Leandro Vendramin

Representation theory of algebras

Notes

Tuesday 5th July, 2022

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 thirteen two-hours lectures.

Most of the material is based on standard results the representation theory of finite groups. Basic texts on representation theory are [2] and [17].

This version was compiled on Tuesday 5$^{\text{th}}$ July, 2022 at 21:40.

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 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 an 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 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 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 $n_1, \dots, n_k \in \mathbb{Z}_{>0}$.

We also basic 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 $x_1, \dots, x_m \in I$. One proves that the Jacboson 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

Kolchin

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 nil.

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 nil.

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, as each element being nilpotent does not force products of distinct elements to vanish.

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

Note that a nil algebra cannot have one.

pro:unit

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 $B/I \simeq K$ 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.

xca:unit **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 an ideal of A, Exercise 2.7 shows that A is a unitary algebra. □

Now we prove another nice result of Wedderburn:

thm: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

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

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. We note that the theorem can be extended to any algebraically closed field. We state and proof Wedderburn's theorem in the case of complex numbers to simplify a little bit 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 $J(A) = A$, then 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 $a_1, \dots, a_N \in A$. Then

$$\pi(a_1 \cdots a_N) = \pi(a_1) \cdots \pi(a_N) = 0,$$

as $(A/J(A))^N = \{0\}$ since $N \geq m$. This means that $a_1 \cdots a_N \in J(A)$. Since $N \geq n$, it follows that $a_1 \cdots a_N = 0$. Thus $J(A) = \{0\}$ and hence 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 $T_g\colon V \to V$, $x \mapsto gx$.

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 $ge_i = v_i$ for all $i \in \{1, \dots, n\}$.

`Borel subgroup`

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:

pro:unipotent

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

Proof. 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 $g_1, \dots, g_m \in G$. The minimality of m implies that there exist $h_1, \dots, h_{m-1} \in G$ 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 $gv = v$. □

thm:Kolchin

Theorem 2.16 (Kolchin). *Every unipotent subgroup of $\mathbf{GL}_n(\mathbb{C})$ is conjugate of 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 $(W_1, \dots, W_n)$ of $V = \mathbb{C}^n$ 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,

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

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 $n = \dim V$. If $n = 1$, the result is trivial. Assume the result holds for $n-1$. By the previous proposition, there exists a non-zero $v \in V$ such that $gv = v$ for all $g \in G$. Let $Q = V/\langle v\rangle$ and $\pi\colon V \to Q$ 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

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

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,

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

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

The ideas behind the theorem are somewhat connected to Sylow's theory. The key is to consider 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 $|O(v_j)| \geq 2$ for all $j \in \{1, \dots, m\}$. 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 $x \in G$. $\square$

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

pro:Kolchin **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 multplication. 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 $\{v_1, \dots, v_n\}$ of V and a sequence $\{0\} \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_n = V$, where $V_j = \langle v_1, \dots, v_j \rangle$ for all $j \in \{1, \dots, n\}$. Moreover, $PV_j \subseteq V_j$ and $Pv_j = v_j + V_{j-1}$ for all j. This means precisely that in the basis $\{v_1, \dots, v_n\}$ every element of P is an upper triangular matrix with ones in the main diagonal. $\square$

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 $n_p \equiv 1 \mod p$.

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.

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

Proof. We need to 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 $p_0(m) \in S$.

Note that, in general, p_0 is not a $K[G]$-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 $K[G]$-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 $M = S \oplus \ker(p)$. $\square$

Exercise 3.4. 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 $\mathbb{C}[G]$-module with

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

Prove that M is a semisimple $\mathbb{C}[G]$-module that is not simple.

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 $M = \mathbb{R}^{2\times 1}$ 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.

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 3.6. *Let K be a finite group of order m. Assume that K acts by automorphisms pn $V = U \times W$, 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 3.7. *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. □

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 3.8. *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 $\dim Z(\mathbb{C}[G])$ is equal to the number of conjugacy classes of G. □

Exercise 3.9. Let G be a finite group of order n with k conjugacy classes. Let $m = (G : [G,G])$. Prove that $m + 3m \geq 4k$.

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

Exercise 3.10. 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 3.11. 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 $\mathbb{C}[G] \simeq \mathbb{C} \times \mathbb{C} \times M_2(\mathbb{C})$.

Lecture 3

§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 $\mathrm{sign}\colon \mathbb{S}_n \to \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ 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.

xca:degree-one

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

$$\rho\colon G \to \mathbf{GL}_3(\mathbb{R}), \quad g \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Thus g acts on $\mathbb{R}^3$ by left matrix multiplication,

$$g\cdot(x,y,z)=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\begin{pmatrix}x\\y\\z\end{pmatrix}.$$

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,

$$\begin{pmatrix}y_0\\z_0\\x_0\end{pmatrix}=\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}\begin{pmatrix}x_0\\y_0\\z_0\end{pmatrix}\in S.$$

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 $x_0=\lambda^3x_0$. 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?

xca:deg2

Exercise 4.18. Let $\phi\colon G\to\mathbf{GL}(V)$, $g\mapsto\phi_g$, be a degree-two representation. Prove that ϕ is ireeducible 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.

We now describe three important 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 $\{v_1,\dots,v_k\}$ and W be a vector space with basis $\{w_1,\dots,w_l\}$. 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 $\rho_1, \dots, \rho_n$ 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 $\rho_i\colon G \to \mathbf{GL}(V_i)$, $i \in \{1, \dots, n\}$, 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.

xca:equivalence

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 compeltely reducible.

Lecture 4

§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.

Proposition 5.2. *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) $|\chi(g)| \leq \chi(1)$.

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

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

If two representations are equivalent, their characters are equal.

Definition 5.3. 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 5.4. Let G be a finite group. For a conjugacy class K of G let

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

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 5.5. *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 5.6. *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 $\rho \otimes \psi$ 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 $\{v_i \otimes w_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ 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 5.7. *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 irreducible 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 $e_ie_j = 0$ 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 $\dim S_j \neq 0$. $\square$

Theorem 5.8. *Let G be a finite group and $S_1,\dots,S_k$ be the simple $\mathbb{C}[G]$-modules (up to isomorphism). If $V = \oplus_{i=1}^k a_jS_j$, 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 $U \simeq V$. $\square$

Exercise 5.9. 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:

xca:char_Hom **Exercise 5.10.** 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 5.11. 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

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

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

Lemma 5.12. $\dim U^G = \frac{1}{|G|} \sum_{x \in G} \chi_U(x)$

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 5.13. *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 5.10,

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

Since $\dim \operatorname{Hom}_G(U,V)\in\mathbb{R}$, 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 $\operatorname{Irr}(G)=\{\chi_1,\dots,\chi_k\}$. Note that k be the number of conjugacy classes of G. Let $g_1,\dots,g_k$ 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 $i,j\in\{1,\dots,k\}$.

exa:S3 **Example 5.14.** Let $G=\mathbb{S}_3$. The group G has three conjugacy classes, so $|\operatorname{Irr}(G)|=3$. 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	?	?

