statements:

1) If $G\simeq H$, then $G\sim H$.
2) If $G\sim H$, then $\mathrm{cp}(G)=\mathrm{cp}(H)$.

Exercise 14.11. Let S be a non-abelian simple group and G be a group such that $G\sim S$. Prove that $G\simeq S\times A$ for some abelian group A.

Exercise 14.12. Let H be a subgroup of G. If $G=HZ(G)$, then $G\sim H$. Conversely, if $G\sim H$ and H is finite, then $G=HZ(G)$.

Exercise 14.13.

The following theorem appeared in 1970, as a problem in the volume 13 of the *Canadian Math. Bulletin*. The solution appeared in 1973. Iván Sadosfchi Costa found the proof we present here.

Theorem 14.14 (Dixon). *If G is a finite simple group, then* $\mathrm{cp}(G)\leq 1/12$.

Proof. We first assume that the commuting probability of G is $>1/12$. Since G is a non-abelian simple group, the identity is the only central element. Let us assume first that there is a conjugacy class of G of size m, where m is such that $1<m\leq 12$. Then G is a transitive subgroup of $\mathbb{S}_m$. For these groups the problem is easy: we show that there are no non-abelian simple groups that act transitively on sets of size $m\in\{2,\dots,12\}$ with commuting probability $>1/12$. To do this, we list these transitive groups and their commuting probabilities and verify that all commuting probabilities are $\leq 1/12$:

```
gap> l := AllTransitiveGroups(NrMovedPoints, [2..12], \\
> IsAbelian, false, IsSimple, true);;
[ A5, L(6) = PSL(2,5) = A_5(6), A6,
  L(7) = L(3,2), A7, L(8)=PSL(2,7), A8,
  L(9)=PSL(2,8), A9, A_5(10), L(10)=PSL(2,9),
  A10, L(11)=PSL(2,11)(11), M(11), A11, A_5(12),
  L(2,11), M_11(12), M(12), A12 ]
gap> List(l, CommutingProbability);
[ 1/12, 1/12, 7/360, 1/28, 1/280, 1/28, 1/1440,
  1/56, 1/10080, 1/12, 7/360, 1/75600, 2/165,
  1/792, 31/19958400, 1/12, 2/165, 1/792, 1/6336,
  43/239500800 ]
gap> ForAny(l, x->CommutingProbability(x)>1/12);
false
```

Now assume that all non-trivial conjugacy class of G have at least 13 elements. Then the class equation implies that

$$|G| \geq \frac{13}{12}|G| - 12,$$

and therefore $|G| \leq 144$. Thus one needs to check what happens with groups of order ≤ 144. But we know that the only non-abelian simple group of size ≤ 144 is the alternating simple group $\mathbb{A}_5$.

```
gap> AllGroups(Size, [2..144], \\
> IsAbelian, false, \\
> IsSimple, true);
[ Alt( [ 1 .. 5 ] ) ]
```

□

The alternating group $\mathbb{A}_5$ is important in this setting:

Theorem 14.15 (Guralnick–Robinson). *If G is a finite non-solvable group such that $\mathrm{cp}(G) > 3/40$, then $G \simeq \mathbb{A}_5 \times T$ for some abelian group T and $\mathrm{cp}(G) = 1/12$.*

The proof appears in [15].

Results on probability of commuting elements generalize in other directions. In [39, 40, 41, 42], Thompson proved the following result:

Theorem 14.16 (Thompson). *If G is a finite group such that every pair of elements of G generate a solvable group, then G is solvable.*

The proof uses the classification of finite simple groups (CFSG). A simpler proof independent of the CFSG appears in [10].

There is a probabilistic version of Thompson's theorem:

Theorem 14.17 (Guralnick–Wilson). *Let G be a finite group.*

1) *If the probability that two random elements of G generate a solvable group is $> 11/30$, then G is solvable.*
2) *If the probability that two random elements of G generate a nilpotent group is $> 1/2$, then G is nilpotent.*
3) *If the probability that two random elements of G generate a group of odd order is $> 11/30$, then G has odd order.*

The proof uses the CFSG and appears in [16].

§15. Jordan's theorem and applications

We now follow [35] to present other applications.

Theorem 15.1 (Jordan). *Let G be a non-trivial finite group. If G acts transitively on a finite set X and $|X| > 1$, then there exists $g \in G$ with no fixed points.*

Proof. Cauchy–Frobenius–Burnside theorem implies that

$$1 = \frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix}(g)| = \frac{1}{|G|}\left(|X| + \sum_{g\neq 1}|\operatorname{Fix}(g)|\right).$$

If every $g \in G \setminus \{1\}$ contains at least one fixed-point, then

$$1 = \frac{1}{|G|}\left(|X| + \sum_{g\neq 1}|\operatorname{Fix}(g)|\right) \geq \frac{1}{|G|}(|X| + |G| - 1) = 1 + \frac{|X|-1}{|G|}$$

and thus $|X| \leq 1$, a contradiction. □

Corollary 15.2. *Let G be a finite group and H be a proper subgroup of G. Then $G \neq \cup_{g\in G} gHg^{-1}$.*

Proof. The group G acts transitively by left multiplication on $X = G/H$. The stabilizer of xH is

$$G_{xH} = \{g \in G : gxH = xH\} = xHx^{-1}.$$

Since $H \neq G$, it follows thast $|X| = |G/H| > 1$. Jordan's theorem now implies that there exists $g \in G$ with no fixed-points, that is there is an element $g \in G$ such that $g \notin \cup_{x\in G} xHx^{-1}$. □

Let G be a finite group. We say that the conjugacy classes C and D **commute** if there exist $c \in C$ and $d \in D$ such that $[c, d] = 1$. Note that C and D commute si y sólo for all $c \in C$ there exists $d \in D$ such that $[c, d] = 1$.

Corollary 15.3 (Wildon). *Let G be a finite group and C be a conjugacy classes of G. Then $|C| = 1$ if and only if C commute with every conjugacy class of G.*

Proof. We prove $\Longleftarrow$. Assume that C commute with every conjugacy class of G. Let $c \in C$ and $H = C_G(c)$. Then $H \cap D \neq \emptyset$ for every conjugacy class D. We claim that $G = \cup_{g\in G} gHg^{-1}$. In fact, let $x \in G$. Then $x \in D$ for some conjugacy class D. Let $h \in H \cap D$. There exists $y \in G$ such that $h = yxy^{-1}$, that is $x = y^{-1}hy \in \cup_{g\in G} gHg^{-1}$. By Jordan's theorem, $H = G$. Thus c is central and hence $C = \{c\}$.

We now prove $\Longrightarrow$. If $C = \{c\}$, then $c \in Z(G)$ and C commute with every conjugacy class of G. □

With the CFSG one proves a result similar to that of Jordan.

Theorem 15.4 (Fein–Kantor–Schacher). *Let G be a non-trivial finite group. If G acts transitively on a finite set X and $|X| > 1$, then there exist a prime number p and an element $g \in G$ with no fixed-points with order a power of p.*

The proof appears in [8].

§16. Derangements: Cameron–Cohen theorem

Let G be a finite group that acts faithfully and transitively on a finite set X, say $G \le \mathbb{S}_n$, where $X = \{1, 2, \dots, n\}$. Let G_0 the set of elements $g \in G$ with no fixed-ponts, that is $g(x) \ne x$ for all $x \in X$. Such permutations are known as **derangements**. Let $c_0 = |G_0|/|G|$.

Theorem 16.1 (Cameron–Cohen). *If G is a subgroup of $\mathbb{S}_n$ that acts transitively on $\{1, \dots, n\}$, then $c_0 \ge \frac{1}{n}$.*

Proof. Let $X = \{1, \dots, n\}$. By definition, the rank of G isthe number of orbitals of G on X. It follows that the rank is ≥ 2, as $X \times X$ decomposes as

$$X \times X = \Delta \cup ((X \times X) \setminus \Delta)$$

Let $\chi(g) = |\mathrm{Fix}(g)|$ and $G_0 = \{g \in G : \chi(g) = 0\}$. If $g \notin G_0$, then $1 \le \chi(g) \le n$. Since $(\chi(g) - 1)(\chi(g) - n) \le 0$,

$$\frac{1}{|G|} \sum_{g \in G \setminus G_0} (\chi(g) - 1)(\chi(g) - n) \le 0.$$

On the one hand,

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} &(\chi(g) - 1)(\chi(g) - n) \\ &= \frac{1}{|G|} \left\{ \sum_{g \in G_0} + \sum_{g \in G \setminus G_0} \right\} (\chi(g) - 1)(\chi(g) - n) \\ &\le n \frac{|G_0|}{|G|} = n c_0. \end{aligned}$$

On the other hand, since the rank of G is ≥ 2,

$$2 - \frac{n+1}{|G|} \sum_{g \in G} \chi(g) + n \le \frac{1}{|G|} \sum_{g \in G} (\chi(g) - 1)(\chi(g) - n) \le n c_0. \tag{7.3}$$

Since G is transitive on X, Cauchy–Frobenius–Burnside theorem implies that $\sum_{g \in G} \chi(g) = |G|$. Thus $2 - (n+1) + n \le n c_0$ and hence $1/n \le c_0$. □

Cameron–Cohen theorem contains another claim: If n is not the power of a prime number, then $c_0 > 1/n$. The proof uses Frobenius' theorem.

With the CFSG the bound in Cameron–Cohen theorem can be improved:

Theorem 16.2 (Guralnick–Wan). *Let G be a finite transitive group of degree $n \ge 2$. If n is not a power of a prime number and $G \ne \mathbb{S}_n$ for $n \in \{2, 4, 5\}$, then $c_0 \ge 2/n$.*

The proof appears in [13] and uses the classification of finite 2-transitive groups, which depends on the CFSG.

Lecture 8

§17. Brauer–Fowler theorem

Let $\rho\colon G \to \mathbf{GL}(V)$ be a representation with character χ. The $\mathbb{C}[G]$-module $V \otimes V$ has character χ^2. Let $\{v_1, \ldots, v_n\}$ be a basis of V and

$$T\colon V \to V, \quad v_i \otimes v_j \mapsto v_j \otimes v_i.$$

It is an exercise to check that $T(v \otimes w) = w \otimes v$ for all $v, w \in V$. It follows that T does not depend on the chosen basis. Note that T is a homomorphism of $\mathbb{C}[G]$-modules, as

$$T(g \cdot (v \otimes w)) = T((g \cdot v) \otimes (g \cdot w)) = (g \cdot w) \otimes (g \cdot v) = g \cdot T(w \otimes v)$$

for all $g \in G$ y $v, w \in V$. In particular, the **symmetric part**

$$S(V \otimes V) = \{x \in V \otimes V : T(x) = x\}$$

and the **antisymmetric** part

$$A(V \otimes V) = \{x \in V \otimes V : T(x) = -x\}$$

of $V \otimes V$ are both $\mathbb{C}[G]$-submodules of $V \otimes V$. The terminology is motivated by the following fact:

$$V \otimes V = S(V \otimes V) \oplus A(V \otimes V).$$

In fact, $S(V \otimes V) \cap A(V \otimes V) = \{0\}$, as $x \in S(V \otimes V) \cap A(V \otimes V)$ implies $x = T(x)$ and $x = -T(x)$. Hence $x = 0$. Moreover, $V \otimes V = S(V \otimes V) + A(V \otimes V)$, as every $x \in V \otimes V$ can be written as

$$x = \frac{1}{2}(x + T(x)) + \frac{1}{2}(x - T(x))$$

with $\frac{1}{2}(x + T(x)) \in S(V \otimes V)$ and $\frac{1}{2}(x - T(x)) \in A(V \otimes V)$.

We claim that $\{v_i \otimes v_j + v_j \otimes v_i : 1 \leq i, j \leq n\}$ is a basis of $S(V \otimes V)$ and that

$$\{v_i \otimes v_j - v_j \otimes v_i : 1 \leq i < j \leq n\}$$

is a basis of $A(V \otimes V)$. Since both sets are linearly independent,

$$\dim S(V \otimes V) \geq n(n+1)/2 \text{ and } \dim A(V \otimes V) \geq n(n-1)/2.$$

Moreover,

$$n^2 = \dim(V \otimes V) = \dim S(V \otimes V) + \dim A(V \otimes V),$$

so it follows that $\dim S(V \otimes V) = n(n+1)/2$ and $\dim A(V \otimes V) = n(n-1)/2$.

Proposition 17.1. *Let G be a finite group and V be a finite-dimensional $\mathbb{C}[G]$-module with character χ. If $S(V \otimes V)$ has character χ_S and $A(V \otimes V)$ has character χ_A, then*

$$\chi_S(g) = \frac{1}{2}(\chi^2(g) + \chi(g^2)) \qquad \text{and} \qquad \chi_A(g) = \frac{1}{2}(\chi^2(g) - \chi(g^2)).$$

Proof. Let $g \in G$ and $\rho\colon G \to \mathbf{GL}(V)$ be the representation associated with V, that is $\rho(g)(v) = \rho_g(v) = g \cdot v$. Since ρ_g is diagonalizable, let $\{e_1, \ldots, e_n\}$ be a basis of eigenvectors of ρ_g, say $g \cdot e_i = \lambda_i e_i$ with $\lambda_i \in \mathbb{C}$ for all $i \in \{1, \ldots, n\}$. In particular, $\chi(g) = \sum_{i=1}^n \lambda_i$.

Since $\{e_i \otimes e_j - e_j \otimes e_i : 1 \leq i < j \leq n\}$ is basis of $A(V \otimes V)$ and

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

it follows that $\chi_A(g) = \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j$. On the other hand, $g^2 \cdot e_i = \lambda_i^2 e_i$ for all i, $\chi(g^2) = \sum_{i=1}^n \lambda_i^2$. Thus

$$\chi^2(g) = \chi(g)^2 = \sum_{i=1}^n \sum_{j=1}^n \lambda_i \lambda_j = 2 \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j + \sum_{i=1}^n \lambda_i^2 = 2\chi_A(g) + \chi(g^2).$$

Since $V \otimes V = S(V \otimes V) \oplus A(V \otimes V)$, it follows that $\chi^2(g) = \chi_S(g) + \chi_A(g)$, that is $\chi_S(g) = \frac{1}{2}(\chi^2(g) + \chi(g^2))$. □

An **involution** of a group is an element $x \neq 1$ such that $x^2 = 1$. It is possible to use the character table to count the number of involutions.

Proposition 17.2. *If G is a finite group with t involutions, then*

$$1 + t = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi(1).$$

Proof. Assume that $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$, where χ_1 is the trivial character of G. For $x \in G$ let

$$\theta(x) = |\{y \in G : y^2 = x\}|.$$

Since θ is a class function, θ is a linear combination of the χ_j's, say

$$\theta = \sum_{\chi \in \mathrm{Irr}(G)} \langle \theta, \chi \rangle \chi.$$

We compute:

$$\begin{aligned}\langle \chi_S - \chi_A, \chi_1 \rangle &= \frac{1}{|G|} \sum_{g \in G} \chi(g^2) \\ &= \frac{1}{|G|} \sum_{x \in G} \sum_{\substack{g \in G \\ g^2 = x}} \chi(g^2) = \frac{1}{|G|} \sum_{x \in G} \theta(x)\chi(x) = \langle \theta, \chi \rangle.\end{aligned}$$

Thus $\theta(x) = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi$. Now the claim follows after evaluating this expression in $x = 1$. □

Before proving the Brauer-Fowler theorem we need a lemma. We will use the Cauchy–Schwartz inequality:

$$x_1, \ldots, x_n \in \mathbb{R} \implies \sum x_i^2 \geq \frac{1}{n} (\sum x_i)^2.$$

Lemma 17.3. *Let G be a finite group with k conjugacy classes. If t is the number of involutions of G, then $t^2 \leq (k-1)(|G|-1)$.*

Proof. Assume that $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$, where χ_1 is the trivial character of G. If $\chi \in \mathrm{Irr}(G)$, then

$$\langle \chi^2, \chi_1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)\chi(g) = \langle \chi, \overline{\chi} \rangle = \begin{cases} 1 & \text{if } \chi = \overline{\chi}, \\ 0 & \text{otherwise.} \end{cases}$$

Since $\chi^2 = \chi_S + \chi_A$, if $\langle \chi^2, \chi_1 \rangle = 1$, then the trivial character either is part of χ_S or χ_A, but not both. Thus

$$\langle \chi_S - \chi_A, \chi_1 \rangle \in \{-1, 1, 0\}.$$

We claim that $t \leq \sum_{i=2}^{k} \chi_i(1)$. In fact, since $|\langle \chi_S - \chi_A, \chi_1 \rangle| \leq 1$,

$$\begin{aligned}1 + t = \theta(1) &= \left| \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi(1) \right| \\ &\leq \sum_{\chi \in \mathrm{Irr}(G)} |\langle \chi_S - \chi_A, \chi_1 \rangle| \chi(1) \leq \sum_{\chi \in \mathrm{Irr}(G)} \chi(1).\end{aligned}$$

It follows that $t \leq \sum_{i=2}^{k} \chi_i(1)$. By the Cauchy–Schwartz inequality,

$$t^2 \leq \left(\sum_{i=2}^{k} \chi_i(1) \right)^2 \leq (k-1) \sum_{i=2}^{k} \chi(1)^2 = (k-1)(|G|-1). \qquad \square$$

Now we prove the Brauer–Fowler theorem.

