

Leandro Vendramin

Representation theory of finite groups

Notes

Sunday 3rd 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 [14].

This version was compiled on Sunday 3rd July, 2022 at 10:21.

Leandro Vendramin
Brussels, Belgium

Contents

1	1
2	9
3	15
4	21
5	29
6	35
7	37
8	45
Some topics for a final project	51
Some solutions	55
References	57
Index	59

List of topics

§1	Artin–Wedderburn’s theorem	1
§2	Kolchin’s theorem	2
§3	Group algebras	9
§4	Representations	15
§5	Characters	21
§6	Schur’s orthogonality relations	29
§7	Algebraic numbers and characters	30
§8	Frobenius’ theorem	33
§9	Examples of character tables	36
§10	McKay’s conjecture	37
§11	Commutators	39
§12	Ore’s conjecture	41
§13	Cauchy–Frobenius–Burnside’s theorem	43
§14	Commuting probability	46
§15	Jordan’s theorem and applications	48
§16	Derangements: Cameron–Cohen’s theorem	49

Lecture 1

§1. Artin–Wedderburn’s theorem

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

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

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

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

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

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

A (left) **module** M (over a unitary algebra A) is an abelian group M together with a map $A \times M \rightarrow M$, $(a, m) \mapsto am$, 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 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 Jacobson radical of A contains every nilpotent ideal of A . An important fact is that

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

§2. Kolchin's theorem

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 $B/I \simeq \mathbb{C}$. \square

Exercise 2.6. Let A_1, \dots, A_k be algebras. Prove that the ideals of $A_1 \times \dots \times A_k$ are of the form $I_1 \times \dots \times I_k$, 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. \square

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

$$E_{11} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix} = \sum_{i=1}^{n^2} \lambda_i A_i. \quad (1.1) \quad \text{eq:nilpotent}$$

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

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 $\pi: A \rightarrow A/J(A)$ 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. \square

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

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

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

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

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

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

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

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

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 $b f(b)^{-1} \in \ker f = U_n(\mathbb{C})$ and therefore $b = (b f(b)^{-1}) f(b) \in U_n(\mathbb{C})T_n(\mathbb{C})$. \square

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 $v \in \mathbb{C}^n$ 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 $w \in \mathbb{C}^n$ 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 $gv = v$. \square

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 $\pi: V \rightarrow Q$ 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 $\{\pi(v_j) : 1 \leq j \leq n-1\}$ 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

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

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 $\pi(gv_j) = \sum_{i \leq j} \lambda_i \pi(v_i)$. This means that

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

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

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

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

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 multiplication. The previous proposition implies that there exists a non-zero $v_1 \in V$ such that $xv_1 = v_1$ for all $x \in P$. Let $V_1 = \langle v_1 \rangle$. The group P acts on the $(n-1)$ -dimensional vector space V/V_1 by

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

This action is well-defined. As before, there exists a non-zero vector of V/V_1 fixed by P . Thus there exists $v_2 \in V \setminus V_1$ such that $xv_2 + V_1 = v_2 + V_1$. Note that $\{v_1, v_2\}$ is linearly independent, as applying the canonical map $V \rightarrow V/V_1$ 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 $n_p \equiv 1 \pmod{p}$.

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 $t_0 \in T_0$. Let

$$p_0: M \rightarrow S, \quad p_0(m) = s,$$

where $m = s + t_0$ with $s \in S$ and $t_0 \in T_0$. 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

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

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.

§3 Group algebras

There is a multiplicative version of Maschke's theorem. A group G acts by automorphisms on A if there is a group homomorphism $\lambda: G \rightarrow \text{Aut}(A)$. 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 on $V = U \times W$, where U and W are subgroups of V and U is abelian and K -invariant. If the map $U \rightarrow U$, $u \mapsto u^m$, is bijective, then there exists a normal K -invariant subgroup N of V such that $V = U \times N$.*

Proof. Let $\theta: U \times W \rightarrow U$, $(u, w) \mapsto u$. 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

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

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 . \square

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. \square

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

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

and hence $\lambda_g = \lambda_{hg}$ 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 . \square

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 $\mathbb{C}[C^4] \simeq \mathbb{C}^4$.