Exercise 5.15. Prove Schur's lemma: 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 very useful application of Schur's lemma. Let G be a finite group and S be a simple $\mathbb{C}[G]$-module. We claim that $\operatorname{Hom}_G(S,S)\simeq\mathbb{C}$. In fact, let $f\in\operatorname{Hom}_G(S,S)$ and $\lambda\in\mathbb{C}$ be an eigenvector of f. The such that $f-\lambda\,\mathrm{id}\colon S\to S$ is not invertible. By Schur's lemma, $f-\lambda\,\mathrm{id}=0$ and hence $f=\lambda\,\mathrm{id}$.

Theorem 5.16 (Schur). *Let G be a finite group and $\chi,\psi\in\operatorname{Irr}(G)$. Then*

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

Proof. Let $S_1,\dots,S_k$ be the simples of $\mathbb{C}[G]$. Then

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

But we know that $S_i\simeq S_j$ if and only if χ... □

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 5.17. 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 $\mathrm{Irr}(G) = \{\chi_1,\dots,\chi_k\}$. If $\alpha = \sum a_i\chi_i$, then $\alpha = \sum\langle\alpha,\chi_i\rangle\chi_i$.

Theorem 5.18. *Let G be a finite group and $S_1,\dots,S_k$ be the simples of G. Then*

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

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

$$\mathbb{C}[G] \simeq a_1S_1 \oplus \cdots \oplus a_kS_k$$

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

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

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

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

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 5.19. 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 $\langle \alpha, \alpha \rangle = n$.

Lecture 5

§6. Schur's othogonality relations

We now prove Schur's second orthogonality relation.

Theorem 6.1 (Schur). *Let G be a finite group and $g, h \in G$. Then*

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

Proof. Let $g_1, \dots, g_r$ be the representative of conjugacy classes of G. Assume that $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. For each $k \in \{1, \dots, r\}$ let $c_k = (G : G_C(g_k))$ 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 $I = \frac{1}{|G|} X D X^*$, where I denotes the identity matrix, $X_{ij} = \chi_i(g_j)$, $X^* = \overline{X}^T$ and

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

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

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

Theorem 6.2 (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 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 $V = \mathbb{C}[G]$ be the vector space with basis $\{e_g : g \in G\}$. The action of G on G by conjugation induces a group homomorphism $\rho\colon G \to \mathbf{GL}(V)$, $g \mapsto \rho_g$, where $\rho_g(e_h) = e_{ghg^{-1}}$. The matrix of ρ_g in the basis $\{e_g : g \in G\}$ is

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

Then

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

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

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

□

§7. Algebraic numbers and characters

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

Let $\mathbb{A}$ be the set of algebraic numbers.

Proposition 7.2. $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.

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 $m/n \in \mathbb{Z}$. □

Proposition 7.3. *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

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

thm:Asubring **Theorem 7.4.** $\mathbb{A}$ *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 $Av = \alpha v$, β is an eigenvalue of an integer matrix $B \in \mathbb{Z}^{m\times m}$, say $Bw = \beta w$. Then

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

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. $\square$

thm:A **Theorem 7.5.** *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 $\chi_\rho = \chi$. Since φ_g is diagonalizable with eigenvalues $\lambda_1, \dots, \lambda_k \in \mathbb{A}$ (because G is finite and the λ_j are roots of one),

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

Theorem 7.6. *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 7.7. *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 7.5. 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:

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

From this 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,

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

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

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

Therefore

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

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

§8. Frobenius' theorem

degree
thm:Frobenius_chi(1)

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 $C_1, \dots, C_r$ 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 of 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. □

Lecture 6

thm:Schur_chi(1)

Theorem 8.4 (Schur). *Let G be a finite group and $\chi \in \operatorname{Irr}(G)$. 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 $\chi \in \operatorname{Irr}(G)$ and $\chi_1 \in \operatorname{Irr}(G_1)$.

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

$$\lambda(z_1z_2)v = \rho_{z_1z_2}(v) = \rho_{z_1}\rho_{z_2}(v) = \lambda(z_2)\rho_{z_1}(v) = \lambda(z_1)\lambda(z_2)v$$

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

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

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 $|G|(G : Z(G))^{n-1} = \chi(1)^n r$ 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). $\square$

§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:

```
gap> C4 := CyclicGroup(4);;
gap> T := CharacterTable(C4);;
gap> Display(T);
CT1

     2  2  2  2  2

       1a 4a 2a 4b

X.1     1  1  1  1
X.2     1 -1  1 -1
X.3     1  A -1 -A
X.4     1 -A -1  A

A = E(4)
  = Sqrt(-1) = i
```

Some remarks:

1) The symbol `E(4)` denotes a primitive fourth root of 1.
2) The function `CharacterTable` computes some more information, not only the character table of the group. The function computes other stuff:

```
gap> OrdersClassRepresentatives(T);
[ 1, 4, 2, 4 ]
gap> SizesCentralizers(T);
[ 4, 4, 4, 4 ]
gap> SizesConjugacyClasses(T);
[ 1, 1, 1, 1 ]
```

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:

```
gap> Display(CharacterTable(AbelianGroup([2,2])));
CT2

     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 $\mathrm{Irr}(A) = \{\rho_1,\dots,\rho_r\}$ and $\mathrm{Irr}(B) = \{\phi_1,\dots,\phi_s\}$. 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 $i\in\{1,\dots,r\}$ and $j\in\{1,\dots,s\}$, 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

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

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

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

```
gap> S3 := SymmetricGroup(3);;
gap> T := CharacterTable(S3);;
gap> Display(T);
CT3

      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:

```
gap> SizesConjugacyClasses(T);
[ 1, 3, 2 ]
gap> SizesCentralizers(T);
[ 6, 2, 3 ]
gap> SizesConjugacyClasses(T);
[ 1, 3, 2 ]
gap> OrdersClassRepresentatives(T);
[ 1, 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 7

§10. McKay's conjecture

McKay

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 [16].

conjecture:McKay

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 [16, 18]. 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 [25] and uses the classification of finite simple groups. It uses a deep result of Isaacs, Malle and Navarro [19].

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:IsaacsNavarro

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

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

Isaacs–Navarro conjecture is still open. However, it is known to be true for solvable groups, sporadic simple groups and symmetric groups, see [20].