Theorem 17.4 (Brauer–Fowler). *Let G be a finite simple group and x be an involution of G. If $|C_G(x)| = n$, then $|G| \leq (n^2)!$*

Proof. We first assume the existence of a proper subgroup H of G such that

$$(G : H) \leq n^2.$$

The group G acts on G/H by left multiplication, so there is a group homomorpihsm $\rho\colon G \to \mathbb{S}_{n^2}$. Since G is simple, either $\ker\rho = \{1\}$ or $\ker\rho = G$. If $\ker\rho = G$, then $\rho(g)(yH) = yH$ for all $g \in G$ and $y \in G$. Hence $g \in H$, a contradiction. Therefore ρ is injective and hence G is isomorphic to a subgroup of $\mathbb{S}_{n^2}$. In particular, $|G|$ divides $(n^2)!$.

Let $m = (|G|-1)/t$. Since $|C_G(x)| = n$, the group G has at least $|G|/n$ involutions (because the conjugacy class of x has size $|G|/n$ and all its elements are involutions), that is $t \geq |G|/n$. Hence $m = (|G|-1)/t < n$. It is enough then to show that G contains a subgroup of index $\leq m^2$.

Let $C_1, \dots, C_k$ be the conjugacy classes of G, where $C_1 = \{1\}$. Since G is simple, $|C_i| > 1$ for all $i \in \{2, \dots, k\}$. By the previous lemma,

$$|G| - 1 \leq \frac{(k-1)(|G|-1)^2}{t^2} \iff t^2 \leq (k-1)(|G|-1).$$

If $|C_i| > m$ for all $i \in \{2, \dots, k\}$, then, since

$$|G| - 1 \leq \frac{(k-1)(|G|-1)^2}{t^2} = (k-1)m^2,$$

it follows that

$$|G| - 1 = \sum_{i=2}^{k} |C_i| > (k-1)m^2,$$

a contradiction. Thus there exists a conjugacy class C of G such that $|C| \leq m^2$. If $g \in C$, then $C_G(g)$ is a subgroup of G of index $|C| \leq m^2$. □

The bound of the Brauer–Fowler theorem is not important. What matters is the following consequence:

Corollary 17.5. *Let $n \geq 1$ be an integer. There are at most finitely many finite simple groups with an involution with a centralizer of order n.*

As an exercise, a simple applications:

Exercise 17.6. If G is a finite simple group and x is an involution with centralizer of order two, then $G \simeq \mathbb{Z}/2$.

§18. The correspondence theorem

Let N be a normal subgroup of G and $\pi\colon G \to G/N$, $g \mapsto gN$, be the canonical map. If $\widetilde{\rho}\colon G/N \to \mathbf{GL}(V)$ is a representation of G/N with character $\widetilde{\chi}$, the composition $\rho = \widetilde{\rho}\pi\colon G \to \mathbf{GL}(V)$, $\rho(g) = \widetilde{\rho}(gN)$, is a representation of G. Thus

$$\chi(g) = \operatorname{trace}\rho_g = \operatorname{trace}(\widetilde{\chi}(gN)) = \widetilde{\chi}(gN).$$

In particular, $\chi(1) = \widetilde{\chi}(1)$. The character χ is the **lifting** to G of the character $\widetilde{\chi}$ of G/N.

Proposition 18.1. *If $\chi \in \operatorname{Irr}(G)$, then*

$$\ker\chi = \{g \in G : \chi(g) = \chi(1)\}$$

is a normal subgroup of G.

Proof. Let $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$ be a representation with character χ. Then $\ker\rho \subseteq \ker\chi$, as $\rho_g = \mathrm{id}$ implies $\chi(g) = \operatorname{trace}(\rho_g) = n = \chi(1)$. We claim that $\ker\chi \subseteq \ker\rho$. If $g \in G$ is such that $\chi(g) = \chi(1)$, since ρ_g is diagonalizable, there exist eigenvalues $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$n = \chi(1) = \chi(g) = \sum_{i=1}^{n} \lambda_i.$$

Since each λ_i is a root of one, $\lambda_1 = \cdots = \lambda_n = 1$. Hence $\rho_g = \mathrm{id}$. □

If χ is an irreducible character, the subgroup $\ker\chi$ is the **kernel** of χ.

Theorem 18.2 (Correspondence theorem). *Let N be a normal subgroup of a finite group G. There exists a bijective correspondence*

$$\operatorname{Char}(G/N) \longleftrightarrow \{\chi \in \operatorname{Char}(G) : N \subseteq \ker\chi\}$$

that maps irreducible characters to irreducible characters.

Proof. If $\widetilde{\chi} \in \operatorname{Char}(G/N)$, let χ be the lifting of $\widetilde{\chi}$ to G. If $n \in N$, then

$$\chi(n) = \widetilde{\chi}(nN) = \widetilde{\chi}(N) = \chi(1)$$

and thus $N \subseteq \ker\chi$.

If $\chi \in \operatorname{Char}(G)$ is such that $N \subseteq \ker\chi$, let $\rho\colon G \to \mathbf{GL}(V)$ be a representationn with character χ. Let $\widetilde{\rho}\colon G/N \to \mathbf{GL}(V)$, $gN \mapsto \rho(g)$. We claim that $\widetilde{\rho}$ is well-defined:

$$gN = hN \iff h^{-1}g \in N \iff \rho(h^{-1}g) = \mathrm{id} \iff \rho(h) = \rho(g).$$

Moreover, $\widetilde{\rho}$ is a representation, as

$$\widetilde{\rho}((gN)(hN)) = \widetilde{\rho}(ghN) = \rho(gh) = \rho(g)\rho(h) = \widetilde{\rho}(gN)\widetilde{\rho}(hN).$$

If $\widetilde{\chi}$ is the character of $\widetilde{\rho}$, then $\widetilde{\chi}(gN) = \chi(g)$.

We now prove that χ is irreducible if and only if $\widetilde{\chi}$ is irreducible. If U is a subspace of V, then

$$\begin{aligned} U \text{ is invariant} &\iff \rho(g)(U) \subseteq U \text{ for all } g \in U \\ &\iff \widetilde{\rho}(gN)(U) \subseteq U \text{ for all } g \in U. \end{aligned}$$

Thus

$$\begin{aligned} \chi \text{ is irreducible} &\iff \rho \text{ is irreducible} \\ &\iff \widetilde{\rho} \text{ is irreducible} \iff \widetilde{\chi} \text{ is irreducible .} \end{aligned}$$ □

Example 18.3. Let $G = \mathbb{S}_4$ and $N = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. We know that N is normal in G and that $G/N = \langle a, b\rangle \simeq \mathbb{S}_3$, where $a = (123)N$ and $b = (12)N$. The character table of G/N is

	1	$(12)N$	$(123)N$
$\widetilde{\chi}_1$	1	1	1
$\widetilde{\chi}_2$	1	−1	1
$\widetilde{\chi}_3$	2	0	−1

For each $i \in \{1,2,3\}$ we compute the lifting χ_i to G of the character $\widetilde{\chi}_i$ of G/N. Since $(12)(34) \in N$ and $(13)(1234) = (12)(34) \in N$,

$$\chi((12)(34)) = \widetilde{\chi}(N), \quad \chi((1234)) = \widetilde{\chi}((13)N) = \widetilde{\chi}((12)N).$$

Since the characters $\widetilde{\chi}_i$ are irreducibles, the liftings χ_i are also irreducibles. With this process we obtain the following irreducible characters of G:

	1	(12)	(123)	$(12)(34)$	(1234)
χ_1	1	1	1	1	1
χ_2	1	−1	1	1	-1
χ_3	2	0	−1	2	0

The character table of a group can be used to find the lattice of normal subgroups. In particular, the character table detect simple groups.

Lemma 18.4. *Let G be a finite group and let $g, h \in G$. Then g and h are conjugate if and only if $\chi(g) = \chi(h)$ for all $\chi \in \mathrm{Char}(G)$.*

Proof. If g and h are conjugate, then $\chi(g) = \chi(h)$, as characters are class functions of G. Conversely, if $\chi(g) = \chi(h)$ for all $\chi \in \mathrm{Char}(G)$, then $f(g) = f(h)$ for all class function f of G, as characters G generate the space of class functions of G. In particular, $\delta(g) = \delta(h)$, where

$$\delta(x) = \begin{cases} 1 & \text{if } x \text{ and } g \text{ are conjugate,} \\ 0 & \text{otherwise.} \end{cases}$$

This implies that g and h are conjugate. □

As a consequence, we get that

$$\bigcap_{\chi \in \mathrm{Irr}(G)} \ker \chi = \{1\}. \tag{8.1}$$

Indeed, if $g \in \ker \chi$ for all $\chi \in \mathrm{Irr}(G)$, then $g = 1$ since the lemma implies that g and 1 are conjugate because $\chi(g) = \chi(1)$ for all $\chi \in \mathrm{Irr}(G)$.

Proposition 18.5. *Let G be a finite group. If N is a normal subgroup of G, then there exist characters $\chi_1, \dots, \chi_k \in \mathrm{Irr}(G)$ such that*

$$N = \bigcap_{i=1}^{k} \ker \chi_i.$$

Proof. Apply the previous remark to the group G/N to obtain that

$$\bigcap_{\widetilde{\chi} \in \mathrm{Irr}(G/N)} \ker \widetilde{\chi} = \{N\}.$$

Assume that $\mathrm{Irr}(G/N) = \{\widetilde{\chi}_1, \dots, \widetilde{\chi}_k\}$. We lift the irreducible characters of G/N to G to obtain (some) irreducible characters $\chi_1, \dots, \chi_k$ of G such that $N \subseteq \ker \chi_1 \cap \cdots \cap \ker \chi_k$. If $g \in \ker \chi_i$ for all $i \in \{1, \dots, k\}$, then

$$\widetilde{\chi}_i(N) = \chi_i(1) = \chi_i(g) = \widetilde{\chi}_i(gN)$$

for all $i \in \{1, \dots, k\}$. This implies that

$$gN \in \bigcap_{i=1}^{k} \ker \widetilde{\chi}_i = \{N\},$$

that is $g \in N$. □

Recall that a non-trivial group is **simple** if it contains no non-trivial normal proper subgroups. Examples of simple groups are cyclic groups of prime order and the alternating groups $\mathbb{A}_n$ for $n \geq 5$. As a corollary of Proposition 18.5, we can use the character table to detect simple groups.

Proposition 18.6. *Let G be a finite group. Then G is not simple if and only if there exists a non-trivial irreducible character χ such that $\chi(g) = \chi(1)$ for some $g \in G \setminus \{1\}$.*

Proof. If G is not simple, there exists a normal subgroup N of G such that $N \neq G$ and $N \neq \{1\}$. By Proposition 18.5, there exist characters $\chi_1, \dots, \chi_k \in \mathrm{Irr}(G)$ such that $N = \ker \chi_1 \cap \cdots \cap \ker \chi_k$. In particular, there exists a non-trivial character χ_i such that $\ker \chi_i \neq \{1\}$. Thus there exists $g \in G \setminus \{1\}$ such that $\chi_i(g) = \chi_i(1)$.

Assume now that there exists a non-trivial character χ such that $\chi(g) = \chi(1)$ for some $g \in G \setminus \{1\}$. In particular, $g \in \ker \chi$ and hence $\ker \chi \neq \{1\}$. Since χ is non-trivial, $\ker \chi \neq G$. Thus $\ker \chi$ is a proper non-trivial normal subgroup of G. □

Example 18.7. If there exists a group G with a character table of the form

χ_1	1	1	1	1	1	1
χ_2	1	1	1	-1	1	-1
χ_3	1	1	1	1	-1	-1
χ_4	1	1	1	-1	-1	1
χ_5	2	-2	2	0	0	0
χ_6	8	0	-1	0	0	0

then G cannot be simple. Note that such a group G would have order $\sum_{i=1}^{6} \chi_i(1)^2 = 72$. Mathieu's group M_9 has precisely this character table!

Example 18.8. Let $\alpha = \frac{1}{2}(-1+\sqrt{7}i)$. If there exists a group G with a character table of the form

χ_1	1	1	1	1	1	1
χ_2	7	-1	-1	1	0	0
χ_3	8	0	0	-1	1	1
χ_4	3	-1	1	0	α	$\overline{\alpha}$
χ_5	3	-1	1	0	$\overline{\alpha}$	α
χ_6	6	2	0	0	0	0

then G is simple. Note that such a group G would have order $\sum_{i=1}^{6} \chi_i(1)^2 = 168$. The group

$$\mathbf{PSL}_2(7) = \mathbf{SL}_2(7)/Z(\mathbf{SL}_2(7))$$

is a simple group that has precisely this character table!

§19. Frobenius's reciprocity

We now present a very quick version of Frobenius' reciprocity theorem. We first define restriction of class functions.

Definition 19.1. Let G be a finite group and $f\colon G \to \mathbb{C}$ be a map. For a subgroup H of G, the **restriction** of f to H is the map $= \mathrm{Res}^G_H = f|_H : H \to \mathbb{C}$, $h \mapsto f(h)$.

Exercise 19.2. Let G be a finite group. Prove that the map $\mathrm{Res}^G_H\colon \mathrm{cf}(G) \to \mathrm{cf}(H)$, $f \mapsto \mathrm{Res}^G_H(f)$, is a well-defined linear map.

We now define induction. Let G be a finite group and H be a subgroup of G. If $f\colon G \to \mathbb{C}$ is a map, then

$$\dot{f}(x) = \begin{cases} f(x) & \text{if } x \in H, \\ 0 & \text{otherwise.} \end{cases}$$

It is an exercise to prove that the map $f \mapsto \dot{f}$ is linear.

Definition 19.3. Let G be a finite group and $f\colon G \to \mathbb{C}$ be a map. For a subgroup H of G, the **induction** of f to H is the map

$$g \mapsto \operatorname{Ind}_H^G f(g) = \frac{1}{|H|} \sum_{x \in G} \dot{f}(x^{-1}gx).$$

Exercise 19.4. Let G be a finite group. Prove that the map $\operatorname{Ind}_H^G\colon \operatorname{cf}(H) \to \operatorname{cf}(G)$, $f \mapsto \operatorname{Ind}_H^G(f)$, is a well-defined linear map.

Theorem 19.5 (Frobenius' reciprocity theorem). *Let G be a finite group and H be a subgroup of G. If $a \in \operatorname{cf}(H)$ and $b \in \operatorname{cf}(G)$, then*

$$\langle \operatorname{Ind}_H^G a, b\rangle = \langle a, \operatorname{Res}_H^G b\rangle.$$

Proof. It follows from a direct calculation:

$$\langle \operatorname{Ind}_H^G a, b\rangle = \frac{1}{|G|} \sum_{x \in G} \operatorname{Ind}_H^G a(x)\overline{b(x)} = \frac{1}{|G|}\frac{1}{|H|} \sum_{x,y \in G} \dot{f}(y^{-1}xy)\overline{b(x)}. \tag{8.2}$$

Since

$$\dot{a}(y^{-1}xy) \neq 0 \Longleftrightarrow y^{-1}xy \in H \Longleftrightarrow x \in yHy^{-1},$$

setting $h = y^{-1}xy$ we can write (8.2) as

$$\begin{aligned}\langle \operatorname{Ind}_H^G a, b\rangle &= \frac{1}{|G|}\frac{1}{|H|} \sum_{x \in G} \sum_{h \in H} a(h)\overline{b(xhx^{-1})} \\ &= \frac{1}{|G|}\frac{1}{|H|} \sum_{x \in G} \sum_{h \in H} a(h)\overline{b(h)} \\ &= \frac{1}{|G|} \sum_{x \in G} \langle a, \operatorname{Res}_H^G b\rangle.\end{aligned}$$

From this the claim follows. □

§20. Frobenius' groups

If p is a prime number, then the units $(\mathbb{Z}/p)^\times$ of $\mathbb{Z}/p$ form a multiplicative group. Moreover, $(\mathbb{Z}/p)^\times$ is cyclic of order $p-1$.