§3 Group algebras

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: $\{\text{id}\}$, $\{(12), (13), (23)\}$ 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 $\rho: G \rightarrow \mathbf{GL}(V)$, where V is a finite-dimensional vector space. The **degree** (or dimension) of the representation is the integer $\deg \rho = \dim V$.

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

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

where $n = \dim V$.

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

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

is a representation of \mathbb{S}_3 .

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

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

is a representation of G .

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

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

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 $G \rightarrow \mathbf{GL}_3(\mathbb{C})$.

Example 4.6. 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

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

is a representation of degree $|X|$.

Example 4.7. The sign $\text{sign} : \mathbb{S}_n \rightarrow \mathbf{GL}_1(\mathbb{C}) = \mathbb{C}^\times$ 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 $\rho : G \rightarrow \mathbf{GL}(V)$ 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 $\rho : G \rightarrow \mathbf{GL}(V)$, $\rho_g : V \rightarrow V$, $v \mapsto g \cdot v$, is a representation.

Exercise 4.8. Let G be a finite group and $\rho : G \rightarrow \mathbf{GL}(V)$ 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 4.9. Let G be a group and $\phi : G \rightarrow \mathbf{GL}(V)$ and $\psi : G \rightarrow \mathbf{GL}(W)$ be representations of G . We say that ϕ and ψ are **equivalent** if there exists a linear isomorphism $T : V \rightarrow W$ 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 4.10. The representation

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

is equivalent to the representation

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

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 4.11. Let $\rho: G \rightarrow \mathbf{GL}(V)$ 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 4.12. Let $\phi: G \rightarrow \mathbf{GL}(V)$ 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 $\rho: G \rightarrow \mathbf{GL}(V)$ be a representation. If W is a G -invariant subspace of V , then the restriction $\rho|_W: G \rightarrow \mathbf{GL}(W)$ is a representation. In particular, W is a submodule (over $\mathbb{C}[G]$) of V .

Definition 4.13. A representation $\rho: G \rightarrow \mathbf{GL}(V)$ is said to be **irreducible** if $\{0\}$ and V are the only G -invariant subspaces of V .

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

Example 4.14. Degree-one representations are irreducible.

xca:degree-one

Exercise 4.15. 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 4.16. Let $G = \langle g \rangle$ be the cyclic group of three elements and

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

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 $x_0 = \lambda^3 x_0$. Since $x_0 = 0$ implies $y_0 = z_0 = 0$, it follows that $\lambda = 1$. In particular, $x_0 = y_0 = z_0$, a contradiction, as $x_0 + y_0 + z_0 = 0$. Hence $\dim S = 2$ and therefore $S = N$.

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

xca:deg2

Exercise 4.17. Let $\phi: G \rightarrow \mathbf{GL}(V)$, $g \mapsto \phi_g$, be a degree-two representation. Prove that ϕ is irreducible if and only if there is no common eigenvector for all the ϕ_g .

Example 4.18. 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 4.17 shows that ϕ is irreducible.

We now describe three important examples of representations.

Example 4.19 (The trivial representation). The map $\rho: G \rightarrow \mathbb{C}^\times$, $g \mapsto 1$, 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 4.20. Let $\rho: G \rightarrow \mathbf{GL}(V)$ and $\psi: G \rightarrow \mathbf{GL}(W)$ be representations. The **direct sum** $\rho \oplus \psi: G \rightarrow \mathbf{GL}(V \oplus W)$, $g \mapsto (\rho_g, \psi_g)$, 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

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

such that $\{v_i \otimes w_j : 1 \leq i \leq k, 1 \leq j \leq l\}$ 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 4.21. Let V and W be $\mathbb{C}[G]$ -modules. The **tensor product** $V \otimes W$ is a $\mathbb{C}[G]$ -module with

§4 Representations

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

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

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

where

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

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

Exercise 4.22. Let G be a finite group and V and W be $\mathbb{C}[G]$ -modules. Prove that the set $\text{Hom}(V, W)$ of complex linear maps $V \rightarrow W$ is a $\mathbb{C}[G]$ -module with

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

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

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

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 4.23. A representation $\rho: G \rightarrow \mathbf{GL}(V)$ is said to be **completely reducible** if ρ can be decomposed as $\rho = \rho_1 \oplus \cdots \oplus \rho_n$ for some irreducible representations ρ_1, \dots, ρ_n of G .