```
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

commutators

Let G be a finite group with conjugacy classes $C_1,\dots,C_s$. For $i\in\{1,\dots,s\}$ 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 7.5, Equality (5.1), we obtained that

$$\omega_\chi(C_i)\omega_\chi(C_j)=\sum_{k=1}^{k}a_{ijk}\omega_\chi(C_k), \tag{7.1}$$ eq:again_omega

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 $C_1,\dots,C_s$. 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 (7.1),

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

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 $C_1,\dots,C_s$ 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 $zgz^{-1} = u_1 v_1$ for some $u_1 \in C_i$ and $v_1 \in C_j$, it follows that $g = (z^{-1}u_1 z)(z^{-1}v_1 z)$, so take $u = z^{-1}u_1 z \in C_i$ and $v = z^{-1}v_1 z \in C_j$). 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 $z_2 x^{-1} z_2 = v$. If $y = z^{-1} z_2$, then g and $[x, y]$ are conjugate, as

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

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 $g \in C_i C_j$, $a_{ijk} > 0$. □

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

Ore

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:Ore

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 [23]. It needs about 70 pages and uses the classification of finite simple groups (CFSG) and character theory. See [24] for more information on Ore's conjecture and its proof a [24].

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 [22] for other applications of character theory.

§13. Cauchy–Frobenius–Burnside theorem

thm:CFB

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*

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

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

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 $x_i \in \mathrm{Fix}(g)$ and $(\rho_g)_{ij} = 0$ if $i \neq j$. Thus

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

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

Claim. $\{v_1, \dots, v_m\}$ 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 $\{v_1, \dots, v_m\} \subseteq V^G$. Moreover, $\{v_1, \dots, v_m\}$ 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 $V^G = \langle v_1, \dots, v_m \rangle$. 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:

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

xca:CFB **Exercise 13.2.** Use the previous idea to prove Theorem 13.1.

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

$$g \cdot (x, y) = (g \cdot x, g \cdot y). \tag{7.2}$$ eq:orbitals

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*

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

Proof. The action (7.2) has $\operatorname{Fix}(g) \times \operatorname{Fix}(g)$ as fixed points, as

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

Now the claim follows from Cauchy–Frobenius–Burnside theorem. $\square$

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 $g \cdot (x, y) = (x_1, y_1)$. $\square$

Lecture 8

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

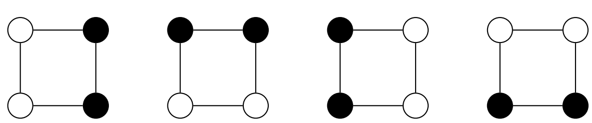
$$2 = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|^2 = \langle \chi, \chi \rangle.$$

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 $\{1, \dots, n\}$. The alternating group $\mathbb{A}_n$ is 2-transitive on $\{1, \dots, n\}$ 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 $\chi(g) = |\mathrm{Fix}(g)| - 1$.

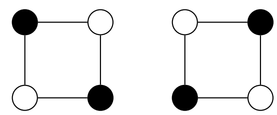
Example 13.9. In how many ways can we color (in black and white) the vertices of a square? We will count colorings up to symmetric. This means that, for example, the colorings



(8.1) eq:orbita

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 (8.1) belong to the same orbit. Another orbit of X is

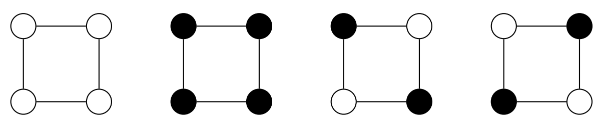


Cauchy–Frobenius–Burnside theorem states that there are

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

orbits.

For each $x \in G = \{1, g, g^2, g^3\}$ we compute $\operatorname{Fix}(x)$. 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

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

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 $\operatorname{cp}(G)$ be the probability that two random elements of G commute. As an application of Cauchy–Frobenius–Burnside theorem we prove that $\operatorname{cp}(G) = k/|G|$, where k is the number of conjugacy classes of G.

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

Proof. Let $C = \{(x, y) \in G \times G : xy = yx\}$. We claim that

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

In fact, 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 $\sum_{g\in G}|C_G(g)| = |C|$.

We now claim that $k/|G| \le 5/8$ if G is non-abelian.

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

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

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, $(G : Z(G)) \geq 4$. 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. Prove that $\operatorname{cp}(Q_8) = 5/8$.

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*

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

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

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

From this the claim follows. □

Theorem 14.6 (Dixon). *If G is a finite simple group, then* $\mathrm{cp}(G) \leq 1/12$.

The theorem appeared in 1970, as a problem in the volume 13 of the *Canadian Math. Bulletin*. The solution appeared in 1973.

Exercise 14.7. Prove that $\mathrm{cp}(\mathbb{A}_5) = 1/12$.

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

Theorem 14.8 (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 [12].

Results on probability of commuting elements generalize in other directions. In [31, 32, 33, 34], Thompson proved the following result:

Theorem 14.9 (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 [7].

There is a probabilistic version of Thompson's theorem:

Theorem 14.10 (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 [13].

§15. Jordan's theorem and applications

We now follow [28] 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

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

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 [6].

§16. Derangements: Cameron–Cohen theorem

Let G be a finite group that acts faithfully and transitively on a finite set X, say $G \leq \mathbb{S}_n$, where $X = \{1, 2, \dots, n\}$. Let G_0 the set of elements $g \in G$ with no fixed-ponts, that is $g(x) \neq x$ 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 $c_0 \geq \frac{1}{n}$.*

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 $1 \leq \chi(g) \leq n$. Since $(\chi(g)-1)(\chi(g)-n) \leq 0$,

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

On the one hand,

$$\begin{aligned} \frac{1}{|G|} \sum_{g \in G} (\chi(g)-1)(\chi(g)-n) \\ &= \frac{1}{|G|} \left\{ \sum_{g \in G_0} + \sum_{g \in G \setminus G_0} \right\} (\chi(g)-1)(\chi(g)-n) \\ &\leq n \frac{|G_0|}{|G|} = nc_0. \end{aligned}$$

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

$$2 - \frac{n+1}{|G|} \sum_{g \in G} \chi(g) + n \leq \frac{1}{|G|} \sum_{g \in G} (\chi(g)-1)(\chi(g)-n) \leq nc_0. \tag{8.2}$$ eq:CameronCohen

Since G is transitive on X, Cauchy–Frobenius–Burnside theorem implies that $\sum_{g \in G} \chi(g) = |G|$. Thus $2-(n+1)+n \leq nc_0$ and hence $1/n \leq c_0$. □

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 $n \geq 2$. If n is not a power of a prime number and $G \neq \mathbb{S}_n$ for $n \in \{2,4,5\}$, then $c_0 \geq 2/n$.*

The proof appears in [10] and uses the classification of finite 2-transitive groups, which depends on the CFSG.

Lecture 9

§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 $\{v_1, \dots, v_n\}$ 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. *Sea G un grupo finito y sea V un $\mathbb{C}[G]$-módulo de dimensión finita con caracter χ. Si el módulo $S(V\otimes V)$ tiene caracter χ_S y el módulo $A(V\otimes V)$ tiene caracter χ_A, entonces*

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

Proof. Sea $g\in G$. Sea $\rho\colon G\to\mathbf{GL}(V)$ la representación asociada al módulo V, es decir $\rho(g)(v)=\rho_g(v)=g\cdot v$. Sabemos que ρ_g es diagonalizable. Sea $\{e_1,\dots,e_n\}$ una base de autovectores de ρ_g, digamos $g\cdot e_i=\lambda_i e_i$ con $\lambda_i\in\mathbb{C}$ para $i\in\{1,\dots,n\}$. En particular, $\chi(g)=\sum_{i=1}^n\lambda_i$.