Let p and q be prime numbers such that q divides $p-1$. Let

$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} : x \in (\mathbb{Z}/p)^\times, y \in \mathbb{Z}/p \right\}.$$

Then G is a group with the usual matrix multiplication and $|G| = p(p-1)$. Let $z \in \mathbb{Z}$ be an element of order q modulo p and let

$$a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} z & 1 \\ 0 & 1 \end{pmatrix}, \quad H = \langle a, b \rangle.$$

A direct calculation shows that

$$a^p = b^q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad bab^{-1} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} = a^z. \tag{8.3}$$

Every element of H is of the form $a^i b^j$ for $i \in \{0, \dots, p-1\}$ and $j \in \{0, \dots, q-1\}$. Thus $|H| = pq$. Using (8.3) we can compute the multiplication table of G.

Exercise 20.1. Let p and q be prime numbers such that q divides $p-1$. Let $u, v \in \mathbb{Z}$ be elements of order q modulo p. Prove that

$$\langle a, b : a^p = b^q = 1, bab = a^u \rangle \simeq \langle a, b : a^p = b^q = 1, bab = a^v \rangle.$$

The group

$$F_{p,q} = \langle a, b : a^p = b^q = 1, bab = a^u \rangle,$$

where $u \in \mathbb{Z}$ has order q modulo p, is a particular case of a *Frobenius group*.

Proposition 20.2. *Let p and q be prime numbers such that $p > q$. Let G be a group of order pq. Then either G is abelian or q divides $p-1$ and $G \simeq F_{p,q}$.*

Proof. Assume that G is not abelian. By Sylow's theorems, q divides $p-1$ and there exists a unique Sylow p-subgroup P of G. Let $a, b \in G$ be such that $P = \langle a \rangle \simeq \mathbb{Z}/p$ and $G/P = \langle bP \rangle \simeq \mathbb{Z}/q$. By Lagrange's theorem, $G = \langle a, b \rangle$. We compute the order of b^q. Since G is not cyclic (because it is not abelian) and $b^q \in P$, we conclude that $|b^q| = q$. Since P is normal in G, $bab^{-1} \in P$ and hence $bab^{-1} = a^z$ for some $z \in \mathbb{Z}$. Therefore $b^q a b^{-q} = a^{z^q}$. This implies that $z^q \equiv 1 \bmod p$. The order of u in $(\mathbb{Z}/p)^\times$ divides q and hence it is equal to q (otherwise, $u = 1$ and thus $bab^{-1} = a$, which implies that G is abelian). In conclusion, $G \simeq F_{p,q}$. □

With the proposition we prove, for example, that every group of order 15 is abelian. We can also prove that up to isomorphism $\mathbb{Z}/20$ and $F_{5,4}$ are the only groups of order 20.

Definition 20.3. Diremos que un grupo G es un **grupo de Frobenius** si G tiene un subgrupo propio no trivial H tal que $H \cap xHx^{-1} = \{1\}$ para todo $x \in G \setminus H$. En este caso, el subgrupo H se llama **complemento de Frobenius**.

Theorem 20.4 (Frobenius). *Sea G un grupo de Frobenius con complemento H. Entonces*

$$N = \left(G \setminus \bigcup_{x \in G} xHx^{-1} \right) \cup \{1\}$$

es un subgrupo normal de G.

Proof. Para cada $\chi \in \mathrm{Irr}(H)$, $\chi \neq 1_H$ definimos $\alpha = \chi - \chi(1)1_H \in \mathrm{cf}(H)$, donde 1_H denota el caracter trivial de H.

Demostremos que $(\alpha^G)_H = \alpha$. Primero, $\alpha^G(1) = \alpha(1) = 0$. Si $h \in H \setminus \{1\}$, entonces, gracias al corolario 29.22,

$$\alpha^G(h) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}hx \in H}} \alpha(x^{-1}hx) = \frac{1}{|H|} \sum_{x \in H} \alpha(h) = \alpha(h),$$

pues si $x \notin H$, entonces, como $x^{-1}hx \in H$, se tiene que $h \in H \cap xHx^{-1} = \{1\}$.

Por la reciprocidad de Frobenius,

$$\langle \alpha^G, \alpha^G \rangle = \langle \alpha, (\alpha^G)_H \rangle = \langle \alpha, \alpha \rangle = 1 + \chi(1)^2. \tag{8.4}$$

Nuevamente por la reciprocidad de Frobenius,

$$\langle \alpha^G, 1_G \rangle = \langle \alpha, (1_G)_H \rangle = \langle \alpha, 1_H \rangle = \langle \chi - \chi(1)1_H, 1_H \rangle = -\chi(1),$$

donde 1_G denota al caracter trivial de G. Si escribimos

$$\alpha^G = \sum_{\eta \in \mathrm{Irr}(G)} \langle \alpha^G, \eta \rangle \eta = \langle \alpha^G, 1_G \rangle 1_G + \underbrace{\sum_{\substack{1_G \neq \eta \\ \eta \in \mathrm{Irr}(G)}} \langle \alpha^G, \eta \rangle \eta}_{\phi}$$

entonces $\alpha^G = -\chi(1)1_G + \phi$, donde ϕ es una combinación lineal entera de caracteres irreducibles no triviales de G. Calculamos además

$$1 + \chi(1)^2 = \langle \alpha^G, \alpha^G \rangle = \langle \phi - \chi(1)1_G, \phi - \chi(1)1_G \rangle = \langle \phi, \phi \rangle + \chi(1)^2$$

y luego $\langle \phi, \phi \rangle = 1$.

Claim. Si $\eta \in \mathrm{Irr}(G)$ es tal que $\eta \neq 1_G$, entonces $\langle \alpha^G, \eta \rangle \in \mathbb{Z}$.

En efecto, por la reciprocidad de Frobenius, $\langle \alpha^G, \eta \rangle = \langle \alpha, \eta_H \rangle$. Si descomponemos a η_H en irreducibles de H, digamos

$$\eta_H = m_1 1_H + m_2 \chi + m_3 \theta_3 + \cdots + m_t \theta_t$$

para ciertos $m_1, m_2, \ldots, m_t \geq 0$, entonces, como

$$\langle \alpha, 1_H \rangle = \langle \chi - \chi(1)1_H, 1_H \rangle = -\chi(1), \qquad \langle \alpha, \chi \rangle = \langle \chi - \chi(1)1_H, \chi \rangle = 1,$$

y además

$$\langle \alpha, \theta_j \rangle = \langle \chi - \chi(1)1_H, \theta_j \rangle = 0$$

para todo $j \in \{3, \ldots, t\}$, se concluye que

$$\langle \alpha^G, \eta \rangle = -m_1\chi(1) + m_2 \in \mathbb{Z}.$$

Claim. $\phi \in \mathrm{Irr}(G)$.

Como $\langle \alpha^G, \eta \rangle \in \mathbb{Z}$ para todo $\eta \in \mathrm{Irr}(G)$ tal que $\eta \neq 1_G$ y además

$$1 = \langle \phi, \phi \rangle = \sum_{\substack{\eta, \theta \in \mathrm{Irr}(G) \\ \eta, \theta \neq 1_G}} \langle \alpha^G, \eta \rangle \langle \alpha^G, \theta \rangle \langle \eta, \theta \rangle = \sum_{\substack{\eta \neq 1_G \\ \eta \in \mathrm{Irr}(G)}} \langle \alpha^G, \eta \rangle^2,$$

entonces existe un único $\eta \in \mathrm{Irr}(G)$ tal que $\langle \alpha^G, \eta \rangle^2 = 1$ y el resto de los productos es cero, es decir $\alpha^G = \pm\eta$ para un cierto $\eta \in \mathrm{Irr}(G)$. Como además

$$\chi - \chi(1)1_H = \alpha = (\alpha^G)_H = (\phi - \chi(1)1_G)_H = \phi_H - \chi(1)1_H,$$

se tiene que $\phi(1) = \phi_H(1) = \chi(1) \in \mathbb{Z}_{\geq 1}$. Luego $\phi \in \mathrm{Irr}(G)$.

Observemos que hemos demostrado que si $\chi \in \mathrm{Irr}(H)$ es tal que $\chi \neq 1_H$, entonces existe $\phi_\chi \in \mathrm{Irr}(G)$ tal que $(\phi_\chi)_H = \chi$.

Vamos a demostrar que N es igual a

$$M = \bigcap_{\substack{\chi \in \mathrm{Irr}(H) \\ \chi \neq 1_H}} \ker \phi_\chi.$$

Demostremos primero que $N \subseteq M$. Sea $n \in N \setminus \{1\}$ y sea $\chi \in \mathrm{Irr}(H) \setminus \{1_H\}$. Como n no pertenece a ningún conjugado de H,

$$\alpha^G(n) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}nx \in H}} \chi(x^{-1}nx) = 0$$

pues como $n \in N$ el conjunto $\{x \in G : x^{-1}nx \in H\}$ es vacío. Como entonces

$$0 = \alpha^G(n) = \phi_\chi(n) - \chi(1) = \phi_\chi(n) - \phi_\chi(1),$$

se concluye que $n \in \ker \phi_\chi$.

Demostremos ahora que $M \subseteq N$. Sea $h \in M \cap H$ y sea $\chi \in \mathrm{Irr}(H) \setminus \{1_H\}$. Entonces

$$\phi_\chi(h) - \chi(1) = \alpha^G(h) = \alpha(h) = \chi(h) - \chi(1),$$

y luego $h \in \ker \chi$ pues

$$\chi(h) = \phi_\chi(h) = \phi_\chi(1) = \chi(1).$$

Por lo tanto $h \in \cap_\chi \ker \chi = \{1\}$, que que vimos en la fórmula (8.1) que la intersección de los núcleos de los irreducibles es trivial. Demostremos ahora que $M \cap xHx^{-1} = \{1\}$ para todo $x \in G$. Sean $x \in G$ y $m \in M \cap xHx^{-1}$. Como $m = xhx^{-1}$ para algún $h \in H$, $x^{-1}mx \in H \cap M = \{1\}$. Esto implica que $m = 1$. □

No se conoce una demostración del teorema de Frobenius que no use teoría de caracteres.

Definition 20.5. Sea G un grupo de Frobenius. El subgrupo normal N construido en el teorema de Frobenius se llama **núcleo de Frobenius**.

Corollary 20.6. *Sea G un grupo de Frobenius con complemento H. Entonces existe un subgrupo normal N de G tal que $G = HN$, $H \cap N = \{1\}$.*

Proof. La existencia del subgrupo normal N está garantizada por el teorema de Frobenius. Demostremos que $H \subseteq N_H(H)$. Si $h \in H \setminus \{1\}$ y $g \in G$ son tales que $ghg^{-1} \in H$, entonces $h \in g^{-1}Hg \cap H$ y luego $g \in H$. Como entonces $H = N_G(H)$, el subgrupo H tiene $(G : H)$ conjugados y luego $|G| = |H||N|$ pues

$$|N| = |G| - (G : H)(|H| - 1) = (G : H).$$

Como $N \cap H = \{1\}$, entonces

$$|HN| = |N||H|/|H \cap N| = |N||H| = |G|$$

y luego $G = NH$. □

Corollary 20.7 (Combinatorial Frobenius' theorem). *Sea X un conjunto finito y sea G un grupo que actúa transitivamente en X. Supongamos que todo $g \in G \setminus \{1\}$ fija a lo sumo un punto de X. El conjunto N formado por la identidad y las permutaciones que mueven todos los puntos de X es un subgrupo de G.*

Proof. Sea $x \in X$ y sea $H = G_x$. Veamos que si $g \in G \setminus H$ entonces $H \cap gHg^{-1} = 1$. Si $h \in H \cap gHg^{-1}$ entonces $h \cdot x = x$ y $g^{-1}hg \cdot x = x$. Como $g \cdot x \neq x$, entonces h fija dos puntos de X. Esto implica que $h = 1$ (pues todo elemento no trivial fija a lo sumo un punto de X).

Por el teorema **??**, el conjunto

$$N = \left(G \setminus \bigcup_{g \in G} gHg^{-1} \right) \cup \{1\}$$

es un subgrupo de G. Veamos cómo son los elementos de N: Si $h \in \cup_{g \in G} gHg^{-1}$ entonces existe $g \in G$ tal que $g^{-1}hg \in H$, es decir $(g^{-1}hg) \cdot x = x$ o quivalentemente $h \in G_{g \cdot x}$. Luego, a excepción de la identidad, los elementos de N son los elementos de G que mueven algún punto de X. □

Example 20.8. Sea F un cuerpo finito y sea G el grupo de funciones $f : G \to G$ de la forma $f(x) = ax + b$, $a, b \in F$ con $a \neq 0$. El grupo G actúa en F y toda $f \neq \mathrm{id}$ fija a lo sumo un punto de F pues

$$x = f(x) = ax + b \implies x = 1 - (b/a).$$

En este caso, $N = \{f : f(x) = x + b\,, b \in F\}$ que es un subgrupo de G.

Exercise 20.9. Prove that Theorem 20.4 can be obtained from Corollary 20.7.

In his doctoral thesis Thompson proved the following result, conjectured by Frobenius.

Theorem 20.10 (Thompson). *Let G be a Frobenius group. If N is the Frobenius kernel, then N is nilpotent.*

See [22, Theorem 6.24] for the proof.

Lecture 9

§21. Some theorems of Burnside

For $n \geq 1$ let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{C}^n$. The **natural representation** of $\mathbb{S}_n$ is $\rho\colon \mathbb{S}_n \to \mathbf{GL}_n(C)$, $\sigma \mapsto \rho_\sigma$, where $\rho_\sigma(e_j) = e_{\sigma(j)}$ for all $j \in \{1, \ldots, n\}$. The matrix of ρ_σ in the standard basis is

$$(\rho_\sigma)_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j), \\ 0 & \text{otherwise.} \end{cases} \tag{9.1}$$

Lemma 21.1. *For $n \geq 1$ let $\rho\colon \mathbb{S}_n \to \mathbf{GL}_n(C)$ be the natural representation of the symmetric group. If $A \in \mathbb{C}^{n\times n}$ and $\sigma \in \mathbb{S}_n$, then*

$$A_{ij} = (\rho_\sigma A)_{\sigma(i)j} = (A\rho_\sigma)_{i\sigma^{-1}(j)}$$

for all $i, j \in \{1, \ldots, n\}$.

Proof. With (9.1) we compute:

$$(A\rho_\sigma)_{ij} = \sum_{k=1}^{n} A_{ik}(\rho_\sigma)_{kj} = A_{i\sigma(j)}, \quad (\rho_\sigma A)_{ij} = \sum_{k=1}^{n} (\rho_\sigma)_{ik} A_{kj} = A_{\sigma^{-1}(i)j}. \qquad \square$$

Definition 21.2. Let G be a finite group. A character χ of G is said to be **real** if $\chi = \overline{\chi}$, that is $\chi(g) \in \mathbb{R}$ for all $g \in G$.

Exercise 21.3. Let G be a finite group. If $\chi \in \mathrm{Irr}(G)$, then $\overline{\chi}$ is irreducible.

Definition 21.4. Let G be a group. A conjugacy class C of G is said to be **real** if for every $g \in C$ one has $g^{-1} \in C$.

We use the following notation: if G is a group and $C = \{xgx^{-1} : x \in G\}$ is a conjugacy class of G, then $C^{-1} = \{xg^{-1}x^{-1} : x \in G\}$.

Theorem 21.5 (Burnside). *Let G be a finite group. The number of real conjugacy classes is equal to the number of real irreducible characters.*

Proof. Let $C_1, \dots, C_r$ be the conjugacy classes of G and let $\chi_1, \dots, \chi_r$ be the irreducible characters of G. Let $\alpha, \beta \in \mathbb{S}_r$ be such that $\overline{\chi_i} = \chi_{\alpha(i)}$ and $C_i^{-1} = C_{\beta(i)}$ for all $i \in \{1, \dots, r\}$. Note that χ_i is real if and only if $\alpha(i) = i$ and that C_i is real if and only if $\beta(i) = i$. The number n of fixed points of α is equal to the number of irreducible characters of G and the number m of fixed points of β is equal to the number of real classes. Let $\rho\colon \mathbb{S}_r \to \mathbf{GL}(r, \mathbb{C})$ be the natural representation of $\mathbb{S}_r$. Then $\chi_\rho(\alpha) = n$ and $\chi_\rho(\beta) = m$. We claim that $\operatorname{trace} \rho_\alpha = \operatorname{trace} \rho_\beta$. Let $X \in \mathbf{GL}(r, \mathbb{C})$ be the character matrix of G. By Lemma 21.1,

$$\rho_\alpha X = \overline{X} = X \rho_\beta.$$

Since X is invertible, $\rho_\alpha = X \rho_\beta X^{-1}$. Thus

$$n = \chi_\rho(\alpha) = \operatorname{trace} \rho_\alpha = \operatorname{trace} \rho_\beta = \chi_\rho(\beta) = m. \qquad \square$$

Corollary 21.6. *Let G be a finite group. Then $|G|$ is odd if and only if the only real $\chi \in \operatorname{Irr}(G)$ is the trivial character.*

Proof. We first prove $\Longleftarrow$. If $|G|$ is even, there exists $g \in G$ of order two (Cauchy's theorem). The conjugacy class of g is real.

We now prove $\Longrightarrow$. Assume that G has a non-trivial real conjugacy class C. Let $g \in C$. We claim that G has an element of even order. Let $h \in G$ be such that $hgh^{-1} = g^{-1}$. Then $h^2 \in C_G(g)$, as $h^2 g h^{-2} = g$. If $h \in \langle h^2 \rangle \subseteq C_G(g)$, then g has even order, as $g^{-1} = g$. If $h \notin \langle h^2 \rangle$, then h^2 does not generate $\langle h \rangle$. Hence h has odd order, as $|h| \neq |h^2| = |h|/(|h| : 2)$. $\square$

Theorem 21.7 (Burnside). *Let G be a finite group of odd order with r conjugacy classes. Then $r \equiv |G| \bmod 16$.*

Proof. Since $|G|$ is odd, every non-trivial $\chi \in \operatorname{Irr}(G)$ is not real by the previous corollary. The irreducible characters of G are then

$$\chi_1, \chi_2, \overline{\chi_2}, \dots, \chi_k, \overline{\chi_k}, \quad r = 1 + 2k,$$

where χ_1 denotes the trivial character. For every $j \in \{2, \dots, k\}$ let $d_j = \chi_j(1)$. Since each d_j divides $|G|$ by Frobenius' theorem and $|G|$ is odd, every d_j is an odd number, say $d_j = 1 + 2m_j$. Thus

$$\begin{aligned} |G| &= 1 + \sum_{j=2}^{k} 2d_j^2 = 1 + \sum_{j=2}^{k} 2(2m_j + 1)^2 \\ &= 1 + \sum_{j=2}^{k} 2(4m_j^2 + 4m_j + 1) = 1 + 2k + 8 \sum_{j=2}^{k} m_j(m_j + 1). \end{aligned}$$

Hence $|G| \equiv r \bmod 16$, as $r = 1 + 2k$ and every $m_j(m_j + 1)$ is even. $\square$

Exercise 21.8. Prove that every group of order 15 is abelian.

Lecture 10

§22. Solvable groups and Burnside's theorem

For a group G let $G^{(0)} = G$ and $G^{(i+1)} = [G^{(i)}, G^{(i)}]$ for $i \geq 0$. The **derived series** of G is the sequence

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

Each $G^{(i)}$ is a characteristic subgroup of G. We say that G is **solvable** if $G^{(n)} = \{1\}$ for some n.

Example 22.1. Abelian groups are solvable.

Example 22.2. The group $\mathbf{SL}_2(3)$ is solvable, as the derived series is

$$\mathbf{SL}_2(3) \supseteq Q_8 \supseteq C_4 \supseteq C_2 \supseteq \{1\}.$$

Here is the what the computer says:

```
gap> IsSolvable(SL(2,3));
true
gap> List(DerivedSeries(SL(2,3)),StructureDescription);
[ "SL(2,3)", "Q8", "C2", "1" ]
```

Example 22.3. Non-abelian simple groups cannot be solvable.

Exercise 22.4. Let G be a group. Prove the following statements:

1) A subgroup H of G is solvable.
2) Let K be a normal subgroup of G. Then G is solvable if and only if K and G/K are solvable.

Example 22.5. For $n \geq 5$ the group $\mathbb{A}_n$ is not solvable. It follows that $\mathbb{S}_n$ is not solvable for $n \geq 5$.

Exercise 22.6. Let p be a prime number. Prove that finite p-groups are solvable.

Theorem 22.7 (Burnside). *Let G be a finite group. If $\phi\colon G \to \mathbf{GL}_n(\mathbb{C})$ is a representation with character χ and C is a conjugacy class of G such that $\gcd(|C|, n) = 1$, then for every $g \in C$ either $\chi(g) = 0$ or ϕ_g is a scalar matrix.*

We need a lemma.

Lemma 22.8. *Let $\epsilon_1, \dots, \epsilon_n$ be roots of one such that $(\epsilon_1 + \cdots + \epsilon_n)/n \in \mathbb{A}$. Then either $\epsilon_1 = \cdots = \epsilon_n$ or $\epsilon_1 + \cdots + \epsilon_n = 0$.*

Proof. Let $\alpha = (\epsilon_1 + \cdots + \epsilon_n)/n$. If the ϵ_js are not all equal, then $N(\alpha) < 1$. Moreover, $N(\beta) < 1$ for every algebraic conjugate β of α. Since the product of the algebraic conjugates of α is an integer of absolute value < 1, it follows that it is zero. □

Now we prove the theorem.

Proof of Theorem 22.7. Let $\epsilon_1, \dots, \epsilon_n$ be the eigenvalues of ϕ_g. By assumption, $\gcd(|C|, n) = 1$, there exist $a, b \in \mathbb{Z}$ such that $a|C| + bn = 1$. Since $|C|\chi(g)/n \in \mathbb{A}$, after multiplying by $\chi(g)/n$ we obtain that

$$a|C|\frac{\chi(g)}{n} + b\chi(g) = \frac{\chi(g)}{n} = \frac{1}{n}(\epsilon_1 + \cdots + \epsilon_n) \in \mathbb{A}.$$

The previous lemma implies that there are two cases to consider: either $\epsilon_1 = \cdots = \epsilon_n$ or $\epsilon_1 + \cdots + \epsilon_n = 0$. In the first case, since ϕ_g is diagonalizable, ϕ_g is a scalar matrix. In the second case, $\chi(g) = 0$. □

Theorem 22.9 (Burnside). *Let p be a prime number. If G is a finite group and C is a conjugacy class of G with $p^k > 1$ elements, then G is not simple.*

Proof. Let $g \in C \setminus \{1\}$. Column orthogonality implies that

$$\begin{aligned} 0 &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) \\ &= \sum_{p \mid \chi(1)} \chi(1)\chi(g) + \sum_{p \nmid \chi(1)} \chi(1)\chi(g) + 1, \end{aligned} \tag{10.1}$$

where the one corresponds to the trivial representation of G.

Look this equation modulo p. If $\chi(g) = 0$ for all $\chi \in \mathrm{Irr}(G)$ such that $\chi \neq \chi_1$ and $p \nmid \chi(1)$, then

$$-\frac{1}{p} = \sum \frac{\chi(1)}{p}\chi(g) \in \mathbb{A} \cap \mathbb{Q} = \mathbb{Z},$$

where the sum is taken over all non-trivial irreducibles of G of degree divisible by p, a contradiction. Hence there exists an irreducible non-trivial representation ϕ with character χ such that p does not divide $\chi(1)$ and $\chi(g) \neq 0$. By the previous theorem, ϕ_g is a scalar matrix. If ϕ is faithful, then g is a non-trivial central element, a contradiction since $|C| > 1$. If ϕ is not faithful, then G is not simple (because $\ker\phi$ is a non-trivial proper normal subgroup of G). □

Theorem 22.10 (Burnside). *Let p and q be prime numbers. If G has order $p^a q^b$, then G is solvable.*

Proof. Let us assume that the theorem is not true. Let G be a group of minimal order $p^a q^b$ that is not solvable. Since $|G|$ is minimal, G is simple. By the previous theorem, G has no conjugacy classes of size p^k nor conjugacy classes of size q^l with $k, l \geq 1$. The size of every conjugacy class of G is one or divisible by pq. By the class equation,

$$|G| = 1 + \sum_{C : |C| > 1} |C|,$$

where the sum is taken over all conjugacy classes with more than one element, a contradiction. □

Some generalizations of Burnside's theorem.

Theorem 22.11 (Kegel–Wielandt). *If G is a finite group and there are nilpotent subgroups A and B of G such that $G = AB$, then G is solvable.*

See [3, Theorem 2.4.3] for the proof.

Another generalization of Burnside's theorem is based on *word maps*. A word map of a group G is a map

$$G^k \to G, \quad (x_1, \ldots, x_k) \mapsto w(x_1, \ldots, x_k)$$

for some word $w(x_1, \ldots, x_k)$ of the free group F_k of rank k. Some word maps are surjective in certain families of groups. For example, Ore's conjecture is precisely the surjectivity of the word map $(x, y) \mapsto [x, y] = xyx^{-1}y^{-1}$ in every finite non-abelian simple group.

Theorem 22.12 (Guralnick–Liebeck–O'Brien–Shalev–Tiep). *Let $a, b \geq 0$, p and q be prime numbers and $N = p^a q^b$. The map $(x, y) \mapsto x^N y^N$ is surjective in every finite simple group.*

The proof appears in [14].

The theorem implies Burnside's theorem. Let G be a group of order $N = p^a q^b$. Assume that G is not solvable. Fix a composition series of G. There is a non-abelian factor S of order that divides N. Since S is simple non-abelian and $s^N = 1$, it follows that the word map $(x, y) \mapsto x^N y^N$ has trivial image in S, a contradiction to the theorem.

§23. Feit–Thompson theorem

Theorem 23.1 (Feit–Thompson). *Groups of odd order are solvable.*

The proof of Feit–Thompson theorem is extremely hard. It occupies a full volume of the *Pacific Journal of Mathematics* [9]. A formal verification of the proof (based on the computer software Coq) was announced in [12].

Back in the day it was believed that if a certain divisibility conjecture is true, the proof of Feit–Thompson theorem could be simplified.

Conjecture 23.2 (Feit–Thompson). There are no prime numbers p and q such that $\frac{p^q-1}{p-1}$ divides $\frac{q^p-1}{q-1}$.

The conjecture remains open. However, now we know that proving the conjecture will not simplify further the proof of Feit–Thompson theorem.

In 2012 Le proved that the conjecture is true for $q = 3$, see [28].

In [37] Stephens proved that a certain stronger version of the conjecture does not hold, as the integers $\frac{p^q-1}{p-1}$ and $\frac{q^p-1}{q-1}$ could have common factors. In fact, if $p = 17$ and $q = 3313$, then

$$\gcd\left(\frac{p^q-1}{p-1}, \frac{q^p-1}{q-1}\right) = 112643.$$

Nowadays we can check this easily in almost every desktop computer:

```
gap> Gcd((17^3313-1)/16,(3313^17-1)/3312);
112643
```

No other counterexamples have been found to Stephen's stronger version of the conjecture.

§24. Hurwitz' theorem

Hurwitz's theorem

We know that $x^2y^2 = (xy)^2$ holds for all $x, y \in \mathbb{C}$. Fibonnaci found the identity

$$(x_1^2+x_2^2)(y_1^2+y_2^2) = (x_1y_1-x_2y_2)^2+(x_1y_2-x_2y_1)^2.$$

Euler and Hamilton, independently, found a similar identity:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = z_1^2+z_2^2+z_3^2+z_4^2,$$

where

$$\begin{aligned} z_1 &= x_1y_1-x_2y_2-x_3y_3-x_4y_4,\\ z_2 &= x_1y_2+x_2y_1-x_3y_3-x_4y_4,\\ z_3 &= x_1y_3+x_3y_1-x_2y_4+x_4y_2,\\ z_4 &= -x_1y_4+x_4y_1x_2y_3-x_3y_2. \end{aligned} \tag{10.2}$$

Cayley found a similar identity for sums of eight squares. Are there other identities of this type? Hurwitz' proved that this is not the case. We present Eckmann's proof of Hurwitz' theorem. The proof uses character theory.

Lemma 24.1. *Let $n > 2$ be an even number. If there exists a group G with generators $\epsilon, x_1, \dots, x_{n-1}$ and relations*

$$x_1^2 = \dots = x_{n-1}^2 = \epsilon \neq 1, \quad \epsilon^2 = 1, \quad [x_i, x_j] = \epsilon \quad \textit{if} \quad i \neq j,$$

then the following statements hold:

1) $|G| = 2^n$.
2) $[G,G] = \{1, \epsilon\}$. *In particular, G has exactly 2^{n-1} degree-one representations.*
3) *If $g \notin Z(G)$, then the conjugacy class of g is $\{g, \epsilon g\}$.*
4) $Z(G) = \{1, \epsilon, x_1 \cdots x_{n-1}, \epsilon x_1 \cdots x_{n-1}\}$.
5) *G has $2^{n-1} + 2$ conjugacy classes.*
6) *G has two irreducible representations of degree $2^{\frac{n-2}{2}} > 1$.*

Proof. Let us prove 1) and 2). Note that $\epsilon \in Z(G)$, as $\epsilon = x_i^2$ for all $i \in \{1, \dots, n-1\}$. Since $n - 1 > 2$, $[x_1, x_2] = \epsilon$. Hence $\epsilon \in [G,G]$. Moreover, $G/\langle \epsilon \rangle$ is abelian. Thus $[G,G] = \langle \epsilon \rangle$. Since $G/[G,G]$ is elementary abelian of order 2^{n-1}, it follows that $|G| = 2^n$.

We now prove 3). Let $g \in G \setminus Z(G)$ and $x \in G$ be such that $[x, g] \neq 1$. Then $[x, g] = \epsilon$ and $xgx^{-1} = \epsilon g$.

To prove 4) let $g \in G$. Write

$$g = \epsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}},$$

where $a_j \in \{0, 1\}$ for all $j \in \{1, \dots, n-1\}$. If $g \in Z(G)$, then $g x_i = x_i g$ for all $i \in \{1, \dots, n-1\}$. Hence $g \in Z(G)$ if and only if

$$\epsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}} = x_i (\epsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}) x_i^{-1}.$$

Since $x_i x_j^{a_j} x_i = \epsilon^{a_j} x_j^{a_j}$ whenever $i \neq j$ y $\epsilon \in Z(G)$, the elmeent g is central if and only if

$$\sum_{\substack{j=1 \\ j \neq i}}^{n-1} a_j \equiv 0 \bmod 2$$

for all $i \in \{1, \dots, n-1\}$. In particular,

$$\sum_{j \neq i} a_j \equiv \sum_{j \neq k} a_j$$

for all $k \neq i$. Therefore $a_i \equiv a_k \bmod 2$ for all $i, k \in \{1, \dots, n-1\}$. Thus $a_1 = \dots = a_{n-1}$ and $Z(G) = \{1, x_1 \cdots x_{n-1}, \epsilon, \epsilon x_1 \cdots x_{n-1}\}$.

To prove 5) we use the class equation:

$$2^n = |G| = |Z(G)| + \sum_{i=1}^{N} 2 = 4 + 2N.$$

It follows that G has $N+4 = 2^{n-1}+2$ conjugacy classes.

Finally we prove 6). Since G has exactly 2^{n-1} degree-one representations (because $|G/[G,G]| = 2^{n-1}$) and has $2^{n-1}+2$ conjugacy classes, it follows from

$$2^n = |G| = \underbrace{1+\cdots+1}_{2^{n-1}} + f_1^2 + f_2^2 = 2^{n-1} + f_1^2 + f_2^2,$$

that G has two irreducible representations of degrees $f_1 = f_2 = 2^{\frac{n-2}{2}} > 1$. □

Example 24.2. The formulas (10.2) give a representation for the group G of the previous lemma. Write each z_i as $z_i = \sum_{k=1}^4 a_{1k}(x_1,\ldots,x_4)y_k$. Let A be a matrix such that $A_{ij} = a_{ij}(x_1,\ldots,x_4)$, that is

$$A = \begin{pmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & -x_4 & x_3 \\ x_3 & x_4 & x_1 & -x_2 \\ x_4 & -x_3 & x_2 & x_1 \end{pmatrix}$$

The matrix A can be written as $A = A_1x_1 + A_2x_2 + A_3x_3 + A_4x_4$, where

$$A_1 = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} & -1 & & \\ 1 & & & \\ & & & -1 \\ & & 1 & \end{pmatrix}, \quad A_3 = \begin{pmatrix} & & -1 & \\ & & & 1 \\ 1 & & & \\ & -1 & & \end{pmatrix}, \quad A_4 = \begin{pmatrix} & & & -1 \\ & & -1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}.$$

For $i \in \{1,\ldots,4\}$ let $B_i = A_iA_4^T$. Then $B_i = -B_i^T$ and $B_i^2 = -I$ for all $i \in \{1,2,3\}$. Moreover, $B_iB_j = -B_jB_i$ for all $i,j \in \{1,2,3\}$ and $i \neq j$. The group generated by $\{B_1,B_2,B_3\}$ has 2^3 element, all of them of the form

$$\pm B_1^{k_1}B_2^{k_2}B_3^{k_3}$$

for $k_j \in \{0,1\}$. The map $G \to \langle B_1,B_2,B_3\rangle$,

$$x_1 \mapsto B_1, \quad x_2 \mapsto B_2, \quad x_3 \mapsto B_3$$

extends to a group isomomorphism.