Note that if $\rho: G \rightarrow \mathbf{GL}(V)$ is completely reducible and $\rho = \rho_1 \oplus \cdots \oplus \rho_n$ for some irreducible representations $\rho_i: G \rightarrow \mathbf{GL}(V_i)$, $i \in \{1, \dots, n\}$, then each V_i is an invariant subspace of V and $V = V_1 \oplus \cdots \oplus V_n$. 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 4.24. A representation $\rho: G \rightarrow \mathbf{GL}(V)$ is **decomposable** if V can be decomposed as $V = S \oplus T$ where S and T are non-zero invariant subspaces of V .

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

xca:equivalence

Exercise 4.25. Let $\rho: G \rightarrow \mathbf{GL}(V)$ and $\psi: G \rightarrow \mathbf{GL}(W)$ be equivalent representations. Prove the following facts:

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

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 $\rho: G \rightarrow \mathbf{GL}(V)$ be a representation. The **character** of ρ is the map $\chi_\rho: G \rightarrow \mathbb{C}, g \mapsto \text{trace } \rho_g$.

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 $\rho: G \rightarrow \mathbf{GL}(V)$ 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

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

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

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

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

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

If two representations are equivalent, their characters are equal.

Definition 5.3. Let G be a group and $f: G \rightarrow \mathbb{C}$ 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

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

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

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

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

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

Proposition 5.5. If $\rho: G \rightarrow \mathbf{GL}(V)$ and $\psi: G \rightarrow \mathbf{GL}(W)$ 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

$$\chi_{\rho \oplus \psi}(g) = \text{trace}((\rho \oplus \psi)_g) = \text{trace}(\rho_g) + \text{trace}(\psi_g) = \chi_\rho(g) + \chi_\psi(g). \quad \square$$

Proposition 5.6. If $\rho: G \rightarrow \mathbf{GL}(V)$ and $\psi: G \rightarrow \mathbf{GL}(W)$ are representations, then

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

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

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

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

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

§5 Characters

We know that it is also possible to define the dual $\rho^*: G \rightarrow \mathbf{GL}(V^*)$ of a representation $\rho: G \rightarrow \mathbf{GL}(V)$ 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 $\chi, \psi: G \rightarrow \mathbb{C}$ 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 $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. By Wedderburn's theorem, there is an algebra isomorphism $f: \mathbb{C}[G] \rightarrow M_{n_1}(\mathbb{C}) \times \dots \times M_{n_k}(\mathbb{C})$, where $\dim S_j = n_j$ for all j . Moreover,

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

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_i . Since $e_i e_j = 0$ if $i \neq j$, it follows that $\chi_i(e_j) = 0$ if $i \neq j$. Moreover, e_j acts as the identity on S_j , thus $\chi_j(e_j) = \dim S_j$.

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

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

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

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

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

For a finite group G we write $\text{Irr}(G)$ 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 $\text{Irr}(G)$ is a basis of $\text{cf}(G)$.

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

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

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

§5 Characters

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

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

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

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*

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

Proof. We claim that

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

Let us first prove that $\text{Hom}_G(U, V) \subseteq \text{Hom}(U, V)^G$. Let $f \in \text{Hom}_G(U, V)$ 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 $\text{Hom}_G(U, V) \supseteq \text{Hom}(U, V)^G$. Let $f \in \text{Hom}(U, V)^G$. Then $f: U \rightarrow V$ 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. \square

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 $g_1 = \operatorname{id}$, $g_2 = (12)$ 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 $U \rightarrow V$ 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 $f - \lambda \operatorname{id}: S \rightarrow S$ is not invertible. By Schur's lemma, $f - \lambda \operatorname{id} = 0$ and hence $f = \lambda \operatorname{id}$.