Como $\{e_i\otimes e_j-e_j\otimes e_i : 1\leq i<j\leq n\}$ es base de $A(V\otimes V)$ y además

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

tenemos $\chi_A(g)=\sum_{1\leq i<j\leq n}\lambda_i\lambda_j$. Por otro lado, como $g^2\cdot e_i=\lambda_i^2 e_i$ para todo i, $\chi(g^2)=\sum_{i=1}^n\lambda_i^2$. Luego

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

Como además $V\otimes V=S(V\otimes V)\oplus A(V\otimes V)$, se tiene $\chi^2(g)=\chi_S(g)+\chi_A(g)$, es decir $\chi_S(g)=\frac{1}{2}(\chi^2(g)+\chi(g^2))$. □

Una **involución** en un grupo es un elemento $x\neq 1$ tal que $x^2=1$. Es posible la cantidad de involuciones con la tabla de caracteres:

Proposition 17.2. *Si G es un grupo finito con t involuciones, entonces*

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

Proof. Supongamos que $\mathrm{Irr}(G)=\{\chi_1,\dots,\chi_k\}$, donde χ_1 es el caracter trivial de G. Para $x\in G$ sea

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

Como θ es una función de clases θ puede escribirse como combinación lineal de los χ_j, digamos

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

Calculamos

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

Luego $\theta(x) = \sum_{\chi \in \mathrm{Irr}(G)} \langle \chi_S - \chi_A, \chi_1 \rangle \chi$ y el resultado se obtiene al evaluar esta expresión en $x = 1$. □

Necesitamos un lema:

Lemma 17.3. *Sea G un grupo finito con k clases de conjugación. Si t es la cantidad de involuciones de G, entonces $t^2 \leq (k-1)(|G|-1)$.*

Proof. Supongamos que $\mathrm{Irr}(G) = \{\chi_1, \dots, \chi_k\}$, donde χ_1 es el carácter trivial de G. Si $\chi \in \mathrm{Irr}(G)$, entonces

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

Como $\chi^2 = \chi_S + \chi_A$, si $\langle \chi^2, \chi_1 \rangle = 1$, entonces el caracter trivial o bien es χ_1 es parte de χ_S o bien es parte de χ_A, pero no de ambos. Esto implica que

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

Vamos a demostrar ahora que $t \leq \sum_{i=2}^{k} \chi_i(1)$. En efecto, como $|\langle \chi_S - \chi_A, \chi_1 \rangle| \leq 1$, entonces

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

de donde se obtiene inmediatamente que $t \leq \sum_{i=2}^{k} \chi_i(1)$. Si utilizamos ahora la desigualdad de Cauchy–Schwartz,

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

Ahora sí estamos en condiciones de dar la primera demostración del teorema de Brauer–Fowler.

Theorem 17.4 (Brauer–Fowler). *Sea G un grupo finito y simple y sea x una involución. Si $|C_G(x)| = n$, entonces $|G| \leq (n^2)!$*

Proof. Supongamos primero que existe un subgrupo propio H de G tal que $(G : H) \leq n^2$. En ese caso, hacemos actuar a G en G/H por multiplicación a izquierda y tenemos un morfismo de grupos $\rho\colon G \to \mathbb{S}_{n^2}$. Como G es un grupo simple, $\ker\rho = \{1\}$ o bien $\ker\rho = G$. Si $\ker\rho = G$, entonces $\rho(g)(yH) = yH$ para todo $g \in G$ e $y \in G$, lo que implica que $g \in H$, una contradicción. Luego ρ es inyectiva y entonces G es isomorfo a un subgrupo de $\mathbb{S}_{n^2}$. En particular, $|G|$ divide a $(n^2)!$

Sea $m = (|G|-1)/t$. Como $|C_G(x)| = n$, el grupo G tiene al menos $|G|/n$ involuciones (pues la clase de conjugación de x tiene tamaño $|G|/n$ y todos sus elementos son involuciones), es decir $t \geq |G|/n$. Luego $m = (|G|-1)/t < n$. Basta demostrar entonces que G contiene un subgrupo de índice $\leq m^2$.

Sean $C_1, \dots, C_k$ las clases de conjugación de G, donde $C_1 = \{1\}$. Como G es simple, $|C_i| > 1$ para todo $i \in \{2, \dots, k\}$. Notar que

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

que vale gracias al lema anterior. Si $|C_i| > m$ para todo $i \in \{2, \dots, k\}$, entonces, como

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

tendríamos

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

una contradicción. Luego existe una clase de conjugación C de G tal que $|C| \leq m^2$. Si $g \in C$, entonces $C_G(g)$ es un subgrupo de G de índice $|C| \leq m^2$. ◻

The bound of Brauer–Fowler's is not important.

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. Induction and restriction

§19. Frobenius' theorem

§20. Some theorems of Burnside

For $n \geq 1$ let $\{e_1, \dots, e_n\}$ be the standard basis of $\mathbb{C}^n$. The **natural representation** of $\mathbb{S}_n$ is $\rho\colon \mathbb{S}_n \to \mathbf{GL}(n,\mathbb{C})$, $\sigma \mapsto \rho_\sigma$, where $\rho_\sigma(e_j) = e_{\sigma(j)}$ for all $j \in \{1, \dots, n\}$. The matrix of ρ_σ in the standard basis is

$$(\rho_\sigma)_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j), \\ 0 & \text{otherwise.} \end{cases} \tag{9.1}$$

eq:Sn_natural

lem:permutaciones **Lemma 20.1.** *For $n \geq 1$ let $\rho\colon \mathbb{S}_n \to \mathbf{GL}(n,\mathbb{C})$ 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 $i, j \in \{1, \dots, n\}$.

Proof. With (9.1) we compute:

$$(A\rho_\sigma)_{ij} = \sum_{k=1}^{n} A_{ik}(\rho_\sigma)_{kj} = A_{i\sigma(j)}, \quad (\rho_\sigma A)_{ij} = \sum_{k=1}^{n} (\rho_\sigma)_{ik} A_{kj} = A_{\sigma^{-1}(i)j}. \quad \square$$

Definition 20.2. 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 $g \in G$.

xca:chi_irreducible **Exercise 20.3.** Let G be a finite group. If $\chi \in \mathrm{Irr}(G)$, then $\overline{\chi}$ is irreducible.

Definition 20.4. 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 20.5 (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 trace ρ_α = trace ρ_β. Let $X \in \mathbf{GL}(r,\mathbb{C})$ be the character matrix of G. By Lemma 20.1,

$$\rho_\alpha X = \overline{X} = X\rho_\beta.$$

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:|G|impar

Corollary 20.6. *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 $h^2gh^{-2} = g$. 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 $|h| \neq |h^2| = |h|/(|h| : 2)$. $\square$

thm:Burnside_mod16

Theorem 20.7 (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 20.8. Prove that every group of order 15 is abelian.

§21. 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 21.1. Abelian groups are solvable.

Example 21.2. 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 21.3. Non-abelian simple groups cannot be solvable.

xca:solvable **Exercise 21.4.** 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 21.5. For $n \geq 5$ the group $\mathbb{A}_n$ is not solvable. It follows that $\mathbb{S}_n$ is not solvable for $n \geq 5$.

xca:pgroups_solvable **Exercise 21.6.** Let p be a prime number. Prove that finite p-groups are solvable.

thm:Burnside_auxiliar **Theorem 21.7 (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.

lem:4Burnside **Lemma 21.8.** *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 $\alpha = (\epsilon_1 + \cdots + \epsilon_n)/n$. Si los ϵ_j no son todos iguales, entonces $N(\alpha) < 1$. Además $N(\beta) < 1$ para todo conjugado algebraico β de α. Como el producto de los conjugados algebraicos de α es un entero de módulo < 1, se conluye que es cero. □

Now we prove the theorem.

Proof of Theorem 21.7. 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 21.9 (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

$$\begin{aligned} 0 &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi(g) \\ &= \sum_{p \mid \chi(1)} \chi(1)\chi(g) + \sum_{p \nmid \chi(1)} \chi(1)\chi(g) + 1, \end{aligned} \tag{9.2}$$

eq:Burnside

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 21.10 (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 21.11 (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.

Theorem 21.12 (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* [**?**]. A formal verification of the proof (based on the computer software Coq) was announced in [9].

En los sesenta se sabía que la demostración del teorema de Feit–Thomson iba a poder simplificarse si la conjetura de Feit–Thompson es verdadera:

No existen primos distintos p y q tales que $\frac{p^q-1}{p-1}$ divide a $\frac{q^p-1}{q-1}$.

Ya no es necesaria esa conjetura para simplificar la demostración, y la conjetura de Feit–Thompson permanece abierta. En [**?**] Stephens demostró que la versión fuerte de la conjetura no es cierta, ya que los enteros $\frac{p^q-1}{p-1}$ y $\frac{q^p-1}{q-1}$ podrían tener factores en común. De hecho, si $p = 17$ y $q = 3313$, entonces

$$\gcd\left(\frac{p^q-1}{p-1}, \frac{q^p-1}{q-1}\right) = 112643.$$

Hoy podemos reproducir los cálculos de Stephens con casi cualquier computadora de escritorio:

```
gap> Gcd((17^3313-1)/16,(3313^17-1)/3312);
112643
```

Another generalization is based on *word maps*. A word map of a group G is a map

$$G^k \to G, \quad (x_1,\dots,x_k) \mapsto w(x_1,\dots,x_k)$$

for some word $w(x_1,\dots,x_k)$ 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 21.13 (Guralnick–Liebeck–O'Brien–Shalev–Tiep). *Let $a,b \geq 0$, p and q be prime numbers and $N = p^aq^b$. The map $(x,y) \mapsto x^Ny^N$ is surjective in every finite simple group.*

The proof appears in [11].

The theorem implies Burnside's theorem. Let G be a group of order $N = p^aq^b$. 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 $(x,y) \mapsto x^Ny^N$ has trivial image in S, a contradiction to the theorem.

Lecture 10

§22. Lie algebras

Definition 22.1. 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

$$[x,x] = 0 \quad \text{for all } x \in L, \tag{10.1}$$ eq:[xx]=0

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0 \quad \text{for all } x, y, z \in L. \tag{10.2}$$ eq:Jacobi

Equality (10.2) is known as the **Jacobi identity**.

Exercise 22.2. Prove that (10.1) 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 22.3. 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 22.4. 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 22.5 (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 22.6. Compute $[e_{ij}, e_{ik}]$.

Example 22.7 (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 22.8. Find a basis of $\mathfrak{sl}(n,\mathbb{C})$.

We discuss a particular important case,

$$\mathfrak{sl}(2,\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} : a, b, c \in \mathbb{C} \right\}$$

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,

$$[h,e] = 2e, \quad [h.f] = -2f, \quad [e,f] = h.$$

Definition 22.9. 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 22.10. 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 22.11. 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 22.12. 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 22.13. Compute $Z(\mathfrak{sl}(n,\mathbb{C}))$.

Exercise 22.14. 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 22.15. Let L and L_1 be Lie algebras. A map $f\colon L \to L_1$ 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 22.16. 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 22.17. 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 22.18. Let $f\colon L \to L_1$ 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 22.19. Let L be a Lie algebra. The **adjoint homomorphism** is the map

$$\mathrm{ad} : L \to \mathfrak{gl}(L), \quad (\mathrm{ad}\, x)(y) = [x, y].$$

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 22.20. Let $f\colon L \to L_1$ be a Lie algebra homomorphism. Prove that $f/\ker f \simeq f(L)$.

Definition 22.21. 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 22.22. Prove that every simple Lie algebra is isomorphic to a linear Lie algebra.

§23. Representations of Lie algebras

Definition 23.1. A **representation** of a Lie algebra L is a Lie homomorphism $\rho\colon L \to \mathfrak{gl}(V)$, 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 23.2. Let L be a Lie algebra. The map $\mathrm{ad} : L \to \mathfrak{gl}(L)$, $x \mapsto (\mathrm{ad}\, x)$, is a lie homomorphism.

Definition 23.3. 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 23.4. Let L be a subalgebra of $\mathfrak{gl}(V)$. Then L is an L-module.

Definition 23.5. 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 23.6. 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 23.7. 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 23.8. 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 23.9. 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 23.10. 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 $S_1, \dots, S_k$.

Exercise 23.11. 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 23.12. 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 23.13. State and prove the isomorphism theorems for modules over Lie algebras.

Exercise 23.14 (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 $\lambda \in \mathbb{C}$.

§24. Representations of $\mathfrak{sl}(2,\mathbb{C})$

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 24.1. Prove that $\varphi\colon \mathfrak{sl}(2,\mathbb{C}) \to \mathfrak{gl}(V_d)$,

$$\varphi(e) = X\frac{\partial}{\partial Y}, \qquad \varphi(f) = Y\frac{\partial}{\partial X}, \qquad \varphi(h) = X\frac{\partial}{\partial X} - Y\frac{\partial}{\partial Y}, \tag{10.3}$$

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 24.2. 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 $a+b=d$.

The following exercise is important:

Exercise 24.3. Prove that each V_d is a simple $\mathfrak{sl}(2,\mathbb{C})$-module.

Now we prove one of the main results of this section.

thm:irreducibles_sl2

Theorem 24.4. *Let V be a finite-dimensional simple $\mathfrak{sl}(2,\mathbb{C})$-module. Then $V \simeq V_d$ for some d.*

We use the notation $e^2v = e(ev)$.
We need some lemmas.

Lemma 24.5. *Let V be an $\mathfrak{sl}(2,\mathbb{C})$-module and $v \in V$ be an eigenvector of h with eigenvalue λ.*

1) *Either $ev = 0$ or ev is an eigenvector of h with eigenvalue $\lambda+2$.*
2) *Either $fv = 0$ or fv is an eigenvector of h with eigenvalue $\lambda-2$.*

Proof. We only prove 1): $h(ev) = e(hv) + [h,e]v = e(\lambda v) + 2ev = (\lambda+2)ev$. □

Lemma 24.6. *Let V be a finite-dimensional $\mathfrak{sl}(2,\mathbb{C})$-module. There exists an eigenvector $w \in V$ of h such that $ew = 0$.*

Proof. The linear map $h\colon V \to V$ has at least one eigenvector v with eigenvalue λ. If the elements $v, ev, e^2v, \ldots$ 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 $e^k v \neq 0$ and $e^{k+1}v = 0$. Let $w = e^k v \neq 0$. Then $hw = (\lambda+2k)w$ and $ew = 0$. □

Now we prove the theorem.

Proof of Theorem 24.4. By the previous lemma, there exists an eigenvector w of h of eigenvalue λ such that $ew = 0$. After considering the sequence $w, fw, f^2w \ldots$, there exists $d \geq 0$ such that $f^d w \neq 0$ and $f^{d+1}w = 0$.

Claim. $\{w, fw, \ldots, f^d w\}$ is a basis of a submodule of V.

The elements are linearly independent, as they are eigenvectors with different eigenvalues. The subspace $W = \langle w, fw, \ldots, f^d w\rangle$ is invariant under h and f. Let us prove that W is invariant under e, that is $eW \subseteq W$. We need to prove that $e(f^k w) \in W$ for all k. We proceed by induction on k. The case $k = 0$ is trivial. If this is true for k, then

$$e(f^k w) = ef(f^{k-1}w) = (fe+h)f^{k+1}w = \ldots$$

Claim. $\lambda = d$.

The matrix of h with respect to $\{w, fw, \ldots, f^d w\}$ is diagonal with trace

$$\lambda + (\lambda-2) + \cdots + (\lambda - 2d) = (d+1)(\lambda - d).$$

Since $[e,f] = h$ has trace zero, it follows that $\lambda = d$.

Claim. $V \simeq V_d$.

The vector spaces are isomorphic, as V has basis $\{w, fw, \ldots, f^d w\}$ and V_d has basis $\{X^d, fX^d, \ldots, f^d X^d\}$, where $f^k X^d \in \mathbb{C}X^{d-k}Y^k$. The eigenvalues of h on $f^k w$ are the same as the eigenvalues of h on $f^k X^d$. Let

$$\varphi\colon V \to V_d, \quad f^k w \mapsto f^k X^d.$$

This bijective linear map commutes with the action of h and f. It also satisfies $\varphi(ew) = \ldots$ and

$$\varphi(ef^k w) = \ldots$$

□

Corollary 24.7.

§25. Enveloping algebras

Topics for final projects

In this chapter we collect some topics for a final presentation.

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. The theorem states that if a finite group G factorizes as $G = AB$ with A and B nilpotent subgroups, then G is solvable. For the proof see [3, Theorem 2.13].

The Drinfeld double of a finite group

See [21, Chapter IX] and [5, 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 [27, §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 [29, §5.2]. Alternatively, one can present the character table of the group $\mathbf{SL}_2(p)$ following Humphreys's paper [15]. The character theory of $\mathbf{SL}_2(q)$ appears in [29, §5.2], see [4, Chapter 20] for details.

Representations of the symmetric group

See for example [29, §10] and [8].

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 [8, 4] and [29, §11].

Fourier analysis on finite groups

See [29, §5] for a very elementary approach and some basic applications. Other applications appear in [30].

McKay's conjecture

Prove McKay's conjecture 10.1 for all sporadic simple groups. This was first proved by Wilson in [35]. 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 [26]. 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 $C_1, \dots, C_k$ be the conjugacy classes of G, where $C_1 = \{1\}$ and $|C_i| > 2n^2$ for all $i \in \{2, \dots, k\}$. 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 [14] Hirsch found a generalization of Burnside's Theorem 20.7. 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?

Hurwitz's theorem

Hurwitz

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

$$\begin{aligned} z_1 &= x_1y_1-x_2y_2-x_3y_3-x_4y_4, & z_2 &= x_2y_1+x_1y_2-x_4y_3+x_3y_4,\\ z_3 &= x_3y_1+x_4y_2+x_1y_3-x_2y_4, & z_4 &= x_4y_1-x_3y_2+x_2y_3-x_1y_4. \end{aligned} \tag{10.4}$$

eq:Hamilton

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 25.1. *Let $n>2$ be an even number. If there exists a group G with generators $\epsilon,x_1,\dots,x_{n-1}$ and relations*

$$x_1^2=\cdots=x_{n-1}^2=\epsilon\neq 1,\quad \epsilon^2=1,\quad [x_i,x_j]=\epsilon \quad \textit{if} \quad i\neq j,$$

then the following statements hold:

1) $|G|=2^n$.
2) $[G,G]=\{1,\epsilon\}$.
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.*

Proof. Primero demostramos las dos primeras afirmaciones. Observemos que $\epsilon\in Z(G)$ pues $\epsilon=x_i^2$ para todo $i\in\{1,\dots,n-1\}$. Como $n-1>2$, $[x_1,x_2]=\epsilon$ y luego

$\epsilon \in [G,G]$. Además $G/\langle \epsilon \rangle$ es abeliano y luego $[G,G] = \langle \epsilon \rangle$. Como $G/[G,G]$ es elemental abeliano de orden 2^{n-1}, se sigue que $|G| = 2^n$.

Demostremos ahora la tercera afirmación. Sea $g \in G \setminus Z(G)$ y sea $x \in G$ tal que $[x,g] \neq 1$. Entonces $[x,g] = \epsilon$ y luego $xgx^{-1} = \epsilon g$.

Demostremos la cuarta afirmación. Sea $g \in G$ y escribamos

$$g = \epsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}},$$

donde $a_j \in \{0,1\}$ para todo $j \in \{1,\dots,n-1\}$. Si $g \in Z(G)$ entonces $gx_i = x_i g$ para todo $i \in \{1,\dots,n-1\}$. Luego $g \in Z(G)$ si y sólo si

$$\epsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}} = x_i (\epsilon^{a_0} x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}) x_i^{-1}.$$

Como $x_i x_j^{a_j} x_i = \epsilon^{a_j} x_j^{a_j}$ si $i \neq j$ y $\epsilon \in Z(G)$, el elemento g es central si y sólo si

$$\sum_{\substack{j=1 \\ j\neq i}}^{n-1} a_j \equiv 0 \bmod 2$$

para todo $i \in \{1,\dots,n-1\}$. En particular,

$$\sum_{j\neq i} a_j \equiv \sum_{j \neq k} a_j$$

para todo $k \neq i$, y en consecuencia $a_i \equiv a_k \bmod 2$ para todo $i,k \in \{1,\dots,n-1\}$. Luego $a_1 = \cdots = a_{n-1}$ y entonces $Z(G) = \{1, x_1 \cdots x_{n-1}, \epsilon, \epsilon x_1 \cdots x_{n-1}\}$.

La última afirmación es entonces consecuencia de la ecuación de clases. Como

$$2^n = |G| = |Z(G)| + \sum_{i=1}^{N} 2 = 4 + 2N,$$

se concluye que G tiene $N + 4 = 2^{n-1} + 2$ clases de conjugación. □

Example 25.2. Las fórmulas (10.4) dan una representación del grupo G del lema anterior. Escribamos a cada z_i como $z_i = \sum_{k=1}^{4} a_{1k}(x_1,\dots,x_4) y_k$. Sea A la matriz tal que $A_{ij} = a_{ij}(x_1,\dots,x_4)$, es decir

$$A = \begin{pmatrix} x_1 & -x_2 & -x_3 & -x_4 \\ x_2 & x_1 & -x_4 & x_3 \\ x_3 & x_4 & x_1 & -x_2 \\ x_4 & -x_3 & x_2 & -x_1 \end{pmatrix}$$

La matriz A puede escribirse como $A = A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4$, donde $A_1 = I$ y

$$A_2 = \begin{pmatrix} & -1 & & \\ 1 & & & \\ & & & -1 \\ & & 1 & \end{pmatrix}, \qquad A_3 = \begin{pmatrix} & & -1 & \\ & & & 1 \\ 1 & & & \\ & -1 & & \end{pmatrix}, \qquad A_4 = \begin{pmatrix} & & & -1 \\ & & -1 & \\ & 1 & & \\ 1 & & & \end{pmatrix}.$$

Para cada $i \in \{1, \dots, 4\}$ sea $B_i = A_4^T A_i$. Entonces $B_i = -B_i^T$ y $B_i^2 = -I$ para todo i y además $B_i B_j = -B_j B_i$ para todo $i \neq j$. El grupo generado por B_1, B_2, B_3 está formado por elementos de la forma

$$\pm B_1^{k_1} B_2^{k_2} B_3^{k_3}$$

para $k_j \in \{0, 1\}$ y luego tiene orden 2^3. La función $G \to \langle B_1, B_2, B_3 \rangle$,

$$x_1 \mapsto B_1, \quad x_2 \mapsto B_2, \quad x_3 \mapsto B_3$$

se extiende entonces a un isomorfismo de grupos.

Theorem 25.3 (Hurwitz). *Si existe una identidad*

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \tag{10.5}$$

eq:Hurwitz

donde los x_j y los y_j son números complejos y las z_k son funciones bilineales en los x_j y los y_j, entonces $n \in \{1, 2, 4, 8\}$.

Proof. Sin pérdida de generalidad podemos suponer que $n > 2$. Para cada $i \in \{1, \dots, n\}$ escribimos

$$z_i = \sum_{k=1}^{n} a_{ik}(x_1, \dots, x_n) y_k,$$

donde las a_{ik} son funciones lineales. Entonces

$$z_i^2 = \sum_{k,l=1}^{n} a_{ik}(x_1, \dots, x_n) a_{il}(x_1, \dots, x_n) y_k y_l$$

para todo $i \in \{1, \dots, n\}$. Si usamos estas expresiones para los z_i en (10.5) y comparamos coeficientes obtenemos

$$\sum_{i=1}^{n} a_{ik}(x_1, \dots, x_n) a_{il}(x_1, \dots, x_n) = \delta_{k,l}(x_1^2 + \cdots + x_n^2), \tag{10.6}$$

eq:delta

donde $\delta_{k,l}$ es la función delta de Kronecker. Escribamos esta última expresión matricialmente. Para eso, sea A la matriz de $n \times n$ dada por

$$A_{ij} = a_{ij}(x_1, \dots, x_n).$$

Entonces

$$AA^T = (x_1^2 + \cdots + x_n^2) I, \tag{10.7}$$

eq:AAT

donde I es la matriz identidad de $n \times n$ pues

$$(AA^T)_{kl} = \sum_{i=1}^{n} a_{ki}(x_1,\ldots,x_n)a_{li}(x_1,\ldots,x_n) = \delta_{kl}(x_1^2+\cdots+x_n^2)$$

por la fórmula (10.6). Como cada $a_{ki}(x_1,\ldots,x_n)$ es una función lineal, existen escalares $\alpha_{ij1},\ldots,a_{ijn} \in \mathbb{C}$ tales que

$$a_{ij}(x_1,\ldots,x_n) = \alpha_{ij1}x_1+\cdots+\alpha_{ijn}x_n.$$

Podemos escribir entonces

$$A = A_1x_1+\cdots+A_nx_n,$$

donde cada A_k es la matriz $(A_k)_{ij} = \alpha_{ijk}$. La fórmula (10.7) queda entonces

$$\sum_{i=1}^{n}\sum_{j=1}^{n} A_iA_j^T x_ix_j = (x_1^2+\cdots+x_n^2)I.$$

Luego

$$A_iA_j^T + A_jA_i^T = 0 \quad i \neq j, \quad A_iA_i^T = I. \tag{10.8}$$

eq:condiciones

Queremos entonces encontrar n matrices complejas de $n \times n$ que cumplan las condiciones (10.8). Para cada $i \in \{1,\ldots,n\}$ sea $B_i = A_n^TA_i$. Entonces (10.8) queda ahora

$$B_iB_j^T + B_jB_i^T = 0 \quad i \neq j, \quad B_iB_i^T = I, \quad B_n = I.$$

Al poner $j = n$ en la primera ecuación obtenemos que $B_i = -B_i^T$ vale para todo $i \in \{1,\ldots,n-1\}$ y luego $B_iB_j = -B_jB_i$ para todo $i,j \in \{1,\ldots,n-1\}$.

Afirmamos que n es par. De hecho, al calcular el determinante de $B_iB_j = -B_jB_i$ obtenemos $\det(B_iB_j) = (-1)^n \det(B_jB_i)$ y luego n es par pues $1 = (-1)^n$.

Si existe una solución a 10.5, entonces se tiene una representación fiel del grupo G del lema anterior (y en particular, este grupo existe). Como $G/[G,G]$ tiene orden 2^{n-1}, G admite 2^{n-1} representaciones de grado uno. Como G tiene $2^{n-1}+2$ clases de conjugación, G admite dos representaciones irreducibles de grados $f_1 > 1$ y $f_2 > 1$ respectivamente. Además

$$2^n = |G| = \underbrace{1+\cdots+1}_{2^{n-1}} + f_1^2 + f_2^2 = 2^{n-1} + f_1^2 + f_2^2$$

implica que $f_1 = f_2 = 2^{\frac{n-2}{2}} > 1$. Nuestra representación de G no contiene subrepresentaciones de grado uno (pues en esta representación ϵ debería representarse como $-I$ y en las representaciones de grado uno ϵ es trivial porque $\epsilon \in [G,G]$). Luego $2^{\frac{n-2}{2}}$ divide a n. Al escribir $n = 2^ab$ con $a \geq 1$ y b un número impar, tenemos que $\frac{n-2}{2} \leq a$ y luego $n \in \{4,8\}$ pues $2^a \leq n \leq 2a+2$. □

Veamos una aplicación.

Theorem 25.4. *Sea V un espacio vectorial real con producto interno tal que* $\dim V = n \geq 3$. *Si existe una función $V \times V \to \mathbb{R}$, $(v,w) \mapsto v \times w$, bilineal tal que $v \times w$ es ortogonal a v y a w y además*

$$\|v \times w\|^2 = \|v\|^2 \|w\|^2 - \langle v, w\rangle^2,$$

donde $\|v\|^2 = \langle v, v\rangle$, entonces $n \in \{3,7\}$.

Proof. Sea $W = V \oplus \mathbb{R}$ con el producto escalar

$$\langle (v_1, r_1), (v_2, r_2)\rangle = \langle v_1, v_2\rangle + r_1 r_2.$$

Primero observemos que

$$\begin{aligned}&\langle v_1 \times v_2 + r_1 v_2 + r_2 v_1, v_1 \times v_2 + r_1 v_2 + r_2 v_1\rangle \\ &\qquad = \|v_1 \times v_2\|^2 + r_1^2 \|v_2\|^2 + 2 r_1 r_2 \langle v_1, v_2\rangle + r_2^2 \|v_1\|^2.\end{aligned}$$

Luego

$$\begin{aligned}(\|v_1\|^2 &+ r_1^2)(\|v_2\|^2 + r_2) \\ &= \|v_1\|^2 \|v_2\|^2 + r_2^2 \|v_1\|^2 + r_1^2 \|v_2\|^2 + r_1^2 r_2^2 \\ &= \|v_1 \times v_2 + r_1 v_1 + r_2 v_2\|^2 - 2 r_1 r_2 \langle v_1, v_2\rangle + \langle v_1, v_2\rangle^2 + r_1^2 r_2^2 \\ &= \|v_1 \times v_2 + r_1 v_1 + r_2 v_2\|^2 + (\langle v_1, v_2\rangle - r_1 r_2)^2 \\ &= z_1^2 + \cdots + z_{n+1}^2,\end{aligned}$$

donde las z_k son funciones bilineales en (v_1, r_1) y (v_2, r_2). El teorema de Hurwitz implica entonces que $n+1 \in \{4,8\}$ y luego $n \in \{3,7\}$. □

Si en el teorema anterior $\dim V = 3$, el resultado nos da el producto vectorial usual. Si en cambio $\dim V = 7$, sea

$$W = \{(v,k,w) : v, w \in V, k \in \mathbb{R}\}$$

con el producto interno dado por

$$\langle (v_1, k_1, w_1), (v_2, k_2, w_2)\rangle = \langle v_1, v_2\rangle + k_1 k_2 + \langle w_1, w_2\rangle.$$

Queda como ejercicio demostrar que la operación

$$\begin{aligned}(v_1, k_1, w_1) &\times (v_2, k_2, w_2) \\ &= (k_1 w_2 - k_2 w_1 + v_1 \times v_2 - w_1 \times w_2, \\ &\qquad - \langle v_1, w_2\rangle + \langle v_2, w_1\rangle, k_2 v_1 - k_1 v_2 - v_1 \times w_2 - w_1 \times v_2)\end{aligned}$$

cumple las propiedades del teorema.

Poincaré–Birkhoff–Witt theorem

Weyl's theorem

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

$$KK^{-1} = K^{-1}K = 1, \qquad KEK^{-1} = q^2 E,$$
$$KFK^{-1} = q^{-2}F, \qquad [E, F] = \frac{1}{(q - q^{-1})}(K - K^{-1}).$$

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 [21, VI]. In particular, if q is not a root of one, finite-dimensional simple $U_q(\mathfrak{sl}(2))$-modules are classified in [21, 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 [21, 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.

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. 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.
5. M. Broué. *On characters of finite groups*. Mathematical Lectures from Peking University. Springer, Singapore, 2017.
6. B. Fein, W. M. Kantor, and M. Schacher. Relative Brauer groups. II. *J. Reine Angew. Math.*, 328:39–57, 1981.
7. P. Flavell. Finite groups in which every two elements generate a soluble subgroup. *Invent. Math.*, 121(2):279–285, 1995.
8. 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.
9. 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.
10. 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.
11. 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.
12. R. M. Guralnick and G. R. Robinson. On the commuting probability in finite groups. *J. Algebra*, 300(2):509–528, 2006.
13. 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.
14. K. A. Hirsch. On a theorem of Burnside. *Quart. J. Math. Oxford Ser. (2)*, 1:97–99, 1950.
15. J. E. Humphreys. Representations of $\mathrm{SL}(2, p)$. *Amer. Math. Monthly*, 82:21–39, 1975.
16. I. M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.*, 95:594–635, 1973.
17. 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].
18. I. M. Isaacs. *Characters of solvable groups*, volume 189 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.

19. I. M. Isaacs, G. Malle, and G. Navarro. A reduction theorem for the McKay conjecture. *Invent. Math.*, 170(1):33–101, 2007.
20. 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.
21. C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.
22. 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.
23. 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.
24. 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.
25. G. Malle and B. Späth. Characters of odd degree. *Ann. of Math. (2)*, 184(3):869–908, 2016.
26. O. Ore. Some remarks on commutators. *Proc. Amer. Math. Soc.*, 2:307–314, 1951.
27. 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.
28. J.-P. Serre. On a theorem of Jordan. *Bull. Amer. Math. Soc. (N.S.)*, 40(4):429–440, 2003.
29. B. Steinberg. *Representation theory of finite groups*. Universitext. Springer, New York, 2012. An introductory approach.
30. A. Terras. *Fourier analysis on finite groups and applications*, volume 43 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.
31. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.*, 74:383–437, 1968.
32. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. II. *Pacific J. Math.*, 33:451–536, 1970.
33. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. III. *Pacific J. Math.*, 39:483–534, 1971.
34. J. G. Thompson. Nonsolvable finite groups all of whose local subgroups are solvable. IV, V, VI. *Pacific J. Math.*, 48, 1973.
35. R. A. Wilson. The McKay conjecture is true for the sporadic simple groups. *J. Algebra*, 207(1):294–305, 1998.

Index