Theorem 24.3 (Hurwitz). *If there is an identity of the form*

$$(x_1^2+\cdots+x_n^2)(y_1^2+\cdots+y_n^2) = z_1^2+\cdots+z_n^2, \tag{10.3}$$

where the x_j's and the y_j's are real (or complex) numbers and each z_k is a bilinear function in the x_j's and the y_j's, then $n \in \{1,2,4,8\}$.

Proof. We work over complex numbers. Without loss of generality we may assume that $n > 2$. For $i \in \{1,\ldots,n\}$ let

$$z_i = \sum_{k=1}^{n} a_{ik}(x_1,\ldots,x_n)y_k,$$

where the a_{ik}'s are linear functions. Then

$$z_i^2 = \sum_{k,l=1}^{n} a_{ik}(x_1,\ldots,x_n)a_{il}(x_1,\ldots,x_n)y_k y_l$$

for all $i \in \{1,\ldots,n\}$. Using these expressions for each z_i in (10.3) and comparing coefficients,

$$\sum_{i=1}^{n} a_{ik}(x_1,\ldots,x_n)a_{il}(x_1,\ldots,x_n) = \delta_{k,l}(x_1^2+\cdots+x_n^2), \tag{10.4}$$

where $\delta_{k,l}$ is the usual Kronecker's map. Let A be the $n\times n$ matrix given by

$$A_{ij} = a_{ij}(x_1,\ldots,x_n).$$

Then

$$AA^T = (x_1^2+\cdots+x_n^2)I, \tag{10.5}$$

where I denotes the $n\times n$ identity matrix, as

$$(AA^T)_{kl} = \sum_{i=1}^{n} a_{ki}(x_1,\ldots,x_n)a_{li}(x_1,\ldots,x_n) = \delta_{kl}(x_1^2+\cdots+x_n^2)$$

by (10.4). Since each $a_{ki}(x_1,\ldots,x_n)$ is a linear function, there exist $\alpha_{ij1},\ldots,a_{ijn} \in \mathbb{C}$ such that

$$a_{ij}(x_1,\ldots,x_n) = \alpha_{ij1}x_1+\cdots+\alpha_{ijn}x_n.$$

Write

$$A = A_1x_1+\cdots+A_nx_n,$$

where each A_k is the matrix $(A_k)_{ij} = \alpha_{ijk}$. The formula (10.5) becomes

$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_iA_j^T x_ix_j = (x_1^2+\cdots+x_n^2)I.$$

Thus

$$A_iA_j^T + A_jA_i^T = 0 \quad i\neq j, \quad A_iA_i^T = I. \tag{10.6}$$

We need n complex square matrices of size $n\times n$ satisfying (10.6). For $i \in \{1,\ldots,n\}$ let $B_i = A_n^T A_i$. Then (10.6) turn into

$$B_iB_j^T + B_jB_i^T = 0 \quad i\neq j, \quad B_iB_i^T = I, \quad B_n = I.$$

Set $j = n$ in the first family of equations to obtain $B_i = -B_i^T$ for all $i \in \{1, \dots, n-1\}$. It follows that

$$\begin{aligned} B_i^2 &= -I \qquad \text{for all } i \in \{1, \dots, n-1\}, \\ [B_i, B_j] &= -I \quad \text{for all } i, j \in \{1, \dots, n-1\}. \end{aligned} \tag{10.7}$$

Claim. n is even.

Computing the determinant of $B_i B_j = -B_j B_i$ we obtain that

$$1 = \det(B_i B_j) = (-1)^n \det(B_j B_i) = (-1)^n.$$

Hence n is even.

Claim. The group G of the lemma admits a faithful representation $\rho\colon G \to \mathbf{GL}_n(\mathbb{C})$.

By (10.7), there is a well-defined injective group homomorphism ρ such that $x_i \mapsto B_i$ for all $i \in \{1, \dots, n-1\}$ and $\epsilon \mapsto -I$.

Claim. $2^{\frac{n-2}{2}}$ divides n.

Since $\epsilon \in [G, G]$ by Lemma 24.1, every one-dimensional representation satisfies $\epsilon \mapsto 1$. This implies that ρ cannot have degree-one sub representations. In fact, if $W = \langle w \rangle$ is G-invariant subspace of $\mathbb{C}^n$, then $\psi = \rho|_W : G \to \mathbf{GL}(W) \simeq \mathbb{C}^\times$ is a representation. In particular,

$$-w = -Iw = \psi_\epsilon(w) = \psi_{[x_i, x_j]}(w) = \psi_{x_i} \psi_{x_j} \psi_{x_i}^{-1} \psi_{x_j}^{-1}(w) = w,$$

a contradiction.

This means that the $\mathbb{C}[G]$-module $\mathbb{C}^n$ decomposes as $\mathbb{C}^n \simeq aS \oplus bT$, where a and b are integers and S and T are simple $\mathbb{C}[G]$-modules of dimension $2^{\frac{n-2}{2}}$. In particular,

$$n = \dim V = \dim(aS \oplus bT) = (a+b) 2^{\frac{n-2}{2}}.$$

To finish the proof of the theorem write $n = 2^a b$ for $a \geq 1$ and b an odd integer. Since $\frac{n-2}{2}$ divides n,

$$2^{\frac{n}{2}-1} = 2^{\frac{n-2}{2}} \leq n = 2^a b.$$

Thus $\frac{n}{2} - 1 \leq a$ and hence $2^a \leq n \leq 2(a+1)$. It follows that $n \in \{4, 8\}$. □

We now present an application, see [43] for more information.

Theorem 24.4. *Let V be a real vector space (with an inner product) such that $\dim V = n \geq 3$. If there exists a bilinear function $V \times V \to \mathbb{R}$, $(v, w) \mapsto v \times w$, such that $v \times w$ is orthogonal both to v and w and*

$$\|v \times w\|^2 = \|v\|^2 \|w\|^2 - \langle v, w \rangle^2,$$

where $\|v\|^2 = \langle v, v \rangle$, then $n \in \{3, 7\}$.

Proof. Let $W = V \oplus \mathbb{R}$ with the inner product

$$\langle (v_1, r_1), (v_2, r_2) \rangle = \langle v_1, v_2 \rangle + r_1 r_2.$$

Note that

$$\begin{aligned} &\langle v_1 \times v_2 + r_1 v_2 + r_2 v_1, v_1 \times v_2 + r_1 v_2 + r_2 v_1 \rangle \\ &\quad = \|v_1 \times v_2\|^2 + r_1^2 \|v_2\|^2 + 2 r_1 r_2 \langle v_1, v_2 \rangle + r_2^2 \|v_1\|^2. \end{aligned}$$

Thus

$$\begin{aligned} &(\|v_1\|^2 + r_1^2)(\|v_2\|^2 + r_2) \\ &\qquad = \|v_1\|^2 \|v_2\|^2 + r_2^2 \|v_1\|^2 + r_1^2 \|v_2\|^2 + r_1^2 r_2^2 \\ &\qquad = \|v_1 \times v_2 + r_1 v_1 + r_2 v_2\|^2 - 2 r_1 r_2 \langle v_1, v_2 \rangle + \langle v_1, v_2 \rangle^2 + r_1^2 r_2^2 \\ &\qquad = \|v_1 \times v_2 + r_1 v_1 + r_2 v_2\|^2 + (\langle v_1, v_2 \rangle - r_1 r_2)^2 \\ &\qquad = z_1^2 + \cdots + z_{n+1}^2, \end{aligned}$$

where the z_k's are bilinear functions in (v_1, r_1) and (v_2, r_2). By Hurwitz' theorem, $n+1 \in \{4, 8\}$. Hence $n \in \{3, 7\}$. □

In the theorem, if $\dim V = 3$, we obtain the usual cross product. If $\dim V = 7$, let

$$W = \{(v, k, w) : v, w \in V, k \in \mathbb{R}\}$$

with the inner product

$$\langle (v_1, k_1, w_1), (v_2, k_2, w_2) \rangle = \langle v_1, v_2 \rangle + k_1 k_2 + \langle w_1, w_2 \rangle.$$

It is an exercise to show that

$$\begin{aligned} &(v_1, k_1, w_1) \times (v_2, k_2, w_2) \\ &\qquad = (k_1 w_2 - k_2 w_1 + v_1 \times v_2 - w_1 \times w_2, \\ &\qquad\quad - \langle v_1, w_2 \rangle + \langle v_2, w_1 \rangle, k_2 v_1 - k_1 v_2 - v_1 \times w_2 - w_1 \times v_2) \end{aligned}$$

satisfies the properties of the theorem.

Lecture 11

§25. Lie algebras

Definition 25.1. Let K be a field. A **Lie algebra** (over K) is a K-vector space L together with a bilinear map $L \times L \to L$, $(x, y) \mapsto [x, y]$, such that

$$[x,x] = 0 \quad \text{for all } x \in L, \tag{11.1}$$

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0 \quad \text{for all } x,y,z \in L. \tag{11.2}$$

Equality (11.2) is known as the **Jacobi identity**.

Exercise 25.2. Prove that (11.1) implies $[x, y] = -[y, x]$ for all $x, y \in L$.

A Lie algebra L is said to be **abelian** if $[x, y] = 0$ for all $x, y \in L$.

Exercise 25.3. If L and L_1 are Lie algebras, then $L \oplus L_1$ is a Lie algebra with $[(x,x_1),(y,y_1)] = ([x,y),(x_1,y_1)]$ for $x, y \in L$ and $x_1, y_1 \in L_1$.

Exercise 25.4. Prove that $\mathbb{R}^3$ with the usual vector product

$$[(x_1,x_2,x_3),(y_1,y_2,y_3)] = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1)$$

is a (real) Lie algebra.

We will main work with finite-dimensional complex Lie algebras.

Example 25.5 (general linear Lie algebra). Let V be a finite-dimensional vector space and $\mathfrak{gl}(V)$ be the set of linear maps $V \to V$. Then $\mathfrak{gl}(V)$ with $[x, y] = xy - yx$ is a Lie algebra.

A matrix version of the previous example: We write $\mathfrak{gl}(n, \mathbb{C})$ to denote the vector space of all $n \times n$ complex matrices with Lie bracket $[x, y] = xy - yx$. The vector space $\mathfrak{gl}(n, \mathbb{C})$ has a basis $\{e_{ij} : 1 \le i, j \le n\}$, where

$$(e_{ij})_{kl} = \begin{cases} 1 & \text{if } (i,j) = (k,l), \\ 0 & \text{otherwise.} \end{cases}$$

Exercise 25.6. Compute $[e_{ij}, e_{ik}]$.

Example 25.7 (special linear Lie algebra). Let $\mathfrak{sl}(n, \mathbb{C})$ be the subspace of $\mathfrak{gl}(n, \mathbb{C})$ consisting of all matrices with trace zero.

Exercise 25.8. Find a basis of $\mathfrak{sl}(n, \mathbb{C})$.

Definition 25.9. A Lie **subalgebra** of L is a vector space L_1 of L such that $[x, y] \in L_1$ for all $x, y \in L_1$.

Of course, $\mathfrak{sl}(n, \mathbb{C})$ is a subalgebra of $\mathfrak{gl}(n, \mathbb{C})$.

Definition 25.10. An **ideal** of a Lie algebra L is a subspace I of L such that $[x, y] \in I$ for all $x \in L$ and $y \in I$.

Trivial examples of ideals of a Lie algebra L are $\{0\}$ and L.

Example 25.11. Let L be a Lie algebra. Then the **center**

$$Z(L) = \{x \in L : [x, y] = 0 \text{ for all } y \in L\}.$$

is an ideal of L.

Example 25.12. Let L be a Lie algebra. The **derived algebra** $[L, L]$ consists of all linear combinations of commutators $[x, y]$ is an ideal of L.

Exercise 25.13. Compute $Z(\mathfrak{sl}(n, \mathbb{C}))$.

Exercise 25.14. Prove that $\mathfrak{sl}(2, \mathbb{C})$ has no non-trivial ideals.

One easily checks that $\mathfrak{sl}(n, \mathbb{C})$ is an ideal of $\mathfrak{gl}(n, \mathbb{C})$. In fact, an ideal is always a subalgebra. The converse is not true. Can you find an example?

Definition 25.15. Let L and L_1 be Lie algebras. A map $f : L \to L_1$ is a **Lie algebra homomorphism** if $f([x, y]) = [f(x), f(y)]$ for all $x, y \in L$.

As usual, an isomorphism between Lie algebras will be a bijective homomorphism of Lie algebras.

Example 25.16. Let L and L_1 be Lie algebras. The canonical injections $L \to L \oplus L_1$ and $L_1 \to L_{\oplus} L_1$ and the canonical surjections $L \oplus L_1 \to L$ and $L \oplus L_1 \to L_1$ are Lie algebras homomorphisms.

Example 25.17. Let L be a Lie algebra. The **opposite Lie algebra** L^{op} is the vector space L with $[x, y]^{\mathrm{op}} = -[x, y]$. Then $L \to L^{\mathrm{op}}$, $x \mapsto -x$, is an isomorphism of Lie algebras.

Exercise 25.18. Let $f : L \to L_1$ be a Lie algebra homomorphism. Prove that the **kernel** of f, $\ker f = \{x \in L : f(x) = 0\}$ is an ideal of L, and that the **image** of f is a subalgebra of L_1.

Example 25.19. Let L be a Lie algebra. The **adjoint homomorphism** is the map

$$\operatorname{ad}: L \to \mathfrak{gl}(L), \quad (\operatorname{ad} x)(y) = [x, y].$$

Let L be a Lie algebra and I be an ideal of L. Then the quotient vector space L/I is a Lie algebra with $[x+I, y+I] = [x, y]+I$. The canonical map $L \to L/I$, $x \mapsto x+I$, is a surjective Lie algebra homomorphism.

Exercise 25.20. Let $f: L \to L_1$ be a Lie algebra homomorphism. Prove that $f/\ker f \simeq f(L)$.

Definition 25.21. A Lie algebra L is said to be **simple** if $[L, L] \neq \{0\}$ and $\{0\}$ and L are the only ideals of L.

If L is a simple Lie algebra, then $Z(L) = \{0\}$ and $L = [L, L]$.

Exercise 25.22. Prove that every simple Lie algebra is isomorphic to a linear Lie algebra.

§26. Representations of Lie algebras

Definition 26.1. A **representation** of a Lie algebra L is a Lie homomorphism $\rho: L \to \mathfrak{gl}(V)$, where V is a vector space.

If $L \to \mathfrak{gl}(V)$ is a representation of a Lie algebra L, fixing a basis for V we obtain a **matrix representation** $L \to \mathfrak{gl}(n, \mathbb{C})$.

Example 26.2. Let L be a Lie algebra. The map $\operatorname{ad}: L \to \mathfrak{gl}(L)$, $x \mapsto (\operatorname{ad} x)$, is a lie homomorphism.

Definition 26.3. Let L be a Lie algebra. A (left) Lie L-module is a vector space V together with a map $L \times V \to V$, $(x, v) \mapsto xv$, such that $(x, v) \mapsto xv$ is bilinear and

$$[x, y]v = x(yv) - y(xv)$$

for all $x, y \in L$ and $v \in V$.

As it happens in the case of groups, Lie modules are in bijective correspondence with representations.

Example 26.4. Let L be a subalgebra of $\mathfrak{gl}(V)$. Then L is an L-module.

Definition 26.5. Let L be a Lie algebra and V be a Lie L-module. A **submodule** of V is a subspace W such that $xw \in W$ for all $x \in L$ and $w \in W$.

Example 26.6. We know that L is an L-module with the adjoint representation. The submodules of L are the ideals of L.

If W is a submodule of V, then V/W with $x(v+W) = xv+W$ is a module.

Definition 26.7. Let L be a Lie algebra. An L-module V is said to be **simple** (or irreducible) if $V \neq \{0\}$ and it has no submodules other than $\{0\}$ and V.

One-dimensional modules are simple. In particular, the trivial module is always simple.

Example 26.8. Let L be a simple Lie algebra (e.g. $\mathfrak{sl}(2,\mathbb{C})$). Then the adjoint representation is irreducible, that is L is a simple L-module.

Definition 26.9. Let L be a Lie algebra and V be an L-module. We say that V is **indecomposable** if there are no non-zero submodules U and W such that $V = U \oplus W$.

Clearly, irreducible modules are indecomposable. The converse is not true.

Definition 26.10. Let L be a Lie algebra and V be an L-module. We say that V is **completely reducible** if $V = S_1 \oplus \cdots \oplus S_k$ for simple modules $S_1, \ldots, S_k$.

Exercise 26.11. Let $\mathfrak{b}(n,\mathbb{C})$ be the set of $n \times n$ upper triangular matrices in $\mathfrak{gl}(n,\mathbb{C})$. Prove that $V = \mathbb{C}^n$ is indecomposable, not irreducible.

Definition 26.12. Let L be a Lie algebra and $f\colon V \to W$ be a map. We say that f is an L-module **homomorphism** if $f(xv) = xf(v)$ for all $x \in L$ and $v \in V$.

As usual, an isomorphism is a bijective module homomorphism.

Exercise 26.13. State and prove the isomorphism theorems for modules over Lie algebras.

Exercise 26.14 (Schur lemma). Let L be a Lie algebra.

1) Let S and T be simple L-modules. Prove that a non-zero homomorphism $f\colon S \to T$ is an isomorphism.
2) Let S be a finite-dimensional simple L-module. Prove that if $f\colon S \to S$ is a homomorphism, then $f = \lambda\,\mathrm{id}$ for some $\lambda \in \mathbb{C}$.

As an example, if V is a simple module, then z acts by scalar multiplication on V, that is $zv = \lambda v$ for some $\lambda \in \mathbb{C}$.

Lecture 12

§27. Representations of $\mathfrak{sl}(2,\mathbb{C})$

We discuss a particular important Lie algebra:

$$\mathfrak{sl}(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a,b,c \in \mathbb{C} \right\}.$$

Note that $e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and $f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ is an ordered basis for $\mathfrak{sl}(2,\mathbb{C})$. In this basis,

$$[h,e] = 2e, \quad [h.f] = -2f, \quad [e,f] = h.$$

Let V be an $\mathfrak{sl}(2,\mathbb{C})$-module. Note that we do not assume that V is simple. For $\lambda \in \mathbb{C}$ an eigenvector of h let

$$V_\lambda = \{v \in V : h \cdot v = \lambda v\}$$

be the **weight space** of λ. If λ is not an eigenvector of h, we set $V_\lambda = \{0\}$. A **weight** of V is a scalar λ such that $V_\lambda \neq \{0\}$.

Lemma 27.1. *Let V be an $\mathfrak{sl}(2,\mathbb{C})$-module and $v \in V_\lambda$.*

1) *Either $e \cdot v = 0$ or $e \cdot v$ is an eigenvector of h with eigenvalue $\lambda + 2$.*
2) *Either $f \cdot v = 0$ or $f \cdot v$ is an eigenvector of h with eigenvalue $\lambda - 2$.*

Proof. We only prove 1):

$$h \cdot (e \cdot v) = e \cdot (h \cdot v) + [h,e] \cdot v = e \cdot (\lambda v) + 2e \cdot v = (\lambda + 2) e \cdot v. \qquad \square$$

Lemma 27.2. *Let V be a finite-dimensional $\mathfrak{sl}(2,\mathbb{C})$-module. There exists an eigenvector $w \in V$ of h such that $e \cdot w = 0$.*

Proof. The linear map $h \colon V \to V$ has at least one eigenvector v with eigenvalue λ. If the elements $v, e \cdot v, e^2 \cdot v, \ldots$ are non-zero, they are linearly independent, as they

form a sequence of eigenvectors of h with different eigenvalues. As $\dim V < \infty$, it follows that there exists k such that $e^k \cdot v \neq 0$ and $e^{k+1} \cdot v = 0$. Let $w = e^k \cdot v \neq 0$. Then $h \cdot w = (\lambda + 2k) \cdot w$ and $e \cdot w = 0$. □

A vector $v \in V$ such that $V_\lambda \neq \{0\}$ and $V_{\lambda+2} = \{0\}$ will be called a **highest weight vector** of weight λ.

Lemma 27.3. *Let V be a finite-dimensional simple $\mathfrak{sl}(2,\mathbb{C})$-module and let w be a maximal vector of weight λ. Let k be such that $f^k \cdot w \neq 0$ and $f^{k+1} \cdot w = 0$. Then $\{w, f \cdot w, \ldots, f^k \cdot w\}$ is a basis of V. Moreover, $\lambda = k$.*

Proof. The elements $w, f \cdot w, \ldots, f^k \cdot w$ are linearly independent, as they are eigenvectors of h with different eigenvalues. Since V is simple, it is enough to prove that the non-zero subspace $W = \langle w, f \cdot w, \ldots, f^k \cdot w \rangle$ is a submodule of V. This subspace is invariant under the action of h and f. In fact, one easily proves by induction that

$$(hf^j) \cdot w = (\lambda - 2j) f^j w$$

for all $j \geq 0$. Let us prove that W is invariant under the action of e, that is $e \cdot W \subseteq W$. We claim that

$$(ef^j) \cdot w = j(\lambda - j + 1) f^{j-1} w \in W$$

for all j. We proceed by induction on j. Note that the case $j = 0$ is trivial, as $e \cdot w = 0$. The case $j = 1$ is easy:

$$(ef) \cdot w = (h + fe) \cdot w = h \cdot w + f \cdot (e \cdot w) = \lambda w.$$

If the claim holds for some j, by using the inductive hypothesis,

$$\begin{aligned} e \cdot (f^{j+1} \cdot w) &= (ef) \cdot (f^j \cdot w) \\ &= (fe + h) \cdot (f^j \cdot w) \\ &= h \cdot (f^j \cdot w) + j(\lambda - j + 1)(f^j \cdot w) \\ &= (j+1)(\lambda - j)(f^j \cdot w). \end{aligned}$$

We now compute λ. The matrix of h with respect to the basis $\{w, f \cdot w, \ldots, f^k \cdot w\}$ is diagonal with trace

$$\lambda + (\lambda - 2) + \cdots + (\lambda - 2k) = (k+1)(\lambda - k).$$

Since $[e, f] = h$ has trace zero, it follows that $\lambda = k$. □

We now summarize what we know about simple $\mathfrak{sl}(2,\mathbb{C})$-modules.

Theorem 27.4. *Let V be a finite-dimensional simple $\mathfrak{sl}(2,\mathbb{C})$-module. Then V is the direct sum of one-dimensional weight spaces*

$$V = V_\lambda \oplus V_{\lambda-2} \oplus \cdots \oplus V_{-\lambda+2} \oplus V_{-\lambda}. \tag{12.1}$$

In particular, $\dim V = \lambda + 1$. *The set* $\{w, f\cdot w, \dots, f^{\lambda}\cdot w\}$ *is a basis of* V *and*

$$\begin{aligned} h\cdot(f^j\cdot w) &= (\lambda - 2j) f^j\cdot w,\\ f\cdot(f^j\cdot w) &= f^{j+1}\cdot w,\\ e\cdot(f^j\cdot w) &= j(\lambda - j + 1) f^{j-1}\cdot w. \end{aligned} \tag{12.2}$$

Proof. By Lemma 27.2, there exists an eigenvector w of h with eigenvalue λ such that $e\cdot w = 0$. By Lemma 27.3, the set $\{w, f\cdot w, \dots, f^k\cdot w\}$ is a basis of V and the formulas of (12.2) follow. For $j \in \{0,\dots,k\}$ the complex vector space generated by $f^j\cdot w$ is a one-dimensional weight space of weight $\lambda - 2j$. Thus (12.1) follows. □

Exercise 27.5. Prove that two finite-dimensional $\mathfrak{sl}(2,\mathbb{C})$ generated by highest weight vectors of the same weight are isomorphic.

Consider the polynomial ring $\mathbb{C}[X,Y]$ in two commuting variables X and Y. Let V_d be the subspace of homogeneous polynomials of degree d. Then

$$\dim V_d = \begin{cases} 1 & \text{if } d = 0,\\ d+1 & \text{otherwise,} \end{cases}$$

as a basis of V_d is given by $\{X^d, X^{d-1}Y, X^{d-2}Y^2, \dots, XY^{d-1}, Y^d\}$.

Exercise 27.6. Prove that $\varphi\colon \mathfrak{sl}(2,\mathbb{C}) \to \mathfrak{gl}(V_d)$,

$$\varphi(e) = X\frac{\partial}{\partial Y}, \qquad \varphi(f) = Y\frac{\partial}{\partial X}, \qquad \varphi(h) = X\frac{\partial}{\partial X} - Y\frac{\partial}{\partial Y}, \tag{12.3}$$

is a representation of $\mathfrak{sl}(2,\mathbb{C})$. This means that

$$\varphi(e)(X^aY^b) = bX^{a+1}Y^{b-1}, \quad \varphi(f)(X^aY^b) = aX^{a-1}Y^{b+1},$$

and that

$$\varphi(h)(X^aY^b) = (a-b)X^aY^b.$$

In the basis $\{X^d, X^{d-1}Y, X^{d-2}Y^2, \dots, XY^{d-1}, Y^d\}$,

$$\varphi(e) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0\\ 0 & 0 & 2 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & d\\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad \varphi(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0\\ d & 0 & \cdots & 0 & 0\\ 0 & d-1 & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad \varphi(h) = \begin{pmatrix} d & 0 & \cdots & 0 & 0\\ 0 & d-2 & \cdots & 0 & 0\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \cdots & -d+2 & 0\\ 0 & 0 & \cdots & 0 & -d \end{pmatrix}.$$

Exercise 27.7. Prove that V_d is generated (as an $\mathfrak{sl}(2,\mathbb{C})$-module) by X^aY^b for some a and b such that $a + b = d$.

Exercise 27.8. Prove that each V_d is a simple $\mathfrak{sl}(2,\mathbb{C})$-module.

Exercise 27.9. Prove that any V finite-dimensional simple $\mathfrak{sl}(2,\mathbb{C})$-module is isomorphic to V_d for some d.

The following result is a particular case of Weyl's theorem in the context of $\mathfrak{sl}(2,\mathbb{C})$-modules.

Theorem 27.10. *Any finite-dimensional $\mathfrak{sl}(2,\mathbb{C})$-module is absolutely reducible.*

Proof. Let V be a finite-dimensional $\mathfrak{sl}(2,\mathbb{C})$-module. We proceed in several steps.

Claim. The elmenet $Z = \frac{1}{2}h^2 + h + 2fe$ commutes with every $X \in \mathfrak{sl}(2,\mathbb{C})$.

We first compute

$$\begin{aligned} ZX - XZ &= \frac{1}{2}h^2X - \frac{1}{2}Xh^2 + [h,X] + 2feX - 2Xfe \\ &= \frac{1}{2}h[e,X] - \frac{1}{2}[X,h]h + [h,X] + 2f[e,X] - 2[X,f]e. \end{aligned} \tag{12.4}$$

Now one checks that Equation (12.4) is zero if $X \in \{h,e,f\}$ and the claim follows.

Claim. If $\dim V = n+1$, then Z acts as the scalar $\frac{1}{2}n^2 + n$, which is not zero unless V is the trivial module.

By Schur's lemma, Z acts by a scalar. Since V is a simple $\mathfrak{sl}(2,\mathbb{C})$-module of dimension $n+1$, $V \simeq V_{n+1}$. In particular, $hv_0 = nv_0$ and $ev_0 = 0$.

Claim. Let $U \subseteq V$ be a submodule of codimension one. Then there exists a submodule W of V such that $V = U \oplus W$ and $\dim W = 1$.

We split the proof of the claim into several steps.

First we assume that $\dim U = 1$. The quotient module V/U is one-dimensional and hence simple. Thus $\mathfrak{sl}(2,\mathbb{C})V \subseteq U$ and $\mathfrak{sl}(2,\mathbb{C})U = \{0\}$. Hence

$$[X,Y]V \subseteq XYV - YXV \subseteq XU + YU = \{0\}.$$

Since $\mathfrak{sl}(2,\mathbb{C}) = [\mathfrak{sl}(2,\mathbb{C}), \mathfrak{sl}(2,\mathbb{C})]$, we conclude that $\mathfrak{sl}(2,\mathbb{C})V = \{0\}$. Thus any complement of U will serve as W.

We now finish the proof of the theorem. □

§28. Enveloping algebras

Let L be a finite-dimensional Lie algebra with basis $\{x_1,\dots,x_n\}$. Write

$$[x_i,x_j] = \sum_{k=1}^{n} c_{ij}^k x_k$$

for scalars $c_{ij}^k \in \mathbb{C}$. These scalars are called the **structure constants** of L.

The **universal enveloping algebra** of L is the associative algebra $U(L)$ with generators $x_1, \dots, x_n$ and relations

$$x_i x_j - x_j x_i = \sum_{k=1}^{n} c_{ij}^k x_k.$$

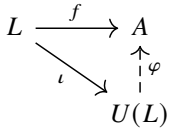
Our definition depends on the choice of the basis of the Lie algebra L. However, it is possible to define $U(L)$ as the quotient of the tensor algebra $T(L)$ by the ideal I generated by $x \otimes y - y \otimes x - [x, y]$ for all $x, y \in L$.

Example 28.1. If L is an abelian Lie algebra, then $U(L)$ is the symmetric algebra $S(L)$.

Example 28.2. The universal enveloping algebra $U(\mathfrak{sl}(2, \mathbb{C}))$ is the algebra with generators e, f, h and relations

$$ef - fe = h, \quad hf - fh = -2f, \quad he - eh = 2e.$$

The universal enveloping algebra satisfies a *universal property*. Let L be a Lie algebra. If A is an associative algebra, then A has the structure of a Lie algebra with bracket $[a, b] = ab - ba$. If $f\colon L \to A$ is a homomorphism of Lie algebras, then there exists a unique algebra homomorphism $\varphi\colon U(L) \to A$ such that



commutes, where $\iota\colon L \to U(L)$ denotes the canonical map.

Theorem 28.3 (Poincaré–Birkhoff–Witt). *Let L be a finite-dimensional Lie algebra and $\{x_1, \dots, x_n\}$ be an ordered basis of L. Then*

$$\{x_1^{a_1} \cdots x_n^{a_n} : a_1, \dots, a_n \geq 0\}$$

is a basis of $U(L)$.

See for example [19, §17.4].

Exercise 28.4. Let L be a finite-dimensional Lie algebra and $U(L)$ be its universal enveloping algebra. Prove that there exists a bijective correspondence between (simple) L-modules and (simple) $U(L)$-modules.

Additional topics

§29. More on induction and restriction

Restriction and induction of modules

Definition 29.1. Let G be a finite group. If U is a $\mathbb{C}[G]$-module and H is a subgroup of G, then U is a $\mathbb{C}[H]$-module by restricting to the action of H. This module will be denoted by $\operatorname{Res}^G_H U$. It will be called the **restriction** of U to H.

The restriction of a simple module may not be a simple module.

Example 29.2. Let $G = \mathbb{D}_4 = \langle r, s : r^4 = s^2 = 1, srs = r^{-1}\rangle$ be the dihedral group of eight elements and V be a vector space with basis $\{v_1, v_2\}$. Then V is a $\mathbb{C}[\mathbb{D}_4]$-module with

$$r \cdot v_1 = v_2, \quad r \cdot v_2 = -v_1, \quad s \cdot v_1 = v_1, \quad s \cdot v_2 = -v_2.$$

The character of V is

$$\chi(g) = \begin{cases} 2 & \text{si } g = 1, \\ -2 & \text{si } g = r^2, \\ 0 & \text{en otro caso.} \end{cases}$$

Note that χ is irreducible, as $\langle \chi, \rangle \chi = 1$. Let $H = \langle r^2, s\rangle = \{1, r^2, s, r^2 s\}$. Then $\operatorname{Res}^G_H V$ is V as a vector space with the structure of $\mathbb{C}[H]$-module given by

$$r^2 \cdot v_1 = -v_1, \quad r^2 \cdot v_2 = -v_1, \quad s \cdot v_1 = -v_1, \quad s \cdot v_2 = -v_2.$$

The character of $\operatorname{Res}^G_H V$ is

$$\chi_H(h) = \chi|_H(h) = \begin{cases} 2 & \text{if } h = 1, \\ -2 & \text{if } h = r^2, \\ 0 & \text{otherwise.} \end{cases}$$

The character χ_H is not irreducible, as $\langle \chi_H, \chi_H \rangle = 0$.

Let G be a finite group and H be a subgroup of G. Write $\mathrm{Irr}(H) = \{\phi_1, \ldots, \phi_l\}$. If $\chi \in \mathrm{Char}(G)$, then

$$\chi|_H = \sum_{i=1}^{l} d_i \phi_i$$

for integers $d_1, \ldots, d_l \geq 0$. Each ϕ_i with $d_i = \langle \chi|_H, \phi_i \rangle \neq 0$ is an **irreducible component** of $\chi|_H$ and these ϕ_i's are the **irreducible components** of $\chi|_H$.

Proposition 29.3. *Let G be a finite group. If H is a subgroup of G and $\phi \in \mathrm{Char}(H)$, then $\chi \in \mathrm{Irr}(G)$ is such that $\langle \chi|_H, \phi \rangle_H \neq 0$.*

Proof. Assume that $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$. If L is the regular representation of G, then

$$\chi_L(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Write $\chi_L = \sum_{i=1}^{k} \chi_i(1)\chi_i$. Since

$$0 \neq \frac{|G|}{|H|}\phi(1) = \langle \chi_L|_H, \phi \rangle_H = \sum_{i=1}^{k} \chi_i(1) \langle \chi_i|_H, \phi \rangle_H,$$

there exists $i \in \{1, \ldots, k\}$ such that $\langle \chi_i|_H, \phi \rangle_H \neq 0$. □

Proposition 29.4. *Let G be a group, $\chi \in \mathrm{Irr}(G)$ and H be a subgroup of G. If $\mathrm{Irr}(H) = \{\phi_1, \ldots, \phi_l\}$, then*

$$\chi|_H = \sum_{i=1}^{l} d_i \phi_i,$$

where $\sum_{i=1}^{l} d_i^2 \leq (G : H)$. Moreover,

$$\sum_{i=1}^{l} d_i^2 = (G : H) \iff \chi(g) = 0 \text{ para todo } g \in G \setminus H.$$

Proof. Since

$$\sum_{i=1}^{l} d_i^2 = \langle \chi|_H, \chi|_H \rangle_H = \frac{1}{|H|} \sum_{h \in H} \chi(h)\overline{\chi(h)}.$$

Since χ is irreducible,

$$
\begin{aligned}
1 = \langle \chi, \chi \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\chi(g)} \\
&= \frac{1}{|G|} \sum_{h \in H} \chi(h)\overline{\chi(h)} + \frac{1}{|G|} \sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)} \\
&= \frac{|H|}{|G|} \sum_{i=1}^{l} d_i^2 + \frac{1}{|G|} \sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)}.
\end{aligned}
$$

Since $\sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)} \geq 0$, it follows that $\sum_{i=1}^{l} d_i^2 \leq (G : H)$. Moreover, the equality holds if and only if $\sum_{g \in G \setminus H} \chi(g)\overline{\chi(g)} = 0$, that is, if and only if $\chi(g) = 0$ for all $g \in G \setminus H$. □

Discutiremos ahora la inducción de módulos. Para eso, repasaremos algunas nociones básicas sobre **bimódulos** y **producto tensorial de bimódulos**. Si R y S son anillos, un grupo abeliano M se dirá un (R, S)-bimódulo si M es un R-módulo a izquierda, M es un S-módulo a derecha y además

$$r \cdot (m \cdot s) = (r \cdot m) \cdot s$$

para todo $r \in R$, $s \in S$ y $m \in M$.

Examples 29.5.

1) Un R-módulo a izquierda es un $(R, \mathbb{Z})$-bimódulo.
2) Un S-módulo a derecha es un $(\mathbb{Z}, S)$-bimódulo.
3) Todo anillo R es un (R, R)-bimódulo.

Example 29.6. Si M es un (R, S)-bimódulo y N es un R-módulo, entonces el conjunto $\mathrm{Hom}_R(M, N)$ de morfismos de R-módulos $M \to N$ es un S-módulo con

$$(s \cdot \varphi)(m) = \varphi(m \cdot s), \quad s \in S, \varphi \in \mathrm{Hom}_R(M, N), m \in M.$$

Sean M un (R, S)-bimódulo, N un S-módulo y U un R-módulo. Diremos que una función $f \colon M \times N \to U$ es **balanceada** si

$$
\begin{aligned}
f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \\
f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \\
f(m \cdot s, n) &= f(m, s \cdot n), \\
f(r \cdot m, n) &= r \cdot f(m, n)
\end{aligned}
$$

para todo $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $r \in R$ y $s \in S$.

Example 29.7. Si M es un R-módulo, la función $f \colon R \times M \to M$, $(r, m) \mapsto r \cdot m$, es balanceada.

Sean M un (R, S)-bimódulo, N un S-módulo y U un R-módulo. Se define el **producto tensorial** $M \otimes_S N$ es un R-módulo provisto con una función balanceada $\eta \colon M \times N \to M \otimes_S N$ que cumple con la siguiente propiedad universal:

Si $f : M \times N \to U$ es una función balanceada, entonces existe un único morfismo de R-módulos $\alpha\colon M \otimes_S N \to U$ tal que $f = \alpha \circ \eta$.

Notación: $m \otimes n = \eta(m,n)$ para $m \in M$ y $n \in N$. El producto tensorial existe y puede demostrarse que es único salvo isomorfismos. Más precisamente, $M \otimes_S N$ se define como el R-módulo generado por el conjunto $\{m \otimes n : m \in M, n \in N\}$, donde los $m \otimes n$ satisfacen las siguientes identidades:

$$(m+m_1) \otimes n = m \otimes n + m_1 \otimes n \qquad m, m_1 \in M, n \in N, \tag{12.5}$$

$$m \otimes (n+n_1) = m \otimes n + m \otimes n_1 \qquad m \in M, n, n_1 \in N, \tag{12.6}$$

$$(ms) \otimes n = m \otimes (sn) \qquad m \in M, n \in N, s \in S, \tag{12.7}$$

$$(rm) \otimes n = r(m \otimes n) \qquad m \in M, n \in N, r \in R. \tag{12.8}$$

Un elemento arbitrario de $M \otimes_S N$ es una suma finita de la forma $\sum_{i=1}^{k} m_i \otimes n_i$, donde $m_1, \ldots, m_k \in M$ y $n_1, \ldots, n_k \in N$, y no necesariamente un tensor elemental $m \otimes n$.

Example 29.8. $M \simeq R \otimes_R M$ como R-módulos. Como la función $R \times M \to M$, $(r,m) \mapsto r \cdot m$, es balanceada, induce un morfismo $R \otimes_R M \to M$, $r \otimes m \mapsto r \cdot m$ con inversa $M \to R \otimes_R M$, $m \mapsto 1 \otimes m$.

Example 29.9. Si $M_1, \ldots, M_k$ son (R,S)-bimódulos y N es un S-módulo, entonces

$$(M_1 \oplus \cdots \oplus M_k) \otimes_S N \simeq (M_1 \otimes_S N) \oplus \cdots \oplus (M_k \otimes_S N).$$

Algunos ejercicios:

Exercise 29.10. Demuestre que $M \otimes_R N \simeq N \otimes_{R^{\mathrm{op}}} M$.

Exercise 29.11. Demuestre que $\mathbb{Z}/n \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}$.

Exercise 29.12. Sean M un (R,S)-bimódulo y N un (S,T)-bimódulo. Demuestre que $M \otimes_S N$ es un (R,T)-bimódulo con $r(m \otimes n)t = (rm) \otimes (nt)$, donde $m \in M$, $n \in N$, $r \in R$, $t \in T$.

Exercise 29.13. Demuestre que $(M \otimes_R N) \otimes_R T \simeq M \otimes_R (N \otimes_R T)$.

Exercise 29.14. Enuncie y demuestre la asociatividad del producto tensorial de bimódulos.

Si G es un grupo finito, H es un subgrupo de G y V es un $K[H]$-módulo, entonces $K[G]$ es un $(K[G], K[H])$-bimódulo.

Definition 29.15. Sea G un grupo finito y sea H un subgrupo de G. Si V es un $K[H]$-módulo de G, se define el $K[G]$-módulo **inducido** de V como

$$\mathrm{Ind}_H^G V = K[G] \otimes_{K[H]} V.$$

Si H es un subgrupo de G, un **transversal** (a izquierda) de H en G es un subconjunto T de G que contiene exactamente un elemento de cada coclase (a izquierda) de H en G.

Example 29.16. Si $G = \mathbb{S}_3$ y $H = \{\mathrm{id}, (12)\}$, entonces $T = \{\mathrm{id}, (123), (23)\}$ es un transversal de H en G. Podemos descomponer a G como

$$G = \{\mathrm{id}, (12)\} \cup \{(123), (13)\} \cup \{(132), (23)\} = \bigcup_{t \in T} tH.$$

Como cada $g \in G$ se escribe en forma única como $g = th$ para $t \in T$ y $h \in H$, podemos definir una transformación lineal $\varphi\colon K[G] \to K[H] \oplus K[H] \oplus K[H] = |T|K[H]$, que para $g = th$ devuelve h en el lugar que corresponde a $t \in T$, es decir

$$\begin{aligned} \mathrm{id} &\mapsto (\mathrm{id}, 0, 0), & (12) &\mapsto ((12), 0, 0), & (123) &\mapsto (0, \mathrm{id}, 0), \\ (23) &\mapsto (0, 0, \mathrm{id}), & (13) &\mapsto (0, (12), 0), & (132) &\mapsto (0, 0, (12)). \end{aligned}$$

Por ejemplo,

$$\varphi(5(12) - 3(123) + 7\,\mathrm{id}) = (7\,\mathrm{id} + 5(12), -3\,\mathrm{id}, 0).$$

Es importante observar que φ es un isomorfismo de $K[H]$-módulos (a derecha).

La observación hecha en el ejemplo anterior es la clave del siguiente resultado.

Proposition 29.17. *Sea G un grupo finito y sea H un subgrupo de G. Si V es un $K[H]$-módulo de G, entonces*

$$\mathrm{Ind}_H^G(V) = \bigoplus_{t \in T} t \otimes V,$$

donde T es un transversal de H en G y $t \otimes V = \{t \otimes v : v \in V\}$. En particular, $\dim \mathrm{Ind}_H^G V = (G : H) \dim V$.

Proof. Descomponemos a G como unión disjunta de coclases de H con el transversal T, es decir

$$G = \bigcup_{t \in T} tH.$$

Cada $g \in G$ se escribe entonces unívocamente como $g = th$ con $t \in T$ y $h \in H$. Tal como hicimos en el ejemplo anterior, esto nos permite obtener un isomorfismo $\varphi\colon K[G] \to |T|K[H]$ de $K[H]$-módulos (a derecha), donde $\varphi(g)$ es h en el sumando que corresponde a $t \in T$ y es cero en el resto de los sumandos. Luego

$$\mathrm{Ind}_H^G V = K[G] \otimes_{K[H]} V \simeq (|T|K[H]) \otimes_{K[H]} V \simeq |T|(K[H] \otimes_{K[H]} V) \simeq |T|V$$

como $K[H]$-módulos. En particular, $\dim \mathrm{Ind}_H^G V = |T| \dim V$.

Si escribimos $g = th$ con $t \in T$ y $h \in H$, entonces $g \otimes v = (th) \otimes v = t \otimes h \cdot v \in t \otimes V$. Luego $K[G] \otimes_{K[H]} V \subseteq \oplus_{t \in T} t \otimes V$. La otra inclusión es trivial. Por definición, la suma sobre $t \in T$ de los $t \otimes V$ es directa. □

Theorem 29.18 (Reciprocidad de Frobenius). *Sea G un grupo finito y H un subgrupo de G. Si U es un $K[G]$-módulo y V es un $K[H]$-módulo, entonces*

$$\mathrm{Hom}_{K[H]}(V, \mathrm{Res}^G_H U) \simeq \mathrm{Hom}_{K[G]}(\mathrm{Ind}^G_H V, U)$$

como espacios vectoriales.

Proof. Si $\varphi \in \mathrm{Hom}_{K[H]}(V, \mathrm{Res}^G_H U)$, sea

$$f_\varphi \colon K[G] \times V \to U, \quad (g, v) \mapsto g \cdot \varphi(v).$$

Veamos que f_φ es balanceada. Un cálculo directo muestra que

$$f_\varphi(g + g_1, v) = f_\varphi(g, v) + f_\varphi(g_1, v), \qquad f_\varphi(g, v + w) = f_\varphi(g, v) + f_\varphi(g, w).$$

Como φ es morfismo de $K[H]$-módulos,

$$f_\varphi(gh, v) = (gh) \cdot \varphi(v) = g \cdot (h \cdot \varphi(v)) = g \cdot (h \cdot \varphi(v)) = g \cdot \varphi(h \cdot v) = f_\varphi(g, h \cdot v)$$

para todo $g \in G$, $h \in H$ y $v \in V$. Por último,

$$f_\varphi(gg_1, v) = (gg_1) \cdot \varphi(v) = g \cdot (g_1 \cdot \varphi(v)) = g \cdot f_\varphi(g_1, v)$$

para todo $g, g_1 \in G$ y $v \in V$. Para cada $\varphi \in \mathrm{Hom}_{K[H]}(V, \mathrm{Res}^G_H U)$ tenemos entonces un $\Gamma(\varphi) \in \mathrm{Hom}_{K[G]}(\mathrm{Ind}^G_H V, U)$ tal que $\Gamma(\varphi)(g \otimes v) = g \cdot \varphi(v)$. Tenemos así definida una función

$$\Gamma \colon \mathrm{Hom}_{K[H]}(V, \mathrm{Res}^G_H U) \to \mathrm{Hom}_{K[G]}(\mathrm{Ind}^G_H V, U), \quad \varphi \mapsto \Gamma(\varphi).$$

La función Γ es lineal e inyectiva, ambas afirmaciones fáciles de verificar.

Es también sobreyectiva, pues si $\theta \in \mathrm{Hom}_{K[H]}(\mathrm{Ind}^G_H V, U)$, entonces la función $\varphi(v) = \theta(1 \otimes v)$ es tal que $\varphi \in \mathrm{Hom}_{K[H]}(V, \mathrm{Res}^G_H U)$ y cumple

$$\Gamma(\varphi)(g \otimes v) = g \cdot \varphi(v) = g \cdot \theta(1 \otimes v) = \theta(g \otimes v). \qquad \square$$

Supongamos ahora que $K = \mathbb{C}$.

Sea H un subgrupo de G. Si U es un $\mathbb{C}[G]$-módulo con caracter χ, el caracter de $\mathrm{Res}^G_H U$ se denota por $\chi|_H$ y vale que que $\chi|_H(1) = \chi(1)$. Si V es un $\mathbb{C}[H]$-módulo con caracter ϕ, el módulo $\mathrm{Ind}^G_H V$ tiene caracter ϕ^G y vale que $\phi^G(1) = (G : H)\phi(1)$.

$$\langle \phi, \chi|_H \rangle_H = \dim \mathrm{Hom}_{\mathbb{C}[H]}(V, \mathrm{Res}^G_H U) = \dim \mathrm{Hom}_{\mathbb{C}[G]}(\mathrm{Ind}^G_H V, U) = \langle \phi^G, \chi \rangle_G,$$

donde $\langle \alpha, \beta \rangle_X = \sum_{x \in X} \alpha(x)\overline{\beta(x)}$ denota el producto interno del espacio de funciones $X \to \mathbb{C}$.

Definition 29.19. Si $\mathrm{Irr}(G) = \{\chi_1, \ldots, \chi_k\}$ e $\mathrm{Irr}(H) = \{\phi_1, \ldots, \phi_l\}$, se define la **matriz de inducción–restricción** como la matriz $(c_{ij}) \in \mathbb{C}^{l \times k}$, donde

$$c_{ij} = \langle \phi_i^G, \chi_j \rangle_G = \langle \phi_i, \chi_j|_H \rangle_H .$$

La fila i-ésima de la matriz de inducción–restricción da la multiplicidad con que el caracter χ_j aparece en la descomposición de ϕ_i^G. La columna j-ésima da la multiplicidad con que el caracter ϕ_i aparece en la descomposición de $\chi_j|H$.

Example 29.20. Sea $G = \mathbb{S}_3$. La tabla de caracteres de G es

	1	3	2
	1	(12)	(123)
χ_1	1	1	1
χ_2	1	−1	1
χ_3	2	0	−1

La tabla de caracteres del subgrupo $H = \{\mathrm{id}, (12)\}$ es

	1	1
	id	(12)
ϕ_1	1	1
ϕ_2	1	−1

A simple vista vemos que $\chi_1|_H = \phi_1$, $\chi_2|_H = \phi_2$ y que $\chi_3|_H = \phi_1 + \phi_2$. La matriz de inducción–restricción es entonces

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Observemos que además $\phi_1^G = \chi_1 + \chi_3$ y que $\phi_2^G = \chi_2 + \chi_3$.

Veamos cómo calcular explícitamente caracteres inducidos.

Proposition 29.21. *Sea H un subgrupo de G y sea V es un $\mathbb{C}[H]$-módulo con caracter χ. Si T es un trasversal de H en G, entonces*

$$\chi^G(g) = \sum_{\substack{t \in T \\ t^{-1}gt \in H}} \chi(t^{-1}gt)$$

para todo $g \in G$.

Proof. Sabemos que $\mathrm{Ind}_H^G V = \oplus_{t \in T} t \otimes V$. Supongamos que $T = \{t_1, \ldots, t_m\}$ y sea $\{v_1, \ldots, v_n\}$ una base de V. Entonces $\{t_i \otimes v_k : 1 \le i \le m, 1 \le k \le n\}$ es una base de $\mathrm{Ind}_H^G V$ y la acción de g en $\mathrm{Ind}_H^G V$ está dada por

$$\rho^G(g) = \begin{cases} \rho(t_j^{-1} g t_i) & \text{si } t_j^{-1} g t_i \in H, \\ 0 & \text{en otro caso.} \end{cases}$$

En efecto, si $gt_i = t_j h$ para $h \in H$ y ciertos i, j, entonces

$$g \cdot (t_i \otimes v_k) = gt_i \otimes v_k = t_j h \otimes v_k = t_j \otimes h \cdot v_k$$

y además $gt_i = t_j h$ si y sólo si $t_j^{-1} g t_i = h \in H$. Se concluye entones que g actúa como $t^{-1}gt$ en V en caso en que $t^{-1}gt \in H$ y como la transformación nula en otro caso. □

Corollary 29.22. *Sea H un subgrupo de G y sea V es un $\mathbb{C}[H]$-módulo con caracter χ. Si $g \in G$, entonces*

$$\chi^G(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \chi(x^{-1}gx).$$

Proof. Sea T un transversal de H en G. Si $x \in G$, escribimos $x = th$ para $t \in T$ y $h \in H$. Como $x^{-1}gx = h^{-1}(t^{-1}gt)h$, entonces $x^{-1}gx \in H \iff t^{-1}gt \in H$ y además, en ese caso, $\chi(x^{-1}gx) = \chi(t^{-1}gt)$ pues χ es una función de clases. Eso implica que existen $|H|$ elementos $x \in G$ tales que $x^{-1}gx \in H$. Para esos x, se tiene $\chi(x^{-1}gx) = \chi(t^{-1}gt)$, lo que implica el corolario. □

Some topics for final projects

We collect here some topics for final presentations. Some topics can also be used as bachelor or master theses.

Staircase groups

This topic describes a situation similar to that of §2, but more general. See [2, Chapter 5].

Solvable and nilpotent groups

The character table of a finite group detects solvability and nilpotency of groups, see [2, Chapter 6].

Kegel–Wielandt theorem

Prove Kegel–Wielandt theorem 22.11. For the proof see [3, Theorem 2.13].

The Drinfeld double of a finite group

See [26, Chapter IX] and [6, Chapter 8].

Ito's theorem

Ito's theorem generalize Frobenius' theorem (Theorem 8.1) and Schur's theorem (Theorem 8.4). The theorem states that if χ is an irreducible character of a finite group G, then $\chi(1)$ divides $(G : A)$ for every normal abelian subgroup A of G. See [34, §8.1].

Characters of $\mathbf{GL_2}(q)$ *and* $\mathbf{SL_2}(q)$

One possible topic is the character table of $\mathbf{GL}_2(q)$, see [36, §5.2]. Alternatively, one can present the character table of the group $\mathbf{SL}_2(p)$ following Humphreys's paper [18]. The character theory of $\mathbf{SL}_2(q)$ appears in [36, §5.2], see [5, Chapter 20] for details.

Representations of the symmetric group

See for example [36, §10] and [11].

Random walks on finite groups

The goal is to construct the character table or the irreducible representations of the symmetric group. The topic has connections with combinatorics and applications to voting and card shuffling. See [11, 4] and [36, §11].

Fourier analysis on finite groups

See [36, §5] for a very elementary approach and some basic applications. Other applications appear in [38].

Mackey's irreducibility criterion

It is not at all clear that induction of an irreducible character will produce an irreducible character. In fact, inducing the trivial character of the trivial subgroup to the whole group produces the regular representation, which in general is not

irreducible. Mackey found a criterion that describes when an induced character is irreducible. See [36, §8.3].

McKay's conjecture

Prove McKay's conjecture 10.1 for all sporadic simple groups. This was first proved by Wilson in [44]. Note that for some "small" sporadic simple groups this can be done with the script presented in §10. However, for several sporadic simple groups a different approach is needed. One needs to know the structure of normalizers.

Ore's conjecture

Prove Ore's conjecture 12.1 for alternating simple groups, see for example [33]. It is also interesting to prove the conjecture for other "small" simple groups such as $\mathbf{PSL}(3,2)$.

An elementary proof of Brauer–Fowler theorem

We need to find a subgroup of index $\leq 2n^2$. Let X be the conjugacy class of x. For $g \in G$ let

$$J(g) = \{z \in X : zgz^{-1} = g^{-1}\}.$$

We claim that $|J(g)| \leq |C_G(g)|$. The map $J(g) \to C_G(g)$, $z \mapsto gz$, is well-defined, as

$$(gz)g(gz)^{-1} = g(xgx^{-1})g^{-1} = g^{-1} \in C_G(g).$$

It is injective, as $gz = gz_1$ implies $z = z_1$.

Let $\{(g,z) \in G \times X : zgz^{-1} = g^{-1}\}$. Since $X \times X \to J$, $(y,z) \mapsto (yz,z)$, is well-defined (since $z(yz)z^{-1} = zy = (yz)^{-1}$) and it is trivially injective,

$$|X|^2 \leq |J| = \sum_{(g,z)\in J} 1 \leq \sum_{g\in G} |J(g)| = \sum_{g\in G} |C_G(g)| = k|G|,$$

where k is the number of conjugacy classes of G, as $(g,z) \in J$ if and only if $z \in J(g)$. Thus $|G| \leq kn^2$, as

$$\left(\frac{|G|}{|C_G(x)|}\right)^2 = |X|^2 = \frac{|G|}{n^2} \leq k|G|.$$

Claim. There exists a conjugacy class with $\leq 2n^2$ elements.

Assume that the claim is not true. Let $C_1, \ldots, C_k$ be the conjugacy classes of G, where $C_1 = \{1\}$ and $|C_i| > 2n^2$ for all $i \in \{2, \ldots, k\}$. Then

$$|G| = 1 + \sum_{i=2}^{k} |C_i| > 1 + \sum_{i=2}^{k} n^2 = 1 + (k-1)2n^2 \geq |G|,$$

a contradiction.

Claim. There exists a subgroup H of G such that $(G : H) \leq 2n^2$.

Let C be a conjugacy class of G such that $|C| \leq 2n^2$. Let $g \in C$. Then $H = C_G(g)$ is a subgroup of G such that $(G : H) \leq 2n^2$. This finishes the proof of the Brauer–Fowler theorem.

Hirsh's theorem

In [17] Hirsch found a generalization of Burnside's Theorem 21.7. If G is a finite group and d is the greatest common divisor of all the numbers $p^2 - 1$, where the p's are prime divisors of $|G|$ and r the number of conjugate sets in G. Then

$$|G| \equiv \begin{cases} r \bmod 2d & \text{if } |G| \text{ odd,} \\ r \bmod 3 & \text{if } |G| \text{ even and } \gcd(|G|, 3) = 1. \end{cases}$$

The proof is elementary, does not use character theory. Is it possible to prove Hirsch's theorem using characters?

Poincaré–Birkhoff–Witt theorem

There are several proofs of the Poincaré–Birkhoff–Witt theorem 28.3, see for example [19, §17.4] or [27, Theorem 2.17]. Bergman's proof based on the diamond lemma appears in [4].

Weyl's theorem

Weyl's theorem states that every finite-dimensional module over a semisimple Lie algebra is completely irreducible. See [7, Theorem 17.4] for a proof.

Irreducible representations of $U_q(\mathfrak{sl}(2,\mathbb{C}))$

Let $q \in \mathbb{C} \setminus \{0, 1, -1\}$. Let $U_q(\mathfrak{sl}(2))$ be the (complex) algebra generated by variables E, F, K and K^{-1} with relations

$$KK^{-1} = K^{-1}K = 1, \qquad KEK^{-1} = q^2E,$$
$$KFK^{-1} = q^{-2}F, \qquad [E, F] = \frac{1}{(q - q^{-1})}(K - K^{-1}).$$

This algebra is a *deformation* of the enveloping algebra of $\mathfrak{sl}(2, \mathbb{C})$. The goal is to study the representation theory of $U_q(\mathfrak{sl}(2))$. This splits into two cases, depending on whether q is a root of one or not. Finite-dimensional simple $U_q(\mathfrak{sl}(2))$-modules are studied in [26, VI]. In particular, if q is not a root of one, finite-dimensional simple $U_q(\mathfrak{sl}(2))$-modules are classified in [26, Theorem VI.3.5].

Semisimple modules of $U_q(\mathfrak{sl}(2,\mathbb{C}))$

Prove that if q is not a root of one, any finite-dimensional $U_q(\mathfrak{sl}(2))$-module is semisimple. See [26, Theorem VII.2.2].

Some solutions

4.18 Assume that ϕ is not irreducible. There exists a proper non-zero G-invariant subspace W of V. Thus $\dim W = 1$. Let $w \in W \setminus \{0\}$. For each $g \in G$, $\phi_g(w) \in W$. Thus $\phi_g(w) = \lambda w$ for some λ. This means that w is a common eigenvector for all the ϕ_g. Conversely, if ϕ admits a common eigenvector $v \in V$, then the subspace generated by v is G-invariant.

14.7 If $\mathrm{cp}(G) > 5/8$, then $|[G,G]| < 2$. Thus $[G,G]$ is the trivial group and hence G is abelian.

14.8

1) If $\mathrm{cp}(G) > 1/2$, then $|[G,G]| < 3$ by Theorem 14.6. If $|[G,G]| = 1$, then G is abelian and hence G is nilpotent. If $|[G,G]| = 2$, then $[G,G] \subseteq Z(G)$. It follows that $G/Z(G)$ is abelian (and hence nilpotent), so G is nilpotent.

2) If $\mathrm{cp}(G) < 21/80$, then $|[G,G]| < 60$. Thus $[G,G]$ is solvable, as groups of order < 60 are solvable. Hence G is solvable.

14.10

1)

2) Using that σ and τ are automorphisms and the commutativity of the diagram (7.2), we compute

$$
\begin{aligned}
(G : Z(G))^2 \operatorname{cp}(G) &= \frac{1}{|Z(G)|^2} |\{(x, y) \in G \times G : xy = yx\}| \\
&= \frac{1}{|Z(G)|^2} |\{(x, y) \in G \times G : [x, y] = 1\}| \\
&= \frac{1}{|Z(G)|^2} |\{(x, y) \in G \times G : c_G(x, y) = 1\}| \\
&= |\{(u, v) \in (G/Z(G))^2 : c_G(u, v) = 1\}| \\
&= |\{(u, v) \in (G/Z(G))^2 : \tau c_G(u, v) = 1\}| \\
&= |\{(u, v) \in (G/Z(G))^2 : c_G(\sigma u, \sigma v) = 1\}| \\
&= |\{(a, b) \in (H/Z(H))^2 : c_H(a, b) = 1\}|.
\end{aligned}
$$

It follows that $(G : Z(G))^2 \operatorname{cp}(G) = (H : Z(G))^2 \operatorname{cp}(H)$.

References

1. J. L. Alperin. The main problem of block theory. In *Proceedings of the Conference on Finite Groups (Univ. Utah, Park City, Utah, 1975)*, pages 341–356, 1976.
2. J. L. Alperin and R. B. Bell. *Groups and representations*, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
3. B. Amberg, S. Franciosi, and F. de Giovanni. *Products of groups*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1992. Oxford Science Publications.
4. G. M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.
5. Y. G. Berkovich and E. M. Zhmud′. *Characters of finite groups. Part 2*, volume 181 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1999. Translated from the Russian manuscript by P. Shumyatsky [P. V. Shumyatskiĭ], V. Zobina and Berkovich.
6. M. Broué. *On characters of finite groups*. Mathematical Lectures from Peking University. Springer, Singapore, 2017.
7. K. Erdmann and M. J. Wildon. *Introduction to Lie algebras*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 2006.
8. B. Fein, W. M. Kantor, and M. Schacher. Relative Brauer groups. II. *J. Reine Angew. Math.*, 328:39–57, 1981.
9. W. Feit and J. G. Thompson. Solvability of groups of odd order. *Pacific J. Math.*, 13:775–1029, 1963.
10. P. Flavell. Finite groups in which every two elements generate a soluble subgroup. *Invent. Math.*, 121(2):279–285, 1995.
11. W. Fulton and J. Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.
12. G. Gonthier, A. Asperti, J. Avigad, and et al. A machine-checked proof of the odd order theorem. In *Interactive theorem proving*, volume 7998 of *Lecture Notes in Comput. Sci.*, pages 163–179. Springer, Heidelberg, 2013.
13. R. Guralnick and D. Wan. Bounds for fixed point free elements in a transitive group and applications to curves over finite fields. *Israel J. Math.*, 101:255–287, 1997.
14. R. M. Guralnick, M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep. Surjective word maps and Burnside's $p^a q^b$ theorem. *Invent. Math.*, 213(2):589–695, 2018.
15. R. M. Guralnick and G. R. Robinson. On the commuting probability in finite groups. *J. Algebra*, 300(2):509–528, 2006.
16. R. M. Guralnick and J. S. Wilson. The probability of generating a finite soluble group. *Proc. London Math. Soc. (3)*, 81(2):405–427, 2000.
17. K. A. Hirsch. On a theorem of Burnside. *Quart. J. Math. Oxford Ser. (2)*, 1:97–99, 1950.
18. J. E. Humphreys. Representations of $\mathrm{SL}(2, p)$. *Amer. Math. Monthly*, 82:21–39, 1975.

19. J. E. Humphreys. *Introduction to Lie algebras and representation theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1978. Second printing, revised.
20. I. M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.*, 95:594–635, 1973.
21. I. M. Isaacs. *Character theory of finite groups*. AMS Chelsea Publishing, Providence, RI, 2006. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].
22. I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.
23. I. M. Isaacs. *Characters of solvable groups*, volume 189 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.
24. I. M. Isaacs, G. Malle, and G. Navarro. A reduction theorem for the McKay conjecture. *Invent. Math.*, 170(1):33–101, 2007.
25. I. M. Isaacs and G. Navarro. New refinements of the McKay conjecture for arbitrary finite groups. *Ann. of Math. (2)*, 156(1):333–344, 2002.
26. C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
27. A. W. Knapp. *Lie groups, Lie algebras, and cohomology*, volume 34 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1988.
28. M. Le. A divisibility problem concerning group theory. *Pure Appl. Math. Q.*, 8(3):689–691, 2012.
29. M. W. Liebeck. Applications of character theory of finite simple groups. In *Local representation theory and simple groups*, EMS Ser. Lect. Math., pages 323–352. Eur. Math. Soc., Zürich, 2018.
30. M. W. Liebeck, E. A. O'Brien, A. Shalev, and P. H. Tiep. The Ore conjecture. *J. Eur. Math. Soc. (JEMS)*, 12(4):939–1008, 2010.
31. G. Malle. The proof of Ore's conjecture (after Ellers-Gordeev and Liebeck-O'Brien-Shalev-Tiep). *Astérisque*, (361):Exp. No. 1069, ix, 325–348, 2014.
32. G. Malle and B. Späth. Characters of odd degree. *Ann. of Math. (2)*, 184(3):869–908, 2016.
33. O. Ore. Some remarks on commutators. *Proc. Amer. Math. Soc.*, 2:307–314, 1951.
34. J.-P. Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
35. J.-P. Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.
36. B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.
37. N. M. Stephens. On the Feit-Thompson conjecture. *Math. Comp.*, 25:625, 1971.
38. A. Terras. *Fourier analysis on finite groups and applications*, volume 43 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.
39. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.
40. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. II. *Pacific J. Math.*, 33:451–536, 1970.
41. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. III. *Pacific J. Math.*, 39:483–534, 1971.
42. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. IV, V, VI. *Pacific J. Math.*, 48, 1973.
43. B. Walsh. Classroom Notes: The Scarcity of Cross Products on Euclidean Spaces. *Amer. Math. Monthly*, 74(2):188–194, 1967.
44. R. A. Wilson. The McKay conjecture is true for the sporadic simple groups. *J. Algebra*, 207(1):294–305, 1998.

Index