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 $\chi_i = \chi_j$. \square

§5 Characters

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 $\text{Irr}(G)$ is an orthonormal basis of $\text{cf}(G)$.

The previous exercise has some consequences. Let G be a finite group and assume that $\text{Irr}(G) = \{\chi_1, \dots, \chi_k\}$. 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

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

for some integers $a_1, \dots, a_k \geq 0$. Let $L: G \rightarrow G$, $g \mapsto L_g$, 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 $\text{Char}(G)$ be the set of characters of G .

Exercise 5.19. Let $n \in \{1, 2, 3\}$. Let G be a finite group and $\alpha \in \text{Char}(G)$. Prove that α is the sum of n irreducible characters if and only if $\langle \alpha, \alpha \rangle = n$.

Lecture 5

§6. Schur's orthogonality 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*

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

Proof. Let g_1, \dots, g_r be the representative of conjugacy classes of G . Assume that $\text{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. 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 ,

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

Theorem 6.2 (Solomon). Let G be a finite group and $\text{Irr}(G) = \{\chi_1, \dots, \chi_r\}$. 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 V by conjugation induces a group homomorphism $\rho: G \rightarrow \mathbf{GL}(V)$, $g \mapsto \rho_g$, 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

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

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

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

§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 $f = X^k + a_{k-1}X^{k-1} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$ of degree $k \geq 1$, then

$$0 = n^k f(m/n) = m^k + a_{k-1}m^{k-1}n + \dots + a_1mn^{k-1} + a_0n^k.$$

This implies that

$$m^k = -n \left(a_{k-1}m^{k-1} + \dots + a_1mn^{k-2} + a_0n^{k-1} \right)$$

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

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

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

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 $\chi \in \text{Char}(G)$ 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),

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

Theorem 7.6. *Let G be a finite group, $\chi \in \text{Irr}(G)$ 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 $f = X^k + a_{k-1}X^{k-1} + \dots + a_1X + a_0 \in \mathbb{Z}[X]$ 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, $xz_k = x^k = -a_0 - a_1x - \dots - a_{k-1}x^{k-1}$.

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 $x \in \mathbb{A}$. \square

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

We proceed in several steps. First we prove that $T_i = \lambda \text{id}$ 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 $T_i = \lambda \text{id}$ 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 :

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

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,

§8 Frobenius' theorem

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

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

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

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

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

is well-defined. It is bijective with inverse

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

Hence $|X_g| = |X_h|$.

Now

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

Therefore

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

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

§8. Frobenius' theorem

Theorem 8.1 (Frobenius). *Let G be a finite group and $\chi \in \text{Irr}(G)$. 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 $|G|$. □

degree
 thm:Frobenius_chi(1)

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 $q \not\equiv 1 \pmod{p}$, 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 $\chi \in \text{Irr}(G)$.

Proof. Let $\chi \in \text{Irr}(G)$ be such that $\chi(1) = 2$. Let $\rho: G \rightarrow \mathbf{GL}_2(\mathbb{C})$ 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

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

is a degree-one representation, which means that $\det \rho_g = 1$ for all $g \in G$. By Frobenius's 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. \square

Lecture 6

thm:Schur_chi(1)

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

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

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 $\chi \in \text{Irr}(G)$ and $\chi_1 \in \text{Irr}(G_1)$.

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 $\rho: G \rightarrow \mathbf{GL}(V)$ 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 $\lambda: Z(G) \rightarrow \mathbb{C}^\times$, $z \mapsto \lambda(z)$, is a well-defined group homomorphism, as

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

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

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

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

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

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

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

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

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). □

§9. Examples of character tables

Lecture 7

§10. McKay's conjecture

McKay

Let G be a finite group and let p be a prime number dividing $|G|$. Write $\text{Syl}_p(G)$ 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 in [13].

conjecture:McKay

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

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

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 [13, 15]. Malle and Späth prove the conjecture for $p = 2$.

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

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

The proof appears in [22] and uses the classification of finite simple groups. It uses a deep result of Isaacs, Malle and Navarro [16].

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

```
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 $P \in \text{Syl}_p(G)$, then

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

Isaacs–Navarro's conjecture is still open. However, it is known to be true for solvable groups, sporadic simple groups and symmetric groups, see [17].

```

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's 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 $\chi \in \text{Irr}(G)$ 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

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

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*

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

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 $\chi \in \text{Irr}(G)$ to obtain

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

because

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

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*

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

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,

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

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

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

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

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

We now prove \Rightarrow . 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 $g \in C_i C_j$, $a_{ijk} > 0$. \square

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

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

Proof. Let $\chi \in \text{Irr}(G)$. 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

§12 Ore's conjecture

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

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

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

§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 [20]. It needs about 70 pages and uses the classification of finite simple groups (CFSG) and character theory. See [21] for more information on Ore's conjecture and its proof [21].

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 $\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0$. 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 [19] for other applications of character theory.

§13. Cauchy–Frobenius–Burnside’s 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*

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

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

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

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

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

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

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 $v = \sum_{x \in X} \lambda_x x$ 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

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

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:

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

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

$$g \cdot (x, y) = (g \cdot x, g \cdot y). \quad (7.2)$$

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

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

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

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

Now the claim follows from Cauchy–Frobenius–Burnside’s 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’s theorem is useful to find characters.

Proposition 13.6. *Let G be 2-transitive on X with character $\chi(g) = |\text{Fix}(g)|$. 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’s, the rank of G on X is

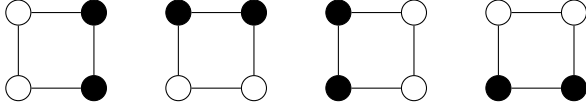
$$2 = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|^2 = \langle \chi, \chi \rangle.$$

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 $\chi(g) = |\text{Fix}(g)| - 1$.

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 $\chi(g) = |\text{Fix}(g)| - 1$.

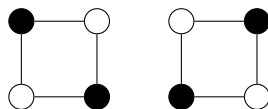
Example 13.9. In how many ways can we color (in black and white) the vertices of a square? We will count colorings up to symmetric. This means that, for example, the colorings


(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

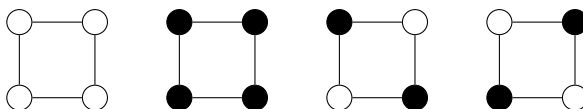


Cauchy–Frobenius–Burnside’s theorem states that there are

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

orbits.

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

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

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

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

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

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

In fact, let G act on G by conjugation. By Cauchy–Frobenius–Burnside’s theorem,

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

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

We now claim that $k/|G| \leq 5/8$ 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 $m \leq (1/2)(|G| - |Z(G)|)$ and hence

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

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

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

that is $k/|G| \leq 5/8$. □

Exercise 14.2. Prove that $\text{cp}(Q_8) = 5/8$.

Exercise 14.3. Let G be a finite non-abelian group and p be the smallest prime number dividing $|G|$. Prove that $\text{cp}(G) \leq (p^2 + p - 1)/p^3$. 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) $\text{cp}(G) \leq \text{cp}(H)$.
- 2) If H is normal in G , then $\text{cp}(G) \leq \text{cp}(G/H) \text{cp}(H)$.

Degrees of irreducible characters give a lower bound:

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

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

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

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

From this the claim follows. \square

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

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

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

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 $\text{cp}(G) > 3/40$, then $G \simeq \mathbb{A}_5 \times T$ for some abelian group T and $\text{cp}(G) = 1/12$.*

The proof appears in [10].

Results on probability of commuting elements generalize in other directions. In [28, 29, 30, 31], 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 [11].

§15. Jordan's theorem and applications

We now follow [25] 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's theorem implies that

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

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

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

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

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 that $|X| = |G/H| > 1$. 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 $g \notin \cup_{x \in G} xHx^{-1}$. \square

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 if and only if 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 class of G . Then $|C| = 1$ if and only if C commute with every conjugacy class of G .*

Proof. We prove \Leftarrow . 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 \Rightarrow . If $C = \{c\}$, then $c \in Z(G)$ and C commute with every conjugacy class of G . \square

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’s 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-points, 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 is the 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 $\chi(g) = |\text{Fix}(g)|$ 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 ,

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

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

Cameron–Cohen’s 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’s 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 [9] and uses the classification of finite 2-transitive groups, which depends on the CFSG.

Topics for final projects

Staircase groups

This topic describes a situation similar to that of §2, but more general. See [2, Chapter 5].

Kegel–Wielandt’s theorem

Prove Kegel–Wielandt’s 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 [18, 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 [24, §8.1].

Characters of $\mathrm{GL}_2(q)$ and $\mathrm{SL}_2(q)$

One possible topic is the character table of $\mathrm{GL}_2(q)$, see [26, §5.2]. Alternatively, one can present the character table of the group $\mathrm{SL}_2(p)$ following Humphreys's paper [12]. The character theory of $\mathrm{SL}_2(q)$ appears in [26, §5.2], see [4, Chapter 20] for details.

Representations of the symmetric group

See for example [26, §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 [26, §11].

Fourier analysis on finite groups

See [26, §5] for a very elementary approach and some basic applications. Other applications appear in [27].

McKay's conjecture

Prove McKay's conjecture 10.1 for all sporadic simple groups. This was first proved by Wilson in [32]. 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 [23]. It is also interesting to prove the conjecture for other "small" simple groups such as $\mathrm{PSL}(3,2)$.

Hirsh's theorem

Some solutions

4.17 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. 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.
10. R. M. Guralnick and G. R. Robinson. On the commuting probability in finite groups. *J. Algebra*, 300(2):509–528, 2006.
11. 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.
12. J. E. Humphreys. Representations of $SL(2, p)$. *Amer. Math. Monthly*, 82:21–39, 1975.
13. I. M. Isaacs. Characters of solvable and symplectic groups. *Amer. J. Math.*, 95:594–635, 1973.
14. 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].
15. I. M. Isaacs. *Characters of solvable groups*, volume 189 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2018.
16. I. M. Isaacs, G. Malle, and G. Navarro. A reduction theorem for the McKay conjecture. *Invent. Math.*, 170(1):33–101, 2007.
17. 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.
18. C. Kassel. *Quantum groups*, volume 155 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

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

Index

- Algebra, 1
 - semisimple, 1
 - unitary, 1
- Augmentation ideal, 9
- Burnside's theorem, 39
- Cameron–Cohen's theorem, 50
- Cauchy–Frobenius–Burnside's theorem, 43
- Character, 21
- Derangements, 49
- Dixon's theorem, 48
- Equivalent representations, 16
- Erdős–Turan's theorem, 46
- Fein–Kantor–Schacher's theorem, 49
- Flag
 - complete, 4
 - standard, 4
- Frobenius' theorem, 33, 40
- Group algebra, 9
- Guralnick–Robinson's theorem, 48
- Guralnick–Wan's theorem, 50
- Guralnick–Wilson's theorem, 48
- Isaacs–Navarro's conjecture, 38
- Jordan's theorem, 48
- Kolchin's theorem, 5
- Liebeck–O'Brien–Shalev–Tiep's theorem, 41
- Malle–Späth's theorem, 37
- Maschke's theorem, 9
 - multiplicative version, 11
- Matrix representation, 15
- McKay's conjecture, 37
- Module, 1
 - semisimple, 1, 9
 - simple, 1, 17
- Nil
 - algebra, 2
 - element, 2
- Nilpotent
 - algebra, 2
 - element, 2
- Orbital, 44
- Ore's conjecture, 41
- Rank, 44
- Representation, 15
 - completely reducible, 19
 - decomposable, 19
 - indecomposable, 19
 - irreducible, 17
- Schur's theorem, 26, 29, 35
- Solomon's theorem, 30
- Submodule, 1
- Sylow's theorems, 7
- Theorem
 - $5/8$, 46
- Thompson's theorem, 48
- Trivial module, 18
- Trivial representation, 18
- Unipotent element, 5
- Unipotent group, 5
- Wedderburn's theorem, 3
- Wildon's theorem, 